Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern

3. Tätigkeitsbericht

Vorwort

Das Datenschutzgesetz von Mecklenburg-Vorpommern sieht vor, daß der Landesbeauftragte für den Datenschutz für jeweils zwei Kalenderjahre einen Tätigkeitsbericht vorlegt. Der Dritte Tätigkeitsbericht umfaßt den Zeitraum vom 1. Januar 1996 bis 31. Dezember 1997.

Wie bereits in den vorherigen Berichten habe ich auch diesmal Vorgänge ausgewählt, die einen Gesamteindruck von der Tätigkeit meiner Behörde vermitteln. Einige Beiträge schließen an Sachverhalte an, die in den ersten beiden Berichten dargestellt wurden. Insofern könnte es für den Interessierten nützlich sein, in dem einen oder anderen Fall auf einen dieser Berichte zurückzugreifen.

Für die gute fachliche und angenehme Zusammenarbeit danke ich meinen Amtskollegen beim Bund und in den Ländern. Ebenso danke ich meinen Mitarbeitern für ihre engagierte, zuverlässige und sachkundige Tätigkeit im Berichtszeitraum sowie für ihre Arbeit bei der Gestaltung der einzelnen Beiträge der vorliegenden Publikation.

Dr. Werner Kessel
Landesbeauftragter für den Datenschutz
Mecklenburg-Vorpommern

1 Einleitung

Eine zunehmende Anzahl von Anfragen, Bitten um Beratung und Petitionen aus der Bevölkerung zeugt davon, daß sich immer mehr Bürger unseres Landes ihres Rechts auf informationelle Selbstbestimmung bewußt werden.

Ebenso erfreulich ist es, daß auch die öffentlichen Stellen im Berichtszeitraum zunehmend um Beratung gebeten und die meisten der von mir empfohlenen Maßnahmen umgesetzt haben. Einige der in diesem Bericht aufgenommenen Beiträge geben hiervon einen kleinen Überblick.

Bedauerlicherweise gab es aber auch Ausnahmen. So kam es vor, daß einzelne Behördenmitarbeiter aus Unkenntnis oder aus Sorglosigkeit gegen datenschutzrechtliche Bestimmungen verstoßen haben. Oft folgte danach allerdings die Einsicht, und, soweit es noch möglich war, eine Änderung der Entscheidung.

Nur in wenigen Fällen entwickelte sich die Bearbeitung einzelner Vorgänge in Behörden ausgesprochen bürgerunfreundlich. So war beispielsweise in einer Argumentation über das Für und Wider einer Entscheidung der Bürger letztlich völlig aus dem Blickfeld eines Behördenmitarbeiters geraten, und anstelle einer vernünftigen Sachdiskussion ging es nur noch darum, einen Fehler nicht zugeben zu müssen. Wenn eine Beanstandung allein keine Einsicht bewirkt, so habe ich die Möglichkeit, mich an den Landtag oder an die Öffentlichkeit zu wenden. Auch das war im Berichtszeitraum erforderlich und hat letztlich zu Korrekturen geführt.

Wie bereits in der Vergangenheit spielte - neben Themen wie datenschutzfreundliche Technologien, Kryptokontroverse, Vorschläge zur Novellierung des Landesdatenschutzgesetzes oder der Europäisierung des Datenschutzes - auch dieses Mal wieder der Große Lauschangriff eine maßgebliche Rolle in den datenschutzrechtlichen Diskussionen. Sollten Bundestag und Bundesrat sich für das heimliche Abhören von Wohnungen zum Zwecke der Strafverfolgung entscheiden, so wird die Polizei in Mecklenburg-Vorpommern demnächst drei rechtliche Möglichkeiten erhalten, technische Mittel zum Abhören privater Wohnungen einzusetzen. Zwei davon im präventiven und eine im repressiven Bereich. Bisher ist das Abhören privater Wohnungen nur erlaubt, wenn Gefahr für Leib und Leben besteht. Nach dem Entwurf eines Ände-

rungsgesetzes zum Sicherheits- und Ordnungsgesetz unseres Landes soll dies auch erlaubt werden bei einer Gefahr für die Freiheit einer Person sowie zur vorbeugenden Verbrechensbekämpfung, wenn Tatsachen die Annahme rechtfertigen, daß bestimmte Straftaten begangen werden sollen. Die dritte Möglichkeit ergibt sich, wenn der Bundestag der Absicht der Bundesregierung folgt, den Lauschangriff oder das Abhören privater Wohnungen auch zum Zwecke der Strafverfolgung einzuführen.

2 Neue Aspekte des Datenschutzes

2.1 Datenschutzfreundliche Technologien

In fast allen Lebensbereichen finden wir heute moderne Informations- und Telekommunikationstechnik (IuK-Technik). Immer mehr Menschen kommunizieren beispielsweise weltweit in Mobilfunknetzen und im Internet oder nutzen Chip- oder Magnetstreifenkarten zum elektronischen Bezahlen. Dabei hinterlassen sie zumeist umfangreiche elektronische Spuren. Es fallen in der Regel eine Fülle von Einzeldaten an, die geeignet sind, persönliche Verhaltensprofile zu bilden.

Bisher wurde lediglich der Zugang zu bereits erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten beschränkt, um den Erfordernissen des Datenschutzes zu genügen. Für die konventionelle Datenverarbeitung, bei der Verfahren üblicherweise in Rechenzentren ablaufen und personenbezogene Daten nur in diesem eng begrenzten Wirkungsbereich gespeichert wurden, war das auch lange Zeit eine angemessene und geeignete Methode. Der Schutz der Daten vor Mißbrauch und unberechtigter Kenntnisnahme ließ sich in einem lokal eingegrenzten Umfeld auf überschaubare Weise durch herkömmliche technische und organisatorische Maßnahmen sicherstellen. Die zur Zeit in den Datenschutzgesetzen von Bund und Ländern normierten zehn Kontrollziele (zum Beispiel § 17 Abs. 2 Landesdatenschutzgesetz von Mecklenburg-Vorpommern - DSG MV) sind Ausdruck dieser Schutzphilosophie.

Heute ermöglicht es die moderne IuK-Technik jedoch, Datenbestände weltweit in vielen Rechnersystemen zu verarbeiten. Weltumspannende Datennetze schaffen zudem die Voraussetzung, um verschiedene Datenbestände problemlos zusammenzuführen. Immer mehr personenbezogene Daten werden verarbeitet, und es ist kaum noch zu überschauen, wer wo auf welche Art und Weise mit diesen Daten umgeht. Mit den oben erwähnten herkömmlichen Maßnahmen allein ist es deshalb kaum noch möglich, die Privatheit des einzelnen zu schützen. Es bietet sich an, bereits vor der Erhebung und Speicherung die Menge der zu speichernden personenbezogenen Daten wesentlich zu reduzieren. Hierfür geeignete technische Verfahren, beispielsweise zur frühzeitigen Anonymisierung oder Pseudonymisierung, waren lange Zeit nur einem kleinen Nutzerkreis zugänglich. Sie stehen heute jedoch der breiten Öffentlichkeit preisgünstig und anwendungsbereit zur Verfügung.

Schon das Bundesverfassungsgericht hat im Volkszählungsurteil von 1983 gefordert, bereits bei der Erhebung von Einzelangaben zu prüfen, ob das Ziel der Erhebung nicht auch durch anonyme Verfahren erreicht werden kann. Dennoch spielt bis heute sowohl der sparsame Umgang (Datensparsamkeit) als auch die vollständige Vermeidung des Umgangs mit personenbezogenen Daten (Datenvermeidung) in den unterschiedlichen Anwendungsbereichen der IuK-Technik (beispielsweise elektronische Zahlungsverfahren, Gesundheits- oder Verkehrswesen) nur eine untergeordnete Rolle. In vielen Fällen ermöglichen moderne kryptographische Verfahren zur Verschlüsselung und Signatur jedoch die Anonymisierung oder Pseudonymisierung, ohne daß die Verbindlichkeit und die Ordnungsmäßigkeit der Datenverarbeitung beeinträchtigt werden. Mit dem Begriff „Privacy enhancing technology (PET)“ wird neuerdings international eine Philosophie der Datensparsamkeit beschrieben, die auf der Basis der modernen Datenschutztechnologie ein ganzes System technischer Maßnahmen umfaßt. Eine datenschutzfreundliche Technologie läßt sich aber nur dann wirksam realisieren, wenn das Bemühen um Datensparsamkeit die Entwicklung und den Betrieb von IuK-Systemen ebenso stark beeinflußt wie beispielsweise die Forderung nach Datensicherheit.

Die Datenschutzbeauftragten des Bundes und der Länder wollen in Zusammenarbeit mit Herstellern und Anbietern von Informations- und Telekommunikationstechnik auf datenschutzgerechte Lösungen hinarbeiten. Der Arbeitskreis "Technische und organisatorische Datenschutzfragen" (AK Technik - siehe auch Punkt 3.20.1) hat deshalb ausführlich die Anwendungsmöglichkeiten datenschutzfreundlicher Technologien untersucht. In Arbeitspapieren werden verschiedene Varianten vorgestellt und Handlungsempfehlungen für Industrie, Gesetzgeber und Verbraucher gegeben.

Datensparsamkeit bis hin zur Datenvermeidung läßt sich verwirklichen, wenn datenschutzfreundliche Technologien bereits beim Ausgestalten und Auswählen technischer Einrichtungen von Datenverarbeitungssystemen berücksichtigt werden. Diese Technologien ermöglichen es in vielen Fällen, Daten ohne Personenbezug zu erheben oder bereits personenbezogen erhobene Daten frühzeitig zu anonymisieren. Es wird jedoch oft Systemteile geben, in denen für einen definierten Zeitraum personenbezogene Daten zur Aufgabenerfüllung unabdingbar sind. Um auch solche Systeme datenschutzfreundlich zu gestalten, steht schon heute ein in seiner Datenschutzfreundlichkeit abgestuftes System von Verfahren und Hilfsmitteln zur Verfügung.

Durch Anonymisierung ist es beispielsweise möglich, personenbezogene Daten derart zu verändern, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Der datenschutzfreundliche Einsatz dieses Verfahrens ist aber nur dann gewährleistet, wenn wichtige Einflußfaktoren wie der Zeitpunkt der Anonymisierung, die Rücknahmefestigkeit der Anonymisierungsprozedur, die Menge der Daten, in der sich die Daten des Betroffenen verbergen, und die Verkettungsmöglichkeit von einzelnen Transaktionen desselben Betroffenen in angemessener Weise berücksichtigt werden.

Ist die Anonymisierung nicht möglich oder ist vorgesehen, bei Bedarf und unter Einhaltung vorher definierter Rahmenbedingungen den Personenbezug wiederherzustellen, kann eine Pseudonymisierung eingesetzt werden.

Dabei werden personenbezogene Daten durch eine Zuordnungsvorschrift derart verändert, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nur mit Hilfe dieser Vorschrift einer natürlichen Person zugeordnet werden können. Dazu werden beispielsweise die Identifikationsdaten durch eine Abbildungsvorschrift in ein willkürlich gewähltes Kennzeichen (das Pseudonym) überführt. Die Qualität der Pseudonymisierungsprozedur hängt von den gleichen Einflußfaktoren ab, wie die Stärke der Anonymisierungsprozedur. Unter sonst gleichen Bedingungen ist die Anonymisierung dabei immer datenschutzfreundlicher als die Pseudonymisierung.

Zur Realisierung datenschutzfreundlicher Technologien steht darüber hinaus eine Vielzahl weiterer Hilfsmittel zur Verfügung. Das sind beispielsweise Hashfunktionen, die in vielfältigem Zusammenhang in Sicherheitsverfahren verwendet werden. Sie eignen sich zur Erzeugung von Pseudonymen, zur Erkennung der Datenunversehrtheit oder als Urheber- und Empfängernachweis. Mit digitalen Signaturen, die vor allem aus elektronischen Kommunikationssystemen bekannt sind, kann der Nachweis der Urheberschaft eines digitalen Schriftstücks erbracht werden. Die „blinde digitale Signatur“ stellt eine Variante der digitalen Signatur dar, bei der kein Rückschluß auf denjenigen möglich ist, der das signierte Objekt verwendet. Ein weiteres wichtiges Hilfsmittel sind Vertrauensstellen, die für die Realisierung bestimmter Sicherheitsdienste und für die Akzeptanz ganzer Informationstechnik(IT)-Infrastrukturen erforderlich sind.

Zusammenfassend läßt sich festhalten, daß schon heute moderne Technologien auf der Basis neuer Verfahren und technischer Hilfsmittel verfügbar sind, mit deren Hilfe Hersteller und Anbieter von Informations- und Telekommunikationstechnik datenschutzfreundliche Datenverarbeitungssysteme entwickeln und anbieten könnten. Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb vom Gesetzgeber, daß er die Verwendung datenschutzfreundlicher Technologien durch Schaffung rechtlicher Rahmenbedingungen forciert (siehe 15. Anlage). Sie begrüßen, daß sowohl der Mediendienste-Staatsvertrag der Länder als auch das Teledienstedatenschutzgesetz des Bundes bereits den Grundsatz der Datenvermeidung normieren. Sie erwarten, daß sich neben Anbietern von Tele- und Mediendiensten auch die Hersteller und Anbieter von Datenverarbeitungssystemen bei der Ausgestaltung und Auswahl technischer Einrichtungen am Grundsatz der Datenvermeidung orientieren und von vornherein auf eine konsequente Minimierung gespeicherter personenbezogener Daten achten.

2.2 Das Informations- und Kommunikationsdienste-Gesetz und der Mediendienste-Staatsvertrag

Am 1. August 1997 sind sowohl das Informations- und Kommunikationsdienste-Gesetz (IuKDG) des Bundes als auch der Mediendienste-Staatsvertrag (MDStV) der Länder in Kraft getreten. Damit gehört Deutschland weltweit zu den ersten Ländern, die spezielle Vorschriften für den Bereich Multimedia erlassen haben. Besonders zu begrüßen ist, daß das IuKDG und der MDStV detaillierte Bestimmungen zum Datenschutz enthalten. Die Zahl der vernetzten PC und Multimedia-Dienste steigt ständig. In gleichem Maße nehmen die damit verbundenen Gefahren der Registrierung des Verhaltens der Nutzer und der Manipulation ihrer Aktivitäten zu. Die vorgenannten Regelungen waren daher dringend nötig.

Inhalt und Aufbau

Das IuKDG ist ein sogenanntes Artikelgesetz, das heißt, es besteht aus mehreren Artikeln, die neue Gesetze oder Änderungen bestehender Rechtsvorschriften beinhalten:

Artikel 1: Das Teledienstegesetz (TDG) definiert die Teledienste und regelt ihre Nutzung.

Artikel 2: Das Teledienstedatenschutzgesetz (TDDSG) normiert den Umgang mit den personenbezogenen Daten der Nutzer durch die Diensteanbieter, das Auskunftsrecht der Nutzer und die Datenschutzkontrolle.

Artikel 3: Das Signaturgesetz (SigG) schafft „Rahmenbedingungen für digitale Signaturen [Unterschriften], unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können“ (§ 1 Absatz 1 SigG).

Artikel 4: bis 11 ändern bestehende Gesetze und Verordnungen und regeln das Inkrafttreten der jeweiligen Vorschriften.

Der MDStV enthält fünf Abschnitte:

1. Abschnitt: Allgemeines (Zweck, Geltungsbereich, Begriffsbestimmungen),
2. Abschnitt: Besondere Rechte und Pflichten der Anbieter (Verantwortlichkeit, Inhalt, unzulässige Dienste, Jugendschutz, Gegendarstellung),
3. Abschnitt: Datenschutz,
4. Abschnitt: Aufsicht (Aufsicht über die Einhaltung des Datenschutzes, des Jugendschutzes sowie der übrigen Bestimmungen, Ordnungswidrigkeiten),
5. Abschnitt: Schlußbestimmungen (Geltungsdauer, Änderung des Rundfunkstaatsvertrages -RStV-, Inkrafttreten).

Anwendungsbereich

Das TDG und das TDDSG regeln die Teledienste, der MDStV die Mediendienste. Die Trennung dieser beiden Dienste ist durch die zwischen dem Bund und den Ländern aufgesplittete Gesetzgebungskompetenz in diesem Bereich begründet.

Teledienste sind für eine individuelle Nutzung bestimmte elektronische Informations- und Kommunikationsdienste(IuK-Dienste). Beispiele dafür sind

– Telebanking,

- Wetter- und Börsendaten,
- Telespiele oder
- Angebote zur Nutzung des Internet.

Mediendienste sind an die Allgemeinheit gerichtete IuK-Dienste, die nicht Rundfunk sind. Dazu gehören

- Fernseheinkaufskanäle,
- Dienste zur Verteilung von Meßergebnissen,
- Fernsehtext und
- Abrufdienste, bei denen nicht der individuelle Leistungsaustausch oder die reine Datenübermittlung im Vordergrund stehen.

Wie man am letzten Beispiel sieht, sind die Übergänge zwischen Tele- und Mediendiensten fließend. Im einzelnen kann die Abgrenzung sehr schwierig sein. Aber nicht nur die Trennung dieser beiden Dienstarten bereitet Probleme, sondern im Einzelfall auch die Unterscheidung dieser Dienste von solchen auf der Ebene der Telekommunikation (TK) sowie die Differenzierung zwischen Mediendiensten und Rundfunk.

In Abhängigkeit von der konkreten Einordnung eines Dienstes können somit das TDDSG, der MDStV, der RStV, das TK-Recht, das Bundesdatenschutzgesetz (BDSG) oder ein Landesdatenschutzgesetz (LDSG) zur Anwendung kommen. Oft müssen sogar mehrere dieser Vorschriften herangezogen werden. Dies liegt daran, daß die verschiedenen Dienste nicht nur nebeneinander stehen, sondern teilweise aufeinander aufbauen, also quasi übereinanderliegende Schichten eines einheitlichen Vorgangs bilden. So stellt sich zum Beispiel der Abruf von Meßergebnissen aus dem Internet, welche von einem entsprechenden Verteildienst angeboten werden, durch einen Nutzer folgendermaßen (von unten nach oben) dar:

1. Schicht: Die Daten werden über ein TK-Netz transportiert (TK-Recht für das Verhältnis Nutzer - Betreiber des TK-Netzes).
2. Schicht: Die Datenübertragung erfolgt über das Internet, zu dem sogenannte Provider den Zugang verschaffen (TDDSG/TKG für das Verhältnis Nutzer - Provider).

3. Schicht: Die Daten werden von einem Verteildienst zum Abruf bereitgestellt (MDStV für das Verhältnis Nutzer - Betreiber des Verteildienstes).

4. Schicht: Möglicherweise enthalten die Meßergebnisse auch personenbezogene Daten, zum Beispiel die Daten desjenigen, welcher die Messungen durchgeführt hat (BDSG/LDSG für das Verhältnis Messender - Betreiber des Verteildienstes, je nachdem, ob der Betreiber ein privates Unternehmen oder eine Bundesbehörde -BDSG- oder eine Landesbehörde -LDSG- ist).

Es sind sogar noch weitere Schichten möglich. Man denke nur an zwischengeschaltete Dienste-Vermittler (vergleiche die Service-Provider im Mobilfunk) oder daran, daß der Anbieter der Meßdaten nicht mit dem identisch ist, der sie eingestellt hat.

Von den anzuwendenden Vorschriften hängt ab, welche Rechte der Betroffene hat und welche Stelle die Einhaltung des Datenschutzes kontrolliert. Da die Betroffenenrechte verschieden ausgestaltet sind und die Datenschutzkontrollstellen unterschiedliche Eingriffsbefugnisse haben, ist beim Umgang mit personenbezogenen Daten in diesem Bereich genau zu prüfen, auf welcher Schicht die zugrunde liegende Handlung einzuordnen ist.

Um die oben ausgeführten Abgrenzungsprobleme zwischen den betroffenen Datenschutzkontrollstellen gemeinsam und einvernehmlich zu klären, wurde auf Initiative des Berliner Datenschutzbeauftragten der Kooperationskreis IuK-Datenschutz gegründet. Mitglieder sind der Bundesbeauftragte für den Datenschutz, die Landesbeauftragten für den Datenschutz, die Aufsichtsbehörden für den nicht-öffentlichen Bereich, ein Vertreter der Konferenz der Rundfunkdatenschutzbeauftragten und ein Vertreter der Datenschutzbeauftragten der Landesmedienanstalten. Die Teilnehmer der bisherigen Sitzungen des Kreises waren sich darüber einig, daß neben den Abgrenzungsproblemen auch sonstige Auslegungsfragen besprochen sowie gemeinsame Kontrollen diskutiert werden sollen und daß generell das Ziel einer einheitlichen Rechtsanwendung verfolgt werden muß.

Datenschutzbestimmungen

Die Datenschutzbeauftragten des Bundes und der Länder haben schon im April 1996 die Entschließung „Eckpunkte für die datenschutzrechtliche Regelung von Mediendiensten“ (siehe 17. Anlage) verabschiedet. Sie empfehlen, 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 beziehen sich auf die Aussagen zu den elektronischen Dienstleistungen in ihrer Entschließung zur Modernisierung und europäischen Harmonisierung des Datenschutzrechts vom März 1996 (siehe 1. Anlage). Sie verzichten bewußt auf die Angabe eines Regelungsortes für die datenschutzrechtlichen Eckpunkte und appellieren an die Gesetzgeber in Bund und Ländern, die nötigen Regelungen nicht an Kompetenzstreitigkeiten scheitern zu lassen. Die Entschließung enthält zehn detaillierte Forderungen für multimediaspezifische Vorschriften.

Die im TDDSG und im 3. Abschnitt des MDStV enthaltenen Vorschriften zum Datenschutz berücksichtigen nahezu vollständig diese Eckpunkte. Dadurch, daß die Regelungen dieser beiden Werke fast wörtlich übereinstimmen, wird auch das Problem der Trennung von Tele- und Mediendiensten zu einem großen Teil entschärft. Die Dienstleister müssen nun bei der Anwendung der einschlägigen Datenschutznormen nicht mehr zwischen diesen beiden Dienstarten differenzieren.

Die wichtigsten, im TDDSG und im 3. Abschnitt des MDStV gleichlautenden Vorschriften zum Umgang mit personenbezogenen Daten sind:

- Der Umgang mit personenbezogenen Daten ist nur zulässig, soweit es eine Rechtsvorschrift erlaubt oder der Nutzer eingewilligt hat.

- Die Dienstleistung darf nicht von einer Einwilligung des Nutzers in den Umgang mit seinen Daten für andere Zwecke abhängig gemacht werden.

- Bei der Gestaltung und Auswahl technischer Einrichtungen gelten die Grundsätze der Datenvermeidung und Datensparsamkeit, das heißt, der Umgang mit personenbezogenen Daten ist auf den für die Erbringung der Dienste unbedingt erforderlichen Umfang zu beschränken.

- Vor der Erhebung seiner Daten ist der Nutzer ausführlich über den Umgang mit ihnen zu unterrichten. Der Inhalt der Unterrichtung muß für den Nutzer jederzeit abrufbar sein.

- Der Nutzer hat das Recht, seine Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen. Darauf ist er vor der Erklärung der Einwilligung hinzuweisen.

- Die Einwilligung kann auch elektronisch erklärt werden. An die Voraussetzungen dafür werden hohe Anforderungen gestellt. Unter anderem wird verlangt, daß die Einwilligung nur durch eine eindeutige und bewußte Handlung des Nutzers erklärt werden kann.

- Die Nutzung der Dienste und ihre Bezahlung muß auch anonym oder pseudonym möglich sein, soweit dies dem Anbieter technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

- Der Diensteanbieter hat Vorkehrungen zu treffen, daß
  (-) der Nutzer seine Verbindung zu ihm jederzeit abbrechen kann,
  (-) anfallende Daten sofort gelöscht werden, falls sie nicht zur Abrechnung benötigt werden,
  (-) Dritte von der Nutzung des Dienstes keine Kenntnis erhalten können und
  (-) die bei Nutzung verschiedener Dienste anfallenden Daten getrennt verarbeitet werden.

- Es sind nur pseudonyme Nutzerprofile erlaubt.

Der MDStV enthält zusätzlich die Möglichkeit eines Datenschutz-Audits. Danach können Anbieter von Mediendiensten ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten sowie das Ergebnis der Prüfung veröffentlichen lassen. Allerdings bedarf es zur Umsetzung eines besonderen Gesetzes. Auch im Entwurf des TDDSG war eine Vorschrift zum Datenschutz-Audit vorgesehen. Sie wurde jedoch gestrichen. Dies hat zur Folge, daß Teledienstean bieter, die nicht auch Mediendienste anbieten, nicht mit einer von neutraler Seite überprüften datenschutzgerechten Gestaltung ihrer Dienste Werbung machen können.

Der TDDSG-Entwurf enthielt noch eine Regelung, wonach die Anbieter von Telediensten die Bestandsdaten ihrer Kunden auf Ersuchen an Sicherheitsbehörden zu übermitteln haben. Eine solche Vorschrift haben die Datenschutzbeauftragten in der Entschließung „Geplante Verpflichtung von Teledienstеanbietern, Kundendaten an Sicherheitsbehörden zu übermitteln“ vom April 1997 (siehe 12. Anlage) strikt abgelehnt. Diese im MDStV nicht enthaltene Regelung ist letztlich auch nicht in das TDDSG aufgenommen worden.

Das Signaturgesetz

Das Signaturgesetz regelt die Rahmenbedingungen für den Einsatz digitaler Signaturen. Digitale Signaturen sind digitale Siegel, die aus den zu sichernden Daten mit asymmetrischen kryptographischen Verfahren berechnet werden. Anhand solcher Signaturen kann zuverlässig festgestellt werden, ob die signierten Daten oder die Signaturen integer oder verfälscht sind. Darüber hinaus kann man eindeutig diejenige Person feststellen, die diese Signatur erzeugt hat, und somit auch die Zurechenbarkeit von informationstechnischen Prozessen sichern (vergleiche §§ 1 und 2 SigG). Mit geeignet implementierten digitalen Signaturverfahren werden die im Rechtsverkehr wesentlichen Eigenschaften von handgeschriebenen Unterschriften nachgebildet.

Zum Umgang mit digitalen Signaturen ist eine besondere Infrastruktur erforderlich, die der Verwaltung von Schlüsselpaaren für die kryptographischen Verfahren (siehe Punkt 2.3) und von Zertifikaten dient. In § 3 Abs. 2 SigG ist der Begriff Zertifikat als eine spezielle digitale Bescheinigung definiert, die zum Beispiel einer Person das von ihr benutzte Schlüsselpaar zuordnet. Innerhalb Deutschlands hat das Zertifikatssystem zwei Stufen: Die Regulierungsbehörde für den Telekommunikationsbereich (siehe Punkt 3.10.2) bildet die oberste Ebene. Sie stellt Zertifikate für Schlüssel sogenannter Zertifizierungsstellen aus, die ihrerseits für ihre Kunden Schlüssel zertifizieren. Datenschutzrechtlich bedeutsam ist diese Infrastruktur aus folgenden Gründen:

- Zum Betrieb der Infrastruktur selbst sind personenbezogene Daten erforderlich. Zertifizierungsstellen prüfen die Identitäten ihrer Kunden anhand von Ausweisdokumenten. Sofern die Kunden es wünschen, nehmen sie auch zusätzliche Angaben in die Zertifikate auf. Es ist sogar möglich, einen Schlüssel mit einem Pseudonym anstelle eines Namens zu verbinden.

Um Kommunikationspartnern die Prüfung von signierten Dokumenten zu erleichtern, werden alle ausgestellten Zertifikate in einer Datenbank für jedermann zum Abruf bereitgehalten. Berechtigte Personen dürfen jederzeit Signaturschlüssel sperren lassen. Diese Möglichkeit wird zum Beispiel derjenige nutzen, dessen Schlüssel in falsche Hände geraten oder gar mißbraucht worden ist. Damit ein Kommunikationspartner nicht versehentlich Nachrichten anerkennt, die mit einem gesperrten Schlüssel signiert worden sind, werden die Sperrungen in der Datenbank besonders gekennzeichnet.

– Eine vergleichbare Infrastruktur eignet sich auch dazu, Schlüssel zu verwalten, mit denen die Vertraulichkeit von Nachrichten gesichert werden soll. Auf diese Weise wird die vertrauliche Datenkommunikation in offenen Netzen unterstützt und damit eine in der Datenschutzpraxis häufig auftretende Schwachstelle beseitigt. Einige potentielle Betreiber von Zertifizierungsstellen planen, die Verwaltung von Schlüsseln zur Signatur und zur Geheimhaltung miteinander zu verbinden.

Das Signaturgesetz enthält in § 16 eine Verordnungsermächtigung, von welcher der Bundesgesetzgeber bereits Gebrauch gemacht hat. Zum 1. November 1997 ist die Signaturverordnung (SigV) in Kraft getreten. Dort sind Verfahrensfragen, vor allem jedoch technische Anforderungen an die Systeme zum Umgang mit digitalen Signaturen geregelt. Um den technischen Entwicklungen schneller als mit einer Rechtsverordnung folgen zu können, wurde das Bundesamt für Sicherheit in der Informationstechnik (BSI) beauftragt, geeignete IT-Sicherheitsmaßnahmen zu bestimmen (vergleiche §§ 12 und 16 SigV).

Zu Rechtsvorschriften zur digitalen Signatur liegen auch international bisher kaum Erfahrungen vor. Aus diesem Grund ist es sicher nicht verwunderlich, daß noch Raum für Verbesserungen geblieben ist. So ist es aus datenschutzrechtlicher Sicht empfehlenswert, die Liste der gesperrten Signaturschlüssel pseudonym zu führen.

Als nächstes sind die digitalen Signaturen in Form- und Verfahrensvorschriften einzubetten. Dann wird es jedermann möglich sein, beispielsweise mit einer digital signierten Nachricht einen Urkundsprozeß zu führen oder die Einkommensteuererklärung digital signiert an das Finanzamt zu übermitteln.

Ausblick

Das IuKDG und der MDStV enthalten Elemente, die es verdienen, auch in andere nationale und internationale Rechtsvorschriften zum Umgang mit personenbezogenen Daten aufgenommen zu werden:

- die konsequente Berücksichtigung der Grundsätze der Datenvermeidung und -sparsamkeit,
- die Nennung der Voraussetzungen für eine elektronische Einwilligung,
- die Pflicht zur umfassenden Unterrichtung des Nutzers über den Umgang mit seinen Daten,
- die Pflicht zur Ermöglichung anonymer oder pseudonymer Nutzung und Zahlung,
- die Möglichkeit eines Datenschutz-Audits und
- die Schaffung von Voraussetzungen für zuverlässige und sichere digitale Signaturen.

Zu denken ist hier insbesondere an die anstehende Novellierung der Datenschutzgesetze des Bundes und der Länder zur Umsetzung der europäischen Datenschutzrichtlinie (siehe Punkt 2.4). Die Grundsätze der Datenvermeidung und -sparsamkeit sowie anonyme und pseudonyme Verfahren sollten dabei übernommen werden. Im novellierten Hamburgischen Datenschutzgesetz ist dies bereits geschehen.

Das Datenschutz-Audit liefert den Unternehmen gute Werbemöglichkeiten und den Kunden einen wertvollen Hinweis auf den datenschutzgerechten Umgang mit ihren Daten. Es bietet sich daher insbesondere für das Bundesdatenschutzgesetz an, das auch den nicht-öffentlichen Bereich regelt.

Das Internet ist international. Die Landes- und die Bundesregierung sowie die Gremien, die sich länderübergreifend mit elektronischen Medien befassen, sind daher aufgefordert, sich dafür einzusetzen, daß die oben stehenden Prinzipien in europäische und internationale Regelungen für den Multimedia-Bereich Eingang finden. Nur so können auch ausländische Diensteanbieter ohne Niederlassung in Deutschland erfaßt und die Verbindlichkeit der internationalen elektronischen Kommunikation gewährleistet werden.

2.3 Verschlüsselung reglementieren?

Die Bundesregierung prüft seit einiger Zeit, ob der Einsatz von Verschlüsselungsverfahren rechtlich geregelt werden muß und kann (vgl. Bundestags-Drucksachen BT-Drs. 13/1889 und BT-Drs. 13/4105). Es wird befürchtet, daß Sicherheitsbehörden im Rahmen staatlicher Abhör- und Überwachungsmaßnahmen künftig keine Nachrichteninhalte mehr entziffern oder nicht einmal mehr feststellen können, ob überhaupt eine versteckte Nachricht übermittelt wurde beziehungsweise gespeichert ist.

Ursache für diese Befürchtung ist die Tatsache, daß immer mehr preiswerte und äußerst leistungsfähige Datenverarbeitungs- und Kommunikationstechnik zur Verfügung steht, die es auch Nichtspezialisten ermöglicht, kryptographische Verfahren in relativ einfacher Weise zu nutzen.

Die in diesem Zusammenhang recht kontrovers geführte Diskussion ist unter dem Begriff „Kryptokontroverse“ bundesweit bekanntgeworden. Politiker, Wissenschaftler, Wirtschaftsfachleute und Informatiker bemühen sich herauszufinden, ob das Verbot oder eine Einschränkung der Verschlüsselung verfassungsrechtlich zulässig, technisch sinnvoll durchsetzbar und wirtschaftlich vertretbar ist. Auch die Datenschutzbeauftragten beteiligen sich wegen der zentralen Bedeutung des Themas für das Recht auf informationelle Selbstbestimmung der Bürger in der Informationsgesellschaft an dieser Diskussion. Sie sehen insbesondere durch eine Reglementierung die durch Artikel 10 des Grundgesetzes geschützte vertrauliche und unbeobachtete Kommunikation gefährdet.

Prinzipiell wäre eine Kryptoreglementierung durch entsprechende Vorschriften nur dann sinnvoll, wenn sich die Einhaltung dieser Vorschriften auch tatsächlich kontrollieren läßt. Die verfassungsrechtliche Zulässigkeit solcher Reglementierungen muß insbesondere deshalb in Frage gestellt werden, weil die dann erforderlichen Überwachungsmaßnahmen jeden Bürger treffen könnten. Auch ohne Vorliegen eines Anhaltspunktes für einen Verstoß müßten nämlich Stichprobenkontrollen erfolgen. Ein Eingriff in das Fernmeldegeheimnis wäre unvermeidbar, da in jedem Fall Kommunikationsbeziehungen und Kommunikationsinhalte bekannt würden. Darüber hinaus ist ungewiß, auf welche Weise Abhörmaßnahmen bei den Sicherheitsbehörden selbst nachträglich wirksam kontrolliert werden können.

Eine Arbeitsgruppe des Arbeitskreises "Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (siehe auch Punkt 3.20.1) hat eine Ausarbeitung zu Grenzen und Möglichkeiten der staatlichen Reglementierung des Einsatzes von Verschlüsselungsverfahren erstellt, die insbesondere die technischen Aspekte dieses Themas beleuchtet. Die folgenden Erläuterungen basieren zum Teil auf diesem Papier.

Der Einsatz von Verschlüsselungsverfahren wird hier für unterschiedliche Bereiche der Informations- und Kommunikationstechnik untersucht. Sowohl im Rahmen von Telekommunikationsvorgängen als auch bei der Speicherung auf elektronischen Datenträgern können Daten verschlüsselt werden. Darüber hinaus werden kryptographische Verfahren im Bereich der digitalen Signatur angewendet.

Die Frage nach der Überwachung der Telekommunikation unter Berücksichtigung verfügbarer Verschlüsselungsverfahren führt zu folgenden Handlungsalternativen:

a) Der Einsatz von Verschlüsselungsverfahren wird verboten; gegebenenfalls besteht ein Genehmigungsvorbehalt.
b) Es werden nur Algorithmen und Verfahren zugelassen, die Schwachstellen besitzen, welche 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.

Im einzelnen wären folgende Konsequenzen absehbar:

zu a)

Die Sicherheitsbehörden könnten ihren gesetzlichen Überwachungsaufgaben bei unverschlüsselter Kommunikation mit vergleichsweise geringem Aufwand nachkommen. Der Bürger wäre selbst einfachsten Abhöraktionen durch neugierige Schnüffler oder der zufälligen Kenntnisnahme durch Dritte schutzlos ausgeliefert. Das betrifft beispielsweise den

Versand elektronischer Post (E-Mail) im Internet. Auch Firmen wären nicht in der Lage, sich gegen Spionage zu schützen.

zu b)

Verschlüsselungsverfahren ermöglichen nicht nur den Sicherheitsbehörden die Dechiffrierung und anschließende Überwachung der Kommunikation. Auch potentielle Angreifer (zum Beispiel ausländische Nachrichtendienste oder kriminelle Organisationen) werden in die Lage versetzt, Verfahren zu brechen und unberechtigt Kenntnis von übermittelten oder gespeicherten Informationen zu erhalten. Diese unerwünschte Dechiffrierung würde nicht registriert und wäre nicht kontrollierbar. Schon heute werden Exportversionen amerikanischer Verschlüsselungssoftware am Markt angeboten und in der Praxis eingesetzt, die schwächere Algorithmen oder verkürzte Schlüssel beinhalten. In diesen Fällen können mögliche Schlüssel mit relativ geringem Aufwand durch Ausprobieren gefunden werden.

Die Sicherheitsbehörden können im Rahmen des geltenden Rechts mit einem überschaubaren Aufwand die Kommunikation abhören. Um diese Handlungsalternative umzusetzen, darf nur zugelassene Verschlüsselungssoftware benutzt werden. Für den Bürger bedeutet diese Alternative, daß er seine Daten lediglich gegen zufällige Kenntnisnahme schützen kann. Er wird jedoch nie sicher sein, ob und wer möglicherweise trotzdem seine Kommunikation verfolgt.

zu c)

Eine erhebliche Schwachstelle dieser Alternative besteht darin, daß zum Hinterlegen von Schlüsselteilen oder ganzen Schlüsseln eine Infrastruktur mit Institutionen, die die Schlüssel speichern, notwendig ist (Key-Escrow). Solche Institutionen sind ein potentieller Angriffspunkt, beispielsweise für kriminelle Organisationen, die an geheime Informationen gelangen wollen. Das Personal wäre beispielsweise vielfältigen Gefahren ausgesetzt. Um an die geheimen Schlüssel zu kommen, gibt es Einwirkungsmöglichkeiten wie Erpressung, Bestechung oder Spionage. Darüber hinaus ist für diese Handlungsalternative eine Vielzahl von Regularien erforderlich, die gewährleisten, daß nur im Rahmen zulässiger Überwachungsmaßnahmen auf die Schlüssel zugegriffen wird.

Überwachungsmaßnahmen sind für die Sicherheitsbehörden mit einem hohen finanziellen, technischen und personellen Aufwand verbunden. Jede von Bürgern und Institutionen eingesetzte Software muß geprüft und freigegeben werden. Gegenüber kriminellen Spionageversuchen oder neugierigen Lauschern besteht ein relativ hoher Schutz der Kommunikation, solange Software eingesetzt wird, die den Anforderungen an ein Key-Escrow-Verfahren genügt.

zu d)
Eine Überwachung der Telekommunikation durch die Sicherheitsbehörden wird in vielen Fällen nicht mehr möglich sein, da der Bürger das Fernmeldegeheimnis mit eigenen Mitteln schützen kann. Er hat selbst die Möglichkeit, sich durch den Einsatz geeigneter kryptographischer Verfahren gegen Abhören durch Dritte zu schützen. Es sollte rechtzeitig nach anderen geeigneten Mitteln zur Bekämpfung der Kriminalität gesucht werden.

Eine Reglementierung des Einsatzes von kryptographischen Verfahren würde nicht nur Telekommunikationsvorgänge betreffen, sondern auch die sichere Speicherung von Daten auf Datenträgern wie Festplatten, Magnetbändern und Disketten beeinflussen. Die nachfolgend genannten Aspekte sprechen gegen ein Verbot oder irgend eine Reglementierung der Verschlüsselung.

Der Schutz von Betriebs- und Geschäftsgeheimnissen ist oftmals nur durch den Einsatz von Verschlüsselungsverfahren möglich. Erfolgt eine Reglementierung kryptographischer Verfahren, ist nicht mehr sichergestellt, daß gesetzlich geschützte Privatgeheimnisse auf angemessene Weise gewahrt werden können.

Schon jetzt wird aus Gründen der Datensicherheit in vielen Bereichen die verschlüsselte Speicherung gefordert (beispielsweise zur Gewährleistung der Datensicherheit bei Diebstahl). Ein Verschlüsselungsverbot würde dazu führen, daß eine ausreichende Datensicherheit nicht mehr gewährleistet ist.

Für den Bereich der Speicherung ist eine individuelle Verschlüsselung mit einem beliebigen Verfahren leicht zu realisieren und kaum festzustellen. Eine zentrale Schlüsselverwaltung ist

dort nicht erforderlich. Da in diesen Fällen der Einsatz von Datenfernübertragungstechnik unterbleiben kann, muß die Einhaltung von Reglementierungen mit Hilfe von Hausdurchsuchungen und der Beschlagnahme von Datenträgern überwacht werden.

Beschlagnahmte verschlüsselte Datenträger werden in der Regel mit Wissen des Betroffenen gelesen. Somit ist es nicht erforderlich, daß Überwachungsbehörden vorher in den Besitz der Schlüssel gelangen. Es reicht aus, den Schlüssel während der Beschlagnahme vom Betroffenen zu fordern. Eine Reglementierung von Verschlüsselungsverfahren würde jedoch nicht automatisch dazu führen, daß diese Datenträger in jedem Fall gelesen werden können. Verweigert der Betroffene beispielsweise schon ohne Reglementierung die Preisgabe des Schlüssels, ist wohl kaum zu erwarten, daß er sich gegebenenfalls an Reglementierungsvorschriften hält. Vielmehr ist damit zu rechnen, daß er den Zugriff auf seine Daten durch die Nutzung nicht genehmigter Verfahren verhindern wird.

Auch für den Bereich der digitalen Signatur ist ein mögliches Kryptogesetz von Bedeutung, da die verwendeten Algorithmen in einigen Fällen prinzipiell geeignet sind, Daten zu verschlüsseln. Eine Reglementierung der Verschlüsselung darf in keinem Fall den Zugriff auf die geheimen Schlüssel zulassen, die zur digitalen Signatur vorgesehen sind. Nach geltendem Recht ist es nicht zulässig, solche Schlüssel als Kopien zu speichern, da dann die Möglichkeit besteht, Dokumente zu fälschen. Das Gesetz zur digitalen Signatur sieht ausdrücklich vor, daß Signaturschlüssel geheim gehalten werden (siehe auch Punkt 2.2). In § 5 Abs. 2 SigG heißt es dazu: „Die Zertifizierungsstelle hat ... Vorkehrungen zu treffen, um die Geheimhaltung der privaten Signaturschlüssel zu gewährleisten. Eine Speicherung privater Signaturschlüssel bei der Zertifizierungsstelle ist unzulässig. “

Kann nun in jedem der beschriebenen Fälle mit einer entsprechenden Kontrollinfrastruktur tatsächlich die Einhaltung von Reglementierungen überwacht werden? Im Rahmen der bis heute überschaubaren technischen Entwicklung ist das nicht der Fall. Vielmehr würde der reglementierte Einsatz von Verschlüsselungstechnik insbesondere kriminelle Organisationen hinsichtlich zu erwartender Abhörmaßnahmen sensibilisieren. Gerade diejenigen, die mit einer Überwa-

chung ihrer Kommunikation rechnen, werden einige der nachfolgend beschriebenen Gegenmaßnahmen treffen, um ein Abhören zu unterlaufen.

Codierte Informationen

Eine relativ einfache Möglichkeit, ohne großen technischen Aufwand Abhörmaßnahmen zu unterlaufen, wäre die Codierung der eigentlichen Nachrichten. Schon die Nutzung einer wenig gebräuchlichen Sprache würde ein Abhören wesentlich erschweren oder gar unmöglich machen, da entsprechende Dolmetscher möglicherweise nicht immer zur Verfügung stünden. Voraussetzung für diese Abwehrmaßnahme ist lediglich die vorherige Absprache der Teilnehmer, die zur Kommunikation zugelassen sind (geschlossene Benutzergruppe).

Überschlüsselung

Informationen werden mit einem nicht reglementierten Verfahren verschlüsselt, bevor sie mit einem zugelassenen Verfahren während der Übertragung oder vor der Speicherung ein zweites Mal verschlüsselt werden. Der Austausch der Schlüssel und die Mitteilung der Version des nicht reglementierten Verfahrens können zu einem beliebigen Zeitpunkt erfolgen. Eine geschlossene Benutzergruppe ist hier nicht notwendig.

Bei einer Überwachung würde erst zum Zeitpunkt der Entschlüsselung auffallen, daß ein nicht reglementiertes Verfahren „im Hintergrund“ genutzt wird. Die Nachrichteninhalte selbst blieben geheim.

Steganographie

Dieses Verfahren ermöglicht es, Informationen in digitalisierten Audio- oder Bildinformationen zu verstecken. Beispielsweise könnte parallel zur Übertragung einer Videokonferenz eine weitere versteckte Information übertragen werden, ohne daß der Betrachter der Videobilder erkennt, daß überhaupt eine zusätzliche Nachricht vorhanden ist. Zur Zeit verfügbare Programmversionen könnten Spuren hinterlassen, die auf den Einsatz des Verfahrens hindeuten. Es müßte aber ganz gezielt danach gesucht werden.

Bevor sie steganographische Verfahren nutzen, müssen sich die Kommunikationspartner hierzu abstimmen. Entsprechende Software ist beispielsweise im Internet verfügbar. Die Überwachung eines solchen Kommunikationsvorganges hätte keine Aussicht auf Erfolg.

Neben verfassungsrechtlichen Bedenken und technischen Einschränkungen spielen auch wirtschaftliche Aspekte eine wesentliche Rolle bei den Überlegungen zur Reglementierung von Verschlüsselungsverfahren. Der Aufbau und die Unterhaltung der erforderlichen Kontrollinfrastruktur wären mit einem erheblichen Kostenaufwand verbunden. So erfordert beispielsweise die Kontrolle von Kommunikationsvorgängen mit Hilfe eines Verfahrens, bei dem Schlüssel oder Schlüsselteile hinterlegt werden müssen (siehe oben Alternative c), die Konstruktion und den Betrieb von hochkomplexen Key-Escrow-Systemen. Insbesondere vor dem Hintergrund zunehmender grenzüberschreitender elektronischer Kommunikationsvorgänge ist damit zu rechnen, daß Schlüssel von vielen Millionen Nutzern hinterlegt werden müßten, die wiederum hunderte unterschiedliche Verschlüsselungsprodukte nutzen. Allein die Betriebskosten für solche Key-Escrow-Systeme, beispielsweise für sehr gut ausgebildetes und höchst vertrauenswürdiges Personal, werden gewaltig sein. Auch die Zertifizierung der zur Nutzung freigegebenen Software verursacht erhebliche Kosten. Es ist fraglich, ob derartige Kosten mit dem zu erwartenden geringen und eher zufälligen Erfolg zu rechtfertigen sind.

Im Ergebnis dieser Betrachtungen ist folgendes festzuhalten:

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 aus technischer Sicht so gut wie nicht kontrollierbar ist,

- 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.

Die Datenschutzbeauftragten des Bundes und der Länder haben im Rahmen ihrer Konferenzen in Form von Entschließungen

- empfohlen, zur Wahrung der Vertraulichkeit zu übertragende personenbezogene Daten zu verschlüsseln (siehe Zweiter Tätigkeitsbericht, 15. Anlage),
- gefordert, beim Transport von elektronisch gespeicherten personenbezogenen Daten geeignete, sichere kryptographische Verfahren zu verwenden (siehe 18. Anlage),
- sich dagegen gewandt, daß den Nutzern von Informations- und Telekommunikationstechnik verboten wird, den Inhalt ihrer Nachrichten zu verschlüsseln (siehe 6. Anlage).

2.4 Umsetzung der Datenschutzrichtlinie der Europäischen Union

Im Juli 1995 ist die EU-Datenschutzrichtlinie vom Rat der Europäischen Union (EU) angenommen und im Oktober 1995 von allen EU-Mitgliedstaaten unterzeichnet worden. Bis zum 24. Oktober 1998 muß sie von allen Beteiligten in nationales Recht umgesetzt werden. Im Zweiten Tätigkeitsbericht hatte ich unter Punkt 2.1 auf den sich damals abzeichnenden Änderungsbedarf im Bundes- und Landesrecht und auf die Bedeutung der Richtlinie für Mecklenburg-Vorpommern hingewiesen.

Die Datenschutzbeauftragten des Bundes und der Länder hatten auf ihrer 51. Konferenz im März 1996 eine Entschließung zur Umsetzung der EU-Datenschutzrichtlinie verabschiedet (siehe 1. Anlage) und die gesetzgebenden Körperschaften aufgefordert, die Richtlinie als ein Gebot zur umfassenden Fortentwicklung und Modernisierung des deutschen Datenschutzrechts zu sehen.

Im Februar 1997 hat das Bundesministerium des Innern (BMI) einen Referentenentwurf zur Änderung des Bundesdatenschutzgesetzes vorgestellt. Dieser Entwurf beschränkte sich auf die von der Richtlinie zwingend geforderten Änderungen und berücksichtigte die notwendigen Anpassungen an die technischen und gesellschaftlichen Entwicklungen nur unzureichend. Mittlerweile ist er mehrfach überarbeitet worden, hält aber im wesentlichen an der äußerst unbefriedigenden Minimallösung fest, wobei teilweise, wie etwa bei der Definition des Dateibegriffs, nicht einmal die Anforderungen der Richtlinie erfüllt werden.

Darüber hinaus ist der Stand des Verfahrens zu kritisieren. Seit über zwei Jahren ist die EU-Datenschutzrichtlinie in Kraft, aber noch immer existiert dazu kein Kabinettsbeschluß der Bundesregierung. Daher droht die Umsetzung der Richtlinie bis zum 24. Oktober 1998 zu scheitern. Wegen Verstoßes gegen europäisches Recht kann es deshalb zu einem Verfahren vor dem Europäischen Gerichtshof kommen. Vor allem hat dies aber neben möglichen finanziellen Sanktionen zur Folge, daß sich überfällige Verbesserungen des Datenschutzes noch weiter verzögern und den ebenso zur Umsetzung verpflichteten Bundesländern eine Orientierung zur Anpassung ihrer Landesdatenschutzgesetze fehlt. Die Datenschutzbeauftragten des Bundes und der Länder haben daher in einer weiteren Entschließung auf der 54. Konferenz im Oktober 1997 (siehe 13. Anlage) nachdrücklich auf diesen Mißstand aufmerksam gemacht und an die Bundesregierung appelliert, für eine fristgerechte Umsetzung der Richtlinie zu sorgen. Des weiteren haben sie detaillierte Empfehlungen für Grundsatzentscheidungen zur Harmonisierung des europäischen Datenschutzrechts sowie zur Anpassung der Vorschriften an die heutige Informationstechnologie und an die Verhältnisse der modernen Informationsgesellschaft gegeben.

Auch für das Land Mecklenburg-Vorpommern läuft die Frist zur Umsetzung der Richtlinie in Landesrecht am 24. Oktober 1998 ab. Da zur Novellierung des Bundesdatenschutzgesetzes immerhin schon ein Referentenentwurf vorliegt, sollte sich die Landesregierung verstärkt mit der Überarbeitung des Landesdatenschutzrechtes befassen. Zwar stellt der Entwurf aufgrund seines vorläufigen Status keine verbindliche und umfassende Hilfe für die landesrechtliche Anpassung an die Datenschutzrichtlinie dar, er bietet aber zumindest eine erste Orientierung. Ich bin jederzeit gern bereit, die Landesregierung bei dieser Arbeit beratend zu unterstützen. Darüber hinaus hätte eine Novellierung des Landesdatenschutzgesetzes schon aus anderen Grün-

den längst vorgenommen werden sollen. Ich verweise hierzu auf meine Novellierungsvorschläge in den ersten beiden Tätigkeitsberichten.

3 Sorgen der Bürger, Vorkommnisse, Beratungen, Kontrollen, Stellungnahmen

3.1 Rechtswesen

3.1.1 Entwurf eines Strafverfahrensänderungsgesetzes

Die Bundesregierung hat im Dezember 1996 den Entwurf eines Strafverfahrensänderungsgesetzes (StVÄG-E) vorgelegt. Ziel des Gesetzentwurfes ist im wesentlichen, die verfassungsrechtlich gebotenen bereichsspezifischen Rechtsgrundlagen zu schaffen für die in das Persönlichkeitsrecht eingreifende strafprozessuale Ermittlungstätigkeit, für die Verwendung personenbezogener Informationen aus einem Strafverfahren sowie für die Verarbeitung und Nutzung personenbezogener Daten in Dateien. Im Rahmen dieser Zielsetzung finden sich unter anderem Vorschriften zur Öffentlichkeitsfahndung, zur Zulässigkeit der Einsichtnahme Verfahrensbeteiligter und -unbeteiligter in Ermittlungs- und Strafakten und zu Auskünften aus letzteren. Weiter ist geregelt, unter welchen Voraussetzungen personenbezogene Daten, die im Rahmen der Strafverfolgung erhoben wurden, auch für die polizeiliche Gefahrenabwehr genutzt werden dürfen. Der Entwurf erfüllt aus datenschutzrechtlicher Sicht die Vorgaben des Bundesverfassungsgerichts im „Volkszählungsurteil“ nicht und bleibt überdies hinter den bereits erreichten Standards anderer bereichsspezifischer Regelungen und den allgemeinen Datenschutzgesetzen zurück. Dies gilt insbesondere auch für die zwischenzeitlich beschlossene Stellungnahme des Bundesrates zum Gesetzentwurf, die zusätzliche gravierende Verschlechterungen vorsieht.

Ich habe gegenüber unserem Justizministerium zu dem Entwurf detailliert Stellung genommen und gebeten, meine Bedenken bei dem weiteren Gesetzgebungsverfahren zu berücksichtigen und mich über dessen Fortgang zu informieren.

Da der Entwurf in der vorgelegten Fassung ebenso wie die Stellungnahme des Bundesrates bundesweit auf im wesentlichen gleichlautende datenschutzrechtliche Kritik stößt, haben die Datenschutzbeauftragten des Bundes und der Länder auf ihrer 53. Konferenz im April 1997 eine Entschließung zum StVÄG 1996 verabschiedet (siehe 11. Anlage). Hinsichtlich der einzelnen Kritikpunkte am Gesetzentwurf und der Stellungnahme des Bundesrates verweise ich auf den Text der Entschließung. Der Bundesminister der Justiz hat unterdessen mitgeteilt, daß

er grundsätzlich bestrebt sei, am Regierungsentwurf und den darin enthaltenen datenschutzrechtlichen Vorkehrungen festzuhalten.

Es bleibt nunmehr abzuwarten, ob und inwieweit den datenschutzrechtlichen Bedenken im weiteren Gesetzgebungsverfahren doch Rechnung getragen werden wird.

3.1.2 Länderübergreifendes staatsanwaltschaftliches Verfahrensregister

Mit dem Verbrechensbekämpfungsgesetz wurden 1994 Vorschriften zum länderübergreifenden staatsanwaltschaftlichen Verfahrensregister (§§ 474 bis 477 Strafprozeßordnung - StPO) eingeführt. Es soll den Strafverfolgungsbehörden den bundesweiten Zugriff auf personenbezogene Daten aus allen laufenden Ermittlungs- und Strafverfahren ermöglichen. Zu diesem Zweck teilen die Staatsanwaltschaften der Registerbehörde personenbezogene Daten der Beschuldigten und weitere für das jeweilige Verfahren notwendige Daten mit.

Im Jahr 1995 bestimmte das Bundesministerium der Justiz die näheren datenschutzrechtlichen Einzelheiten, wie die Art der zu verarbeitenden Daten, in einer Errichtungsanordnung (§ 476 Abs. 5 StPO). Datenschutzrechtlich bedenklich war insbesondere die neu eingeführte Berechtigung der Registerbehörde, an die auskunftsersuchende Strafverfolgungsbehörde personenbezogene Daten aus Ermittlungsverfahren zu übermitteln, die dort unter abweichenden, aber ähnlichen Personendaten gespeichert sind („Ähnlichen-Service“). Eine besondere Gefahr besteht darin, daß Daten von Dritten, die im Ermittlungsverfahren bei der auskunftsersuchenden Staatsanwaltschaft nicht Beschuldigte sind, diesem Verfahren zugeordnet und entsprechend gespeichert werden. Zu kritisieren sind auch die unzureichenden technischen und organisatorischen Maßnahmen zum Schutz der Daten.

Anfang 1996 wurden die in der Errichtungsanordnung geforderten organisatorisch-technischen Leitlinien im Entwurf ausgearbeitet. Dort sollten unter anderem Einzelheiten zur Kommunikation zwischen den anliefernden Behörden und der Registerbehörde sowie zum Datenschutz und zur Datensicherheit geregelt werden. Der Entwurf wurde mir von unserem Justizministerium übersandt. Ich habe im wesentlichen folgende Bedenken geäußert:

– Für Eilfälle war im Entwurf die Möglichkeit vorgesehen, durch besondere Kennzeichnung der Anfrage im automatisierten Auskunftsverfahren deren vorrangige Bearbeitung durch die Registerbehörde zu veranlassen. In Fällen, in denen wegen besonderer Eilbedürftigkeit auch dieses Verfahren nicht in Betracht kommt, wurde im Entwurf zusätzlich die Auskunft per Telex, Telefax oder Telefon zugelassen. Hier kann die Registerbehörde jedoch nicht sicher erkennen, ob die auskunftsersuchende Person tatsächlich zur Anfrage berechtigt ist. Es besteht die Gefahr, daß auf diese Weise unberechtigte Dritte Auskünfte aus dem Register erhalten. Ich habe daher vorgeschlagen, die Nutzung per Telefon oder Telefax nicht zuzulassen.

– Bei der ebenfalls im Entwurf vorgesehenen Sonderanfrage war der an die Registerbehörde zu übermittelnde Datensatz stark reduziert. Lediglich ein weiteres Identifizierungsmerkmal mußte neben dem Geburts- oder Familiennamen angegeben werden. Dadurch kann es zu Auskünften über mehr als eine Person kommen. Für eine derartige Gruppenauskunft fehlt jedoch eine gesetzliche Grundlage.

– Die notwendigen technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten waren auch in den organisatorisch-technischen Leitlinien nicht festgelegt.

Die Ausarbeitung der organisatorisch-technischen Leitlinien zur Errichtung des länderübergreifenden staatsanwaltschaftlichen Verfahrensregisters fand Mitte 1996 ihren Abschluß.

Das Register wird voraussichtlich Anfang 1999 in Betrieb genommen werden.

3.1.3 Öffentlichkeitsfahndung in Strafverfahren

Fahndungsmaßnahmen in der Öffentlichkeit greifen in das informationelle Selbstbestimmungsrecht der gesuchten Person ein. Einschränkungen dieses Grundrechts bedürfen jedoch einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen für den Betroffenen erkennbar ergeben.

Derzeit ist lediglich der Steckbrief als eine der möglichen Maßnahmen der Öffentlichkeitsfahndung in § 131 Strafprozeßordnung (StPO) ausdrücklich gesetzlich normiert. Ein Steckbrief ist eine Aufforderung an die Strafverfolgungsbehörden, insbesondere an die Polizei, nach einem flüchtigen oder sich verbergenden namentlich bekannten Beschuldigten zu fahnden und ihn festzunehmen. Voraussetzungen und Hilfsmittel der Fahndung nach anderen gesuchten Personen, zum Beispiel auch nach Zeugen, finden sich lediglich in der Verwaltungsvorschrift „Richtlinien für das Strafverfahren und das Bußgeldverfahren“ (RiStBV). Zur Regelung derartiger Einschränkungen des informationellen Selbstbestimmungsrechts sind jedoch gesetzliche Bestimmungen erforderlich. Eine Verwaltungsvorschrift ist dafür jedenfalls nicht ausreichend.

Dies gilt in besonderem Maße dann, wenn bei der Fahndung in der Öffentlichkeit die Medien eingeschaltet werden. Durch deren Reichweite, die Informationen in nahezu jeden bundesdeutschen Haushalt transportieren, wird in besonders starkem Maße in das Persönlichkeitsrecht der gesuchten Person eingegriffen. Geben die Strafverfolgungsbehörden personenbezogene Daten zu Zwecken der Fahndung an die Medien, handelt es sich aus datenschutzrechtlicher Sicht um eine Datenübermittlung. Hierfür existiert bisher keine Rechtsgrundlage. Dieser Themenkomplex ist gegenwärtig gleichfalls nur in Verwaltungsvorschriften wie „Richtlinien über die Inanspruchnahme von Publikationsorganen zur Fahndung nach Personen bei der Strafverfolgung“ (Anlage B zur RiStBV) und „Grundsätze für die bundesweite Ausstrahlung von Fahndungsmeldungen im Fernsehen“ geregelt.

In zunehmendem Maße wird das Internet als weltweites Medium der Öffentlichkeitsfahndung genutzt. Die Voraussetzungen für dessen Einsatz als Fahndungshilfsmittel bedürfen angesichts der Eingriffstiefe in das informationelle Selbstbestimmungsrecht der gesuchten Personen dringend einer Normierung durch den Gesetzgeber.

Die Datenschutzbeauftragten des Bundes und der Länder haben im März 1996 auf ihrer 51. Konferenz Grundsätze für die öffentliche Fahndung im Strafverfahren erarbeitet (siehe 3. Anlage) und diese als Empfehlung den zuständigen Justizressorts zugeleitet. Der Justizminister unseres Landes hat zwischenzeitlich zu den Grundsätzen Stellung genommen und mir mitgeteilt, daß er eine klarstellende Ergänzung der Verwaltungsvorschriften im Justizbereich durch die Grundsätze nicht für erforderlich hält.

Die Bundesregierung hat den verfassungsrechtlichen Vorgaben nunmehr teilweise Rechnung getragen und mit den neuen §§ 131 - 131 c des Entwurfes des Strafverfahrensänderungsgesetzes 1996 (StVÄG-E, siehe auch Punkt 3.1.1) bereichsspezifische Rechtsgrundlagen für die Fahndung in der Öffentlichkeit formuliert. Aus datenschutzrechtlicher Sicht bestehen jedoch erhebliche Zweifel an der Verfassungsmäßigkeit dieser Vorschriften. Diesen Bedenken haben die Datenschutzbeauftragten des Bundes und der Länder auf ihrer 53. Konferenz im April 1997 mit ihrer Entschließung Ausdruck verliehen (siehe 11. Anlage). Schwerpunkt der Kritik ist die mangelnde Bestimmtheit der normierten Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung, insbesondere die fehlende Differenzierung zwischen Beschuldigten und Zeugen. Auch die Stellungnahme des Bundesrates zum Gesetzentwurf ist aus datenschutzrechtlicher Sicht unbefriedigend (siehe Punkt 3.1.1).

Zu hoffen ist, daß die von den Datenschutzbeauftragten geäußerten Bedenken in den weiteren Beratungen des Bundestages und im Bundesrat ihren Niederschlag finden werden.

3.1.4 Täter-Opfer-Ausgleich

Im September 1996 hat mich das Justizministerium unseres Landes gebeten, zum Entwurf der „Richtlinien zur Durchführung des Täter-Opfer-Ausgleichs im Rahmen staatsanwaltschaftlicher und gerichtlicher Entscheidungen im Allgemeinen Strafrecht“ Stellung zu nehmen.

Für den Bereich der Gerichtshilfe ist eine Regelung auf gesetzlicher Ebene erforderlich. Im Rahmen der Prüfung eines möglichen Täter-Opfer-Ausgleichs und dessen anschließender Durchführung gehen die mit diesen Aufgaben Betrauten sowohl mit personenbezogenen Daten der Täter als auch der Opfer um. Dazu bedarf es entweder einer Einwilligung der Betroffenen oder einer normenklaren gesetzlichen Grundlage. Letztere ist jedoch weder im Strafgesetzbuch noch in der Strafprozeßordnung enthalten. Die gesetzlichen Regelungen über die (Erwachsenen-)Gerichtshilfe erschöpfen sich in bloßen Aufgabenzuweisungen beziehungsweise Organisationsentscheidungen (siehe § 160 Abs. 3 Satz 2 StPO, § 463 d StPO, Art. 294 e, g Strafgesetzbuch - StGB). Festzustellen bleibt, daß die verfahrensrechtliche Stellung der Gerichtshilfe vom Gesetzgeber nicht geregelt worden ist.

Die Einwilligung beim Täter-Opfer-Ausgleich war im Entwurf nur lückenhaft geregelt. Aus datenschutzrechtlicher Sicht war es notwendig, den pauschalen Hinweis auf § 7 DSG MV durch nähere Ausgestaltung der unterschiedlichen Formen des Umgangs mit personenbezogenen Daten zu konkretisieren. Ich habe daher vorgeschlagen, einen eigenständigen Unterpunkt zu formulieren, der sich ausschließlich mit datenschutzrechtlichen Aspekten auseinandersetzt. Dieser Unterpunkt sollte in folgende Abschnitte untergliedert werden:

- Datenerhebung,
- Speicherung, Veränderung und Nutzung der Daten,
- Datenübermittlung,
- Löschung, Anonymisierung und Sperrung der Daten,
- Auskunftsrechte für die Beteiligten,
- gesonderte Führung der beim Täter-Opfer-Ausgleich erstellten Akten,
- Rechtsfolgen einer Nichteinwilligung.

Das Justizministerium ist meinen Empfehlungen zur Gestaltung der Richtlinien gefolgt. Diese sind am 29. Juli 1997 in Kraft getreten. Sie sehen die Freiwilligkeit der Durchführung von Ausgleichsbemühungen für Täter und Opfer und die Erklärung des Einverständnisses zur Übermittlung von Daten an den Konfliktberater vor. Eine gesetzliche Regelung auf Landesebene wurde hingegen für nicht erforderlich gehalten. Richtiger Regelungsort sei vielmehr das Strafverfahrensänderungsgesetz 1996 (StVÄG).

Es bleibt abzuwarten, ob die Bundesregierung im Zuge ihrer Beratungen auf die gemeinsame Linie der Länder einlenkt und eine eindeutige Rechtsgrundlage zur Datenübermittlung bei der Durchführung des Täter-Opfer-Ausgleichs in das Gesetzeswerk einstellt.

3.1.5 Novellierung des Bundeszentralregistergesetzes

Im Bundeszentralregister (BZR) sind besonders sensible personenbezogene Daten gespeichert. In ihm werden unter anderem strafrechtliche Verurteilungen, Entscheidungen über Straferlaß, Freisprüche und Verfahrenseinstellungen wegen Schuldunfähigkeit sowie Ausweisungen und

Gewerbeuntersagungen vermerkt. Der Umgang mit diesen Daten ist in einem speziellen Gesetz geregelt, dem Bundeszentralregistergesetz (BZRG)

Es ist vorgesehen, dieses Gesetz zu novellieren. Der Referentenentwurf mit Stand vom 15. Februar 1997 enthält viele Regelungen, die einige der bisher bestehenden datenschutzrechtlichen Defizite beseitigen. Dies gilt insbesondere für

- die Streichung der Eintragungen ausländerrechtlicher Sachverhalte, welche schon im Ausländerzentralregister (AZR) gespeichert sind,

- das Erfordernis eines Sachverständigengutachtens für Eintragungen über Entscheidungen wegen Schuldunfähigkeit,

- die Einschränkung der Eintragungsfähigkeit staatsanwaltschaftlicher Verfügungen,

- die Pflicht zur Unterrichtung des Betroffenen über Eintragungen wegen Schuldunfähigkeit,

- die Berichtigungspflichtenund

- die Löschungspflichten bei Eintragungen wegen Schuldunfähigkeit.

Der Entwurf enthält aber auch Vorschriften, die datenschutzrechtlichen Belangen noch nicht in ausreichendem Maße Rechnung tragen, beispielsweise

- den Vorschlag des Bundesministeriums des Innern, Eintragungen den Nachrichtendiensten mitteilen zu können, auch wenn sie gesperrt sind, weil ihre Richtigkeit vom Betroffenen bestritten wird und die Richtigkeit/Unrichtigkeit noch nicht festgestellt werden konnte,

- die neue Vorschrift zur Zulässigkeit automatisierter Abrufverfahren, die irreführenderweise mit „Automatisiertes Auskunftsverfahren“ überschrieben ist und wesentliche Aussagen zu den Voraussetzungen und Teilnehmern automatisierter Abrufverfahren sowie zu den davon erfaßten Daten vermissen läßt,

– die Regelung zur Protokollierung der Auskünfte und Hinweise der Registerbehörde, welche nicht die vorgesehenen automatisierten Abrufe berücksichtigt, diesbezüglich also erheblich ergänzungsbedürftig ist, und welche die Verwendung der Protokolldaten nicht ausreichend bestimmt festlegt.

Ich habe dem Justizminister unseres Landes meine Bedenken mitgeteilt und ihn gebeten, meine Anregungen im Rahmen der anstehenden Beratungen zur Novellierung zu berücksichtigen.

Hinsichtlich der Eintragungen über die Schuldunfähigkeit im BZR habe ich empfohlen, bis zur Novellierung des BZRG die Pflichten zur Benachrichtigung des Betroffenen und zur Löschung nach einer festgelegten Zeit per Erlaß zu regeln. Im Juli 1996 ist ein entsprechender Erlaß ergangen.

3.1.6 Datenschutz bei Notaren

Solange keine notarspezifischen Datenschutznormen existieren, gilt für Notare unseres Landes das Landesdatenschutzgesetz von Mecklenburg-Vorpommern (DSG MV). Die Notarkammer Mecklenburg-Vorpommern hat unter meiner Mitarbeit ein Merkblatt zu den Pflichten der Notare nach diesem Gesetz sowie Muster für Dienstanweisungen, Verpflichtungserklärungen, Dateibeschreibungen und Geräteverzeichnisse erstellt, welche bei der Erfüllung der datenschutzrechtlichen Anforderungen hilfreich sein können.

Auch die Vorschriften des DSG MV, die die Kontroll- und Auskunftsrechte des Landesbeauftragten für den Datenschutz regeln, gelten für die Notare des Landes. Sie unterliegen ohne jede Einschränkung seiner Kontrollkompetenz. Insbesondere das Notargeheimnis kann ihm bei der Ausübung seiner nach dem DSG MV zustehenden Rechte nicht entgegengehalten werden.

Im zurückliegenden Berichtszeitraum hatte ich empfohlen, bereichsspezifische Datenschutzvorschriften für Notare zu schaffen (siehe Zweiter Tätigkeitsbericht, Punkt 2.2.6). Der mittlerweile dem Rechtsausschuß des Bundestages vorliegende Regierungsentwurf des Dritten Gesetzes zur Änderung der Bundesnotarordnung und anderer Gesetze enthält datenschutzrechtliche

Regelungen. Er stellt in einer Vorschrift zur Datenübermittlung aber immer noch darauf ab, daß die Daten für bestimmte Verfahrensschritte „von Bedeutung sein können“, anstatt das Kriterium der Erforderlichkeit zugrunde zu legen. Es ist zu hoffen, daß bald ein Änderungsgesetz verabschiedet wird, das durchgehend die Erforderlichkeit zur Aufgabenerfüllung als Maßstab für den Umgang mit personenbezogenen Daten normiert.

Anläßlich einer Eingabe hatte ich das Recht auf Grundbucheinsicht von Notaren zu untersuchen.

Jeder darf nur dann ein Grundbuch einsehen, wenn er ein berechtigtes Interesse daran hat. Zugunsten des Notars wird dieses Interesse gesetzlich vermutet. Die Vermutung gilt aber nur im Zusammenhang mit Amtsgeschäften. Bei Notaren gehen die Grundbuchämter allerdings zunächst davon aus, daß sie die Grundbucheinsicht für amtliche Zwecke begehren, und verlangen daher von ihnen im Regelfall keine Darlegung ihres berechtigten Interesses. Begehrt der Notar jedoch außerhalb seiner dienstlichen Tätigkeit Einsicht in ein Grundbuch, beispielsweise für den privaten Kauf eines Grundstücks, so muß er das Grundbuchamt auf den nicht-amtlichen Charakter seines Ersuchens hinweisen und ihm gegenüber - wie jeder andere Bürger auch - sein berechtigtes Interesse darlegen.

3.1.7 Das Elektronische Grundbuch

Im März 1997 war Pressemitteilungen zu entnehmen, daß in Mecklenburg-Vorpommern die Einführung eines maschinell geführten Grundbuches geplant sei. Auf meine Bitte hin erhielt ich aus dem Justizministerium die vollständigen Projektunterlagen und werde seitdem regelmäßig zu den datenschutzrechtlichen Fragen des Projektes konsultiert.

Bereits im November 1992 hatten die Justizminister der Länder vor dem Hintergrund der Schwächen des konventionellen Grundbuchsystems Rechtsänderungen gefordert, um das Grundbuch in elektronischer Form führen zu können. Mit dem Registerverfahrensbeschleunigungsgesetz wurden Ende 1993 die erforderlichen Rechtsgrundlagen geschaffen, damit bei der Führung des Grundbuches künftig weitgehend auf das Papier als Datenträger verzichtet werden kann. Weil damit unter anderem erreicht wird, daß der Datenbestand gleichzeitig an ver-

schiedenen Stellen beliebig oft zur Verfügung steht, erhoffen sich die Justizverwaltungen insbesondere bei der Grundbuchauskunft einen erheblichen Rationalisierungseffekt.

Bei der Realisierung des Elektronischen Grundbuches muß berücksichtigt werden, daß die Grundbuchordnung und die Grundbuchverfügung bereits viele Anforderungen stellen, deren softwaretechnische Umsetzung mit erheblichem finanziellen und personellen Aufwand verbunden sein wird. Beispielsweise sollen anerkannte automatisierte kryptographische Verfahren zur Erzeugung digitaler Signaturen und zum sicheren Datenaustausch sowohl innerhalb des Systems als auch mit externen Stellen angewandt werden. Das bedeutet unter anderem, daß eine vertrauenswürdige Stelle (Trustcenter) zur Verwaltung der Schlüssel zu installieren ist (siehe auch Punkt 2.3). Weiterhin muß sichergestellt sein, daß auch die elektronisch gespeicherten Daten auf Dauer inhaltlich unverändert in lesbarer Form wiedergegeben werden können. Es werden darüber hinaus Maßnahmen gegen unbefugtes Eindringen in das System sowie umfangreiche Protokollierungsmöglichkeiten gefordert. Dem Aspekt der „Zukunftsfähigkeit“ kommt eine Bedeutung zu, die mit den bisherigen Betrachtungen von Lebenszyklen einer Anwendungssoftware nicht mehr zu vergleichen ist.

In einer Planungsstudie zum Projekt Elektronisches Grundbuch hat die Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) als Mitentwickler einiger Komponenten des neuen Verfahrens erste Realisierungskonzepte dargestellt. Sie sehen vor, künftig das eigentliche Grundbuch, nicht jedoch die Grundakten, in elektronischer Form zu führen. Die Datenhaltung wird voraussichtlich zentral auf Rechnern des Justizministeriums, die im Hochsicherheitsbereich der DVZ M-V GmbH untergebracht sind, erfolgen. Der Zugriff auf die Datenbestände durch die verschiedenen Grundbuchämter zur Bearbeitung der einzelnen Grundbuchblätter ist über das Landesdatennetz LAVINE geplant. Dabei sollen die schon erwähnten kryptographischen Verfahren zur elektronischen Unterschrift und zur sicheren Übertragung der Daten auf öffentlichen Leitungen verwendet werden. Neben dem konventionellen Auskunftssystem ist ein automatisiertes Abrufverfahren vorgesehen. Zum Abruf zugelassene Stellen, beispielsweise Gerichte, Notare oder öffentlich bestellte Vermessungsingenieure, sollen durch Nutzung moderner Internet-Kommunikationsstrukturen auf der Basis von Standards des World Wide Web (WWW) Daten aus dem Elektronischen Grundbuch abrufen können. Eingeschränkte Abrufmöglichkeiten sollen unter anderem Personen oder Stellen erhalten, die beispielsweise die Zustimmung des Grundstückseigentümers besitzen oder die Zwangsvollstreckungen in die-

sem Bereich durchsetzen müssen. Ob bei den automatisierten Abrufen auf den Originaldatenbestand oder auf eine Auskunftskopie zugegriffen wird und welche Sicherheitsvorkehrungen erforderlich sind, ist noch nicht endgültig geklärt.

In meiner Stellungnahme zur Planungsstudie habe ich darauf hingewiesen, daß beim Elektronischen Grundbuch höchste Anforderungen an Verfügbarkeit und Integrität der Daten gestellt werden, die meines Erachtens nur wenige datenverarbeitende Stellen im Land erfüllen können. Für die Beauftragung kommen ohnehin nur staatliche Stellen oder juristische Personen des öffentlichen Rechts in Frage (§ 126 Abs. 3 Grundbuchordnung), so daß der Kreis der möglichen Auftragnehmer noch weiter eingeschränkt wird. Ich habe empfohlen, die Grundbuchauskunft durch ein automatisiertes Abrufverfahren ohne direkten Zugriff auf den Originaldatenbestand zu realisieren. Es könnte beispielsweise ein spezieller Auskunftsdatenbestand zum Abruf bereitgestellt werden, der regelmäßig aktualisiert wird. Im Hinblick auf die Protokollierung habe ich verdeutlicht, daß jederzeit die Überprüfung der Zulässigkeit von automatisierten Abrufen möglich sein muß und hierzu die zunächst vorgesehene Stichprobenkontrolle nicht geeignet ist. Ich habe deshalb empfohlen, die automatisierten Datenabrufe vollständig zu protokollieren.

Erste Gespräche mit der Justizverwaltung haben bereits stattgefunden. Es zeichnet sich eine konstruktive Zusammenarbeit ab. Unter anderem ist vorgesehen, in Arbeitsgruppen die erforderlichen Randbedingungen zum Einsatz kryptographischer Verfahren und zum Betrieb von Trustcentern zu definieren.

Die Einführung des Elektronischen Grundbuches ist für den Datenschutz in Mecklenburg-Vorpommern auch deshalb von besonderer Bedeutung, weil hier erstmalig in einem Verfahren von landesweiter Bedeutung kryptographische Verfahren zur Realisierung digitaler Signaturen vorgesehen sind.

3.1.8 Auskunftsrecht bei Staatsanwaltschaften

Die Staatsanwaltschaft stellte ein Ermittlungsverfahren gegen einen Bürger wegen Geringfügigkeit ein und teilte ihm dies mit. Der Betroffene trat an mich heran und bemängelte, daß er

im Verfahren nicht angehört wurde. Ferner wollte er Auskunft zu den sonst noch gegen seine Person geführten Ermittlungsverfahrenbei der Staatsanwaltschaft erhalten.

Dem Beschuldigten ist im strafrechtlichen Ermittlungsverfahren grundsätzlich Gelegenheit zu geben, sich zu den gegen ihn gerichteten Verdachtsgründen zu äußern. Bei Verfahrenseinstellungen kann hiervon abgesehen werden. Insofern war das Vorgehen der Staatsanwaltschaft zulässig.

Dieser Fall zeigt aber auch, daß eine solche Verfahrensweise dazu führen kann, daß der Betroffene erst durch die Einstellungsverfügung der Staatsanwaltschaft von einem gegen ihn durchgeführten Ermittlungsverfahren Kenntnis erlangt. Er hat damit keine Möglichkeit, in das laufende Verfahren einzugreifen, und weiß nicht, welche Daten über ihn erhoben und gespeichert wurden. Darüber hinaus gibt es auch Fälle, in denen der Betroffene über eine Einstellung des Ermittlungsverfahrens nicht informiert wird. Zwar ist nach § 170 Abs. 2 Strafprozeßordnung (StPO) eine Benachrichtigung des Betroffenen vorgeschrieben, wenn er im Verfahren beteiligt war, beispielsweise im Rahmen einer Beschuldigtenvernehmung, eine generelle Mitteilungspflicht besteht jedoch nicht. Es kann deshalb nicht ausgeschlossen werden, daß der Betroffene nicht erfährt, daß ein Ermittlungsverfahren gegen ihn durchgeführt wurde und daß über ihn Daten bei der Staatsanwaltschaft gespeichert werden.

Nach Abschluß von staatsanwaltschaftlichen Ermittlungsverfahren besteht nach allgemeinem Datenschutzrecht grundsätzlich ein Auskunftsanspruch. Mit dem Recht auf informationelle Selbstbestimmung wäre es nicht vereinbar, daß der Betroffene nicht weiß, wer was wann und bei welcher Gelegenheit über ihn speichert (Entscheidungen des Bundesvefassungsgerichts Band 65, Seite 43 - BVerfGE 65, 43).

Unser Justizministerium äußerte Bedenken gegen diesen Auskunftsanspruch und die Anwendbarkeit des Landesdatenschutzgesetzes für diesen Bereich. Ich teile diese Bedenken nicht, denn ein Anspruch auf Auskunft steht dem Interesse an einer effektiven Strafverfolgung im Rahmen der rechtsstaatlichen Grundsätze von Strafgesetzbuch und Strafprozeßordnung nicht entgegen. Bei Auskünften nach Abschluß des Ermittlungsverfahrens handelt es sich um Verwaltungsangelegenheiten, so daß mangels bereichsspezifischer Vorschriften § 20 DSG MV anwendbar ist. Hiernach steht dem Betroffenen grundsätzlich ein Auskunftsanspruch über die zu seiner Person

gespeicherten Daten, die Herkunft der Daten, etwaige Empfänger und den Zweck der Speicherung zu. Darüber hinaus werden in dieser Regelung Fallkonstellationen genannt, in denen Ausnahmen von diesem Grundsatz zulässig sind, beispielsweise bei einer Gefährdung der Aufgabenerfüllung der auskunftgebenden Stelle. Der Gesetzgeber war sich bewußt, daß der Auskunftsanspruch nicht absolut sein kann, sondern in bestimmten Fällen im überwiegenden öffentlichen Interesse eingeschränkt werden muß. Dadurch wird auch dem Interesse an einer effektiven Strafverfolgung hinreichend Rechnung getragen.

Das Justizministerium unseres Landes hat auf § 492 des aktuellen Entwurfes des Bundesrates zum Strafverfahrensänderungsgesetz 1996 (Bundesrats-Drucksache BR-Drs. 961/96) hingewiesen, in dem ein Auskunftsrecht für Betroffene vorgesehen ist, und hält derzeit zumindest eine Auskunftserteilung im Einzelfall für möglich.

Auf der Basis der Mitteilung des Justizministeriums konnte ich dem Petenten im vorliegenden Fall die ihn betreffenden Daten übermitteln. Darüber hinaus habe ich ihm empfohlen, ein entsprechendes Auskunftsersuchen an die Staatsanwaltschaft zu richten.

3.2 Polizei

3.2.1 Europäisches Polizeiamt (EUROPOL)

In Punkt 2.3.1 meines Zweiten Tätigkeitsberichtes hatte ich mich zu EUROPOL geäußert und die Bedenken der Datenschutzbeauftragten gegen das am 26. Juli 1995 von den Mitgliedstaaten der Europäischen Union unterzeichnete Übereinkommen über die Errichtung eines europäischen Polizeiamtes (EUROPOL-Konvention) dargelegt. Das Übereinkommen befindet sich nunmehr im Ratifizierungsverfahren. EUROPOL soll über ein europaweit arbeitendes, automatisiert geführtes Informationssystem verfügen, in dem alle beteiligten Länder Daten eingeben und abrufen können. Zum Zwecke der Verhütung, Bekämpfung oder Analyse von Straftaten sollen sogenannte Analysedateien errichtet werden. Danach können bei EUROPOL nicht nur tatverdächtige, sondern ebenfalls Personen gespeichert werden, von denen angenommen wird, daß sie eine Straftat begehen werden. Es wird hinsichtlich des Umfangs der Datenerhebung wenig differenziert zwischen Tatverdächtigen einerseits sowie Zeugen, Hinweisgebern, Opfern, Kontakt- und Begleitpersonen oder sonstigen Informanten andererseits. Darüber hinaus sollten in den Analysedateien beispielsweise auch Charaktermerkmale, DNA-

Profile (Profile über Erbinformationen) oder sexuelle Gewohnheiten gespeichert werden. Nach den Polizeigesetzen der Bundesländer ist eine Speicherung derartiger Daten nicht zulässig. Die Datenschutzbeauftragten des Bundes und der Länder haben daher auf ihrer 53. Konferenz im April 1997 eine Forderung des Europäischen Parlaments unterstützt (siehe 10. Anlage), nach der „alle Informationen persönlichen Charakters, wie Angaben zur Religionszugehörigkeit, philosophischen oder religiösen Überzeugungen, Rasse, Gesundheit und sexuellen Gewohnheiten von der Erfassung in Datenbanken in EUROPOL auszuschließen“ sind.

Ein weiteres offenes Problem bei EUROPOL ist die Durchsetzung der Rechte Betroffener. Angesichts des europaweiten Zugriffs auf Daten ist für den Bürger nicht mehr überschaubar, was EUROPOL zu seiner Person gespeichert hat und wohin diese Daten übermittelt werden.

Trotz zahlreicher Bedenken der Datenschutzbeauftragten hat der Bundesrat dem bereits vom Bundestag verabschiedeten „EUROPOL-Gesetz“ zugestimmt. Offene Punkte bei EUROPOL sind auch nach der Verabschiedung des Gesetzes die Immunität von EUROPOL-Bediensteten, die fehlende fachliche beziehungsweise parlamentarische Kontrolle von EUROPOL und die rechtliche Ausgestaltung der Übermittlung von Informationen an Drittstaaten und Drittstellen. Zur Übermittlung von Informationen an Drittstaaten und Drittstellen finden zur Zeit Beratungen in der Gruppe EUROPOL statt, die demnächst abgeschlossen werden sollen.

3.2.2 Änderung des Sicherheits- und Ordnungsgesetzes

Der vorliegende Gesetzentwurf enthält gegenüber dem noch gültigen Sicherheits- und Ordnungsgesetz (SOG MV) eine recht erhebliche Ausweitung polizeilicher Befugnisse. Im wesentlichen handelt es sich hierbei um

- die Einführung von ereignis- und verdachtsunabhängigen Kontrollen im Grenzgebiet,
- die Erweiterung des Großen Lauschangriffs in Wohnungen über die Abwehr einer allgemeinen Gefahr oder einer Lebensgefahr für einzelne Personen hinaus,
- den erweiterten Einsatz von verdeckten Ermittlern und
- den Direktverkehr mit ausländischen Polizeidienststellen.

In meiner Stellungnahme gegenüber dem Innenministerium unseres Landes und anläßlich der Anhörung vor dem Rechts- und Innenausschuß bin ich auf die datenschutzrechtlichen Aspekte der geplanten Erweiterungen im einzelnen eingegangen.

Zu den ereignis- und verdachtsunabhängigen Kontrollen

Bei der vorliegenden Gesetzesformulierung werden weder Tatsachen noch tatsächliche Anhaltspunkte für die Annahme gefordert, daß die kontrollierte Person irgend etwas mit grenzüberschreitender Kriminalität zu tun haben könnte. Jeder Bürger müßte damit rechnen, „im Grenzgebiet bis zu einer Tiefe von 30 km“ und auf „Durchgangsstraßen“, in „öffentlichen Einrichtungen des internationalen Verkehrs“ oder im „Küstenmeer“ einer Identitätsfeststellung durch die Polizei unterzogen zu werden. Bei der Feststellung der Identität durch die Polizei handelt es sich keineswegs um einen geringfügigen Eingriff in das informationelle Selbstbestimmungsrecht. Die Befugnis zu derart weitgehenden Personenkontrollen würde faktisch dazu führen, daß die Polizei sehr viel mehr Personenkontrollen ohne Anlaß als bisher vornehmen könnte.

Schon nach geltendem Recht darf die Polizei unter bestimmten Voraussetzungen Personen anhalten und sie zur Dienststelle mitnehmen, wenn die Identität auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden kann. Dabei können die betroffene Person sowie die von ihr mitgeführten Sachen zum Zwecke der Identitätsfeststellung durchsucht werden. Die Polizei kann die kontrollierte Person mit Hilfe elektronischer Datenverarbeitungssysteme überprüfen und durch Eingabe der Personalien zum Beispiel feststellen, ob die betreffende Person in ein strafrechtliches Ermittlungsverfahren involviert war oder ob sie zur Fahndung ausgeschrieben ist.

Würde die vorgesehene Regelung von verdachtsunabhängigen Kontrollen Gesetz, so ist damit zu rechnen, daß eine Vielzahl von Bürgern ohne jeden Anlaß in das Visier polizeilicher Maßnahmen gerät. Und das wären nicht nur Personen, die verdächtig sind, im Bereich von Kfz-Verschiebung, Rauschgifthandel oder Schlepperunwesen tätig zu sein.

Erklärte Absicht ist, die (organisierte) Kriminalität im Grenzgebiet zu bekämpfen. In der Begründung zum Gesetzentwurf heißt es an dieser Stelle, die an Osteuropa unmittelbar angren-

zenden Regionen seien zu einem bevorzugten Operationsfeld für ost- und westeuropäische Banden geworden. Ob bei der Bekämpfung dieser Art von Kriminalität jedoch eine „flächendeckende“ Personenkontrolle sinnvoll und verhältnismäßig ist, erscheint fraglich. Besser wäre es gewesen, zunächst einmal konkrete Zahlen vorzulegen, wie sich die Entwicklung von sogenannter grenzüberschreitender Kriminalität - nach Delikten aufgeschlüsselt - seit dem Inkrafttreten des Schengener Durchführungsübereinkommens darstellt. Aus anderen Bundesländern ist bekannt, daß die im Zusammenhang mit dem Abbau von Grenzkontrollen gehegten Befürchtungen nicht eingetreten sind.

Werden die verdachtsunabhängigen Kontrollen geltendes Recht, würde die Unterscheidung des Polizeirechts zwischen Störer und Nichtstörer aufgegeben, nach der die Polizei gegen Nichtstörer nur ausnahmsweise bei Vorliegen der Voraussetzungen des polizeilichen Notstandes vorgehen darf.

Zur Erweiterung des Großen Lauschangriffs in Wohnungen über die Abwehr einer allgemeinen Gefahr oder einer Lebensgefahr für einzelne Personen hinaus

Als besonders gravierend erachte ich die Ausweitung des sogenannten Großen Lauschangriffs im präventiven Bereich. Die vorgeschlagene gesetzliche Regelung läßt zu, daß bereits zur vorbeugenden Bekämpfung von Verbrechen und bei bestimmten Vergehen die Möglichkeit besteht, in Wohnungen technische Mittel zur Datenerhebung einzusetzen. Und das soll keineswegs nur bei Personen geschehen, bei denen Tatsachen die Annahme rechtfertigen, daß sie mit hinreichender Wahrscheinlichkeit in näherer Zeit solche Straftaten begehen wollen, sondern auch bei anderen Personen, soweit beispielsweise der Verantwortliche für eine Gefahr nicht oder nicht rechtzeitig erreicht werden kann oder die Maßnahmen direkt gegen ihn keinen Erfolg versprechen. Diese beiden Alternativen dürften in der Praxis relativ häufig vorkommen. Daher ist es besonders bedenklich, wenn die Polizei schon dann die Möglichkeit hat, in der Wohnung eines anderen technische Mittel einzusetzen, wenn nach ihrer Einschätzung der Lauschangriff auf die Wohnung des Störers selbst keine Aussicht auf Erfolg verspricht. Insgesamt gesehen wird dadurch die Schwelle, auch in Wohnungen „anderer Personen“ einen Lauschangriff durchzuführen, in tatsächlicher Hinsicht erheblich gesenkt. Würde diese Regelung geltendes Recht, verliert der rechtsstaatliche Grundsatz, daß der gesetzestreue Bürger das Recht hat, „vom Staat in Ruhe gelassen zu werden“, seine Bedeutung. Dem einzelnen muß um der freien

und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen aber ein „Innenraum“ verbleiben, in dem er „sich selbst besitzt und in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem er in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt“ (BVerfGE 27, 1 ff.).

Neu ist auch die ausdrückliche Regelung hinsichtlich der durch Amts- und Berufsgeheimnisse geschützten Vertrauensverhältnisse. Auch hier soll unter bestimmten Voraussetzungen gelauscht werden dürfen.

Die Verfassung Mecklenburg-Vorpommern (Art. 24 Abs. 3) und das Grundgesetz der Bundesrepublik Deutschland (Art. 4, 5 Abs. 1, Art. 12, 47) schützen durch Grundrechte und institutionelle Gewährleistung eine Vielzahl von Vertrauensverhältnissen, beispielsweise zwischen Arzt und Patient oder Anwalt und Mandant, deren Funktionsfähigkeit durch Amts- und Berufsgeheimnisse gewahrt werden und für die einfachgesetzliche Vorkehrungen getroffen wurden (zum Beispiel §§ 53, 53a, 97 StPO, § 43 a BRAO, § 35 SGB I, § 203 StGB). Nach dem Urteil des Sächsischen Verfassungsgerichtshofes vom 14. Mai 1996 (Vf. 44 - II - 94, S. 65 ff.) bedarf die polizeiliche Datenverarbeitung aus verfassungsrechtlich geschützten Vertrauensverhältnissen einer gesetzlichen Grundlage, die mit hinreichender Bestimmtheit die konkurrierenden verfassungsrechtlichen Rechtspositionen zum Ausgleich bringt. Eine solche Regelung existiert in Mecklenburg-Vorpommern bisher nicht, so daß Eingriffe in verfassungsrechtlich geschützte Vertrauensverhältnisse nach geltendem Recht nicht zulässig sind. Im Ergebnis wird somit erst durch die geplante Regelung eine entsprechende Befugnisnorm geschaffen. Hier von einer Schutzmaßnahme zu sprechen, wie dies in der Gesetzesbegründung erläutert wird, halte ich für verfehlt. Ungeachtet dessen ist zu beachten, daß Eingriffe für Zwecke der Gefahrenvorsorge bei Vertrauensverhältnissen nur in Betracht kommen können, „wenn sie das einzige Mittel zur Informationsgewinnung darstellen“ (siehe Urteil des Sächsischen Verfassungsgerichtshofs a. a. O. S. 65 ff.). Insofern ist auch diese Gesetzesänderung aus datenschutzrechtlicher Sicht kritikwürdig.

Aus den vorstehenden Gründen habe ich daher empfohlen, für diesen Bereich die bisherige Gesetzesregelung beizubehalten.

Zum erweiterten Einsatz von verdeckten Ermittlem

Nach dem vorliegenden Gesetzentwurf sollen die Voraussetzungen für Observationen, den Einsatz technischer Mittel sowie von verdeckten Ermittlern und V-Leuten erheblich gelockert werden. Nach der bisherigen Regelung konnten besondere Mittel der Datenerhebung lediglich als letzte Möglichkeit der Informationsbeschaffung angewandt werden.

Angesichts der einschneidenden Eingriffe in das Recht auf informationelle Selbstbestimmung bei verdeckten Datenerhebungen halte ich auf jeden Fall weitere grundrechtsichernde Verfahrensregelungen für erforderlich. Ich hatte daher eine gesetzlich zu regelnde Berichtspflicht der Landesregierung gegenüber dem Landtag empfohlen, die sich auf alle „besonderen Mittel der Datenerhebung“ bezieht. Derartige Berichtspflichten sehen derzeit das Niedersächsische Gefahrenabwehrgesetz und das Brandenburgische Polizeigesetz vor. Erst wenn Fakten zur Verfügung stehen, kann der Gesetzgeber im Rahmen der Verhältnismäßigkeitsprüfung abwägen, ob die gravierenden Einschnitte in die Persönlichkeits- und Freiheitsrechte der Bürger hingenommen werden sollten.

Zum Direktverkehr mit ausländischen Polizeidienststellen

Datenübermittlungen an bestimmte ausländische Polizeibehörden sollen künftig im Rahmen der Zusammenarbeit im Grenzgebiet sowie der internationalen polizeilichen Zusammenarbeit zulässig sein, soweit dies erforderlich ist. Auf die Abwehr einer im Einzelfall bevorstehenden Gefahr, so wie dies nach geltendem Polizeirecht der Fall ist, wird dabei nicht mehr abgestellt.

Kritisch sehe ich die Datenübermittlung unter dem Aspekt des offensichtlich bestehenden unterschiedlichen Datenschutzniveaus, insbesondere bei osteuropäischen Staaten. In einem Land, in dem der Datenschutz nicht in etwa dem Standard des bei uns geltenden Rechts entspricht und verfassungsmäßig abgesichert ist, bestehen auch keine rechtlichen Möglichkeiten, ein Unterlaufen der entsprechenden Vorschriften zu unterbinden. Soweit keine adäquaten Bestimmungen existieren, soll durch eine Zusage sichergestellt werden, daß die ausländischen Polizeidienststellen unser geltendes Datenschutzrecht beachten. In der Gesetzesbegründung wird auf diese Zusage als Hilfsmittel hingewiesen. Es bestehen erhebliche Zweifel, inwieweit derartige Zusagen ausreichen, um den entsprechenden Schutzstandard zu gewährleisten, und ob es nicht hierzu unter Umständen sogar völkerrechtlicher Vereinbarungen bedarf. Daher sollten,

soweit keine vergleichbare rechtsstaatliche Verankerung des Grundrechts auf informationelle Selbstbestimmung im Ausland vorgesehen ist, Festlegungen und Sicherungsvorkehrungen in einem Regierungsabkommen anstelle von Zusagen angestrebt werden.

Die Einrichtung eines Datenverbundes sowie eines automatisierten Abrufverfahrens über Landesgrenzen hinweg ist daher als äußerst kritisch anzusehen. Dabei sind auch die mit dem Einsatz von Verfahren der automatisierten Datenverarbeitung einhergehenden Gefährdungen zu berücksichtigen. Erhebliche Bedenken bestehen insbesondere gegen die Ermächtigung für die Einrichtung eines automatisierten Abrufverfahrens. Die abrufende Stelle hat grundsätzlich die Möglichkeit, über die bei der speichernden Stelle zum Abruf bereitgehaltenen Daten zu verfügen. Diese Verfügungsgewalt durch Dritte birgt naturgemäß Risiken und Gefahren in sich. Daher ist die Einrichtung automatisierter Abrufverfahren nicht schon dann zulässig, wenn sie an die Stelle der bisherigen konventionellen Auskunftsverfahren treten. Vielmehr ist unter den Aspekten der zusätzlichen Gefährdung sowie unter Beachtung des Verhältnismäßigkeitsgrundsatzes der Nachweis zu erbringen, daß ein solches Verfahren tatsächlich erforderlich ist und geeignete technische und organisatorische Maßnahmen getroffen werden, den bestehenden Gefährdungen wirksam zu begegnen. Dieser Nachweis wurde bisher nicht geführt. Ebenso bleibt ungeklärt, ob für einen Datenverbund beziehungsweise ein automatisiertes Abrufverfahren über die Grenzen der Bundesrepublik Deutschland hinaus überhaupt eine Regelung im SOG MV ausreichend ist. Die entsprechenden Gesetzesänderungen sollten aus den oben genannten Gründen ganz entfallen.

Zur Zeit wird die Gesetzesnovellierung noch in den zuständigen Ausschüssen des Landtages behandelt. Etwaige Änderungsanträge aus den Fraktionen waren bei Redaktionsschluß noch nicht bekannt.

3.2.3 Großer Lauschangriff

Am 6. März 1996 hat der Landtag mit den Stimmen der Fraktionen der CDU und der SPD einen Antrag (Drucksache 2/1274) angenommen, mit dem die Landesregierung aufgefordert wurde, Initiativen im Bundesrat zur Einführung des Großen Lauschangriffes zu unterstützen,

um so den besonderen Bedrohungen durch die organisierte Kriminalität und das organisierte Verbrechen entgegenzuwirken.

Der Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich im Oktober 1996 mit einem Schreiben an den Vorsitzenden der Ministerpräsidentenkonferenz gewandt und noch einmal deutlich auf die besondere Eingriffstiefe des Großen Lauschangriffes in das Grundrecht auf informationelle Selbstbestimmung hingewiesen. Die Mehrheit der Datenschutzbeauftragten lehnt den Großen Lauschangriff zum Zwecke der Strafverfolgung weiterhin ab. Für den Fall, daß ungeachtet der nach wie vor bestehenden Bedenken die Pläne zur Einführung des Großen Lauschangriffes weiterverfolgt werden, hatte die Konferenz der Datenschutzbeauftragten klare Begrenzungen und verfahrenssichernde Maßnahmen gefordert, um den Schutz der Privatsphäre zumindest teilweise zu gewährleisten. Die wesentlichen Punkte müßten dann bereits in der Verfassung verankert werden.

Sollten die auf Basis eines Kompromisses von SPD und Regierungskoalition zur Zeit diskutierten Gesetzentwürfe - Entwurf eines Gesetzes zur Änderung des Grundgesetzes (Artikel 13 GG - BT-Drs. 13/8650) und Entwurf eines Gesetzes zur Verbesserung der Bekämpfung der Organisierten Kriminalität (BT-Drs. 13/8651) - vom Bundestag und Bundesrat beschlossen werden, wäre damit auch der letzte bisher unantastbare Bereich privater Lebensgestaltung in den Bereich staatlicher Überwachung einbezogen.

Die Überwachung ist nach den vorliegenden Gesetzentwürfen nicht, wie immer wieder gern von Befürwortern des Großen Lauschangriffes betont wird, auf „Gangsterwohnungen“ beschränkt. Vielmehr kann dieses Mittel auch in Wohnungen anderer Personen zum Einsatz kommen, in denen sich der Beschuldigte vermutlich aufhält. Dies ist unabhängig davon, in welcher Beziehung der Wohnungsinhaber zum Beschuldigten steht. Bereits im Ansatz ist es nicht gelungen, unter Beachtung des Verhältnismäßigkeitsgrundsatzes eine hinreichende Beschränkung dieser mit höchster Eingriffsintensität verbundenen Maßnahme vorzunehmen. Zielrichtung soll eine wirksamere Bekämpfung der organisierten Kriminalität sein. Der Straftatenkatalog ist beispielsweise jedoch nicht nur auf Verbrechen beschränkt, sondern erfaßt auch Vergehen. Bedenken habe ich auch hinsichtlich der Tatsache, daß für einen derart schwerwiegenden Eingriff ein einfacher Tatverdacht genügt und nicht auf das Vorliegen eines dringenden Tatverdachtes abgestellt wird. Die neuerlich geführten Diskussionen zeigen längst, daß durch diese

Maßnahme zwangsläufig auch Unbeteiligte in das Visier der Ermittler geraten und massive Eingriffe in die Privatsphäre hinzunehmen haben. Der Lauschangriff macht auch nicht vor den besonders geschützten Vertrauensverhältnissen zwischen Betroffenen und Ärzten, Priestern, Anwälten sowie Journalisten halt. Ein wirksamer Schutz oder entsprechende Sicherungsmaßnahmen, etwa ausreichende Verwertungsbeschränkungen, sind bisher noch nicht vorgesehen. Trotz der zahlreichen Bedenken der breiten Fachöffentlichkeit beinhalten die Entwürfe nur unzureichende Berichtspflichten, die keinesfalls ausreichen, fundierte Aussagen über die Erforderlichkeit einzelner Maßnahmen und deren Auswirkungen auf die Betroffenen zu erhalten. Zur Notwendigkeit eines qualifizierten Berichtswesen als objektives Instrument zur Bewertung polizeilicher Befugnisse hatte ich mich bereits in meinem Zweiten Tätigkeitsbericht (siehe Punkt 2.3.3) geäußert. Der Gesetzgeber ist gehalten, sich ein objektives Bild über die Auswirkungen neuer Eingriffsinstrumente zu verschaffen, um gegebenenfalls bei der Gesetzgebung nicht voraussehbare Schieflagen bei Eingriffen in das Persönlichkeitsrecht Betroffener zu korrigieren.

Die vorgesehene Einschränkung des Grundrechtes der Unverletzlichkeit der Wohnung (Artikel 13 GG) und die damit verbundene Entscheidung für den Großen Lauschangriff ist mit dem Verlust eines wesentlichen Teils individueller Freiheit verbunden. Damit verbleibt dem einzelnen kein geschützter „Innenraum“ mehr, in den er sich unbeobachtet zurückziehen kann.

Gegenwärtig wird in die politische Auseinandersetzung um den Großen Lauschangriff die Forderung eingebracht, Gespräche mit Seelsorgern, Ärzten und Anwälten nicht abzuhören. Auch wenn es relativ spät geschieht, so ist es doch sehr zu begrüßen, daß eine Gruppe Abgeordneter die Unverletzlichkeit des Beichtgeheimnisses und die Wahrung bestimmter Berufsgeheimnisse nunmehr nicht ohne weiteres einer aus mehreren Gründen und im Prinzip immer fragwürdig bleibenden polizeilichen Maßnahme opfern will. Wichtig erscheint mir, bei der weiteren Auseinandersetzung daran zu denken, daß Beichten und andere seelsorgerische Gespräche nicht nur in Beichtstühlen geführt werden, sondern beispielsweise auch in Beichtzimmern, Krankenhäusern und privaten Wohnungen. Eine saubere gesetzliche Regelung ist unter Beachtung dieser Tatsache nahezu ausgeschlossen, da niemand vorher wissen kann, wann ein Seelsorger zu einem Gespräch in welche private Wohnung bestellt worden ist. Wenn es zufällig die Wohnung sein sollte, die vorher mit großem zeitlichen, personellen und technischen Aufwand zum Abhören präpariert wurde, dann waren diese Maßnahmen umsonst oder das Beichtgeheimnis wird in

Frage gestellt. Denkbar wären auch verschiedene Formen des Mißbrauchs der seelsorgerischen Tätigkeit für kriminelle Zwecke, ohne daß sich der Seelsorger dessen bewußt ist. Eine vernünftige gesetzliche Normierung des Großen Lauschangriffs scheint mir unter Berücksichtigung dieser Aspekte nahezu ausgeschlossen. Wenn das Abhören von Wohnungen beschlossen werden sollte, dann ist auch die Wahrung des Beichtgeheimnisses prinzipiell nicht mehr sicherzustellen. Aber nicht nur deshalb sollte der Gesetzgeber generell auf das Abhören von Beichtstühlen, Arztpraxen, Anwaltskanzleien und privaten Wohnungen zum Zwecke der Strafverfolgung verzichten, sondern vor allem deshalb, weil jedem Bürger ein privates Refugium verbleiben muß, das der staatlichen Ausforschung entzogen ist.

Nach wie vor halte ich die mit dem Großen Lauschangriff einhergehenden Eingriffe in das Persönlichkeitsrecht für zu weitgehend und nicht gerechtfertigt. Dazu habe ich mich bereits mehrfach geäußert (Erster Tätigkeitsbericht, Punkte 2.4.1 und 2.21.5; Zweiter Tätigkeitsbericht, Punkt 2.3.8). An meinen grundsätzlichen Bedenken hat sich nichts geändert.

3.2.4 Sicherheit für Landesweites Polizei-Informationssystem nur auf dem Papier?

Im Zweiten Tätigkeitsbericht hatte ich ausführlich zu den datenschutzrechtlichen Aspekten des Landesweiten Polizei-Informationssystems (LAPIS) Stellung genommen (Punkt 2.17.2). Das für die IT-Sicherheit vorgesehene Konzept erschien mir beispielhaft (Punkt 2.16.5).

Um mir einen Überblick über den Realisierungsstand von LAPIS und über die Umsetzung dieses Konzeptes zu verschaffen, kontrollierte ich Ende 1996 die DVZ M-V GmbH, weil das EDV-Verfahren LAPIS auf deren Rechnern läuft und dort die sensiblen personenbezogenen Daten gespeichert werden. Ebenso kontrollierte ich eine Poizeiinspektion, die an dem LAPIS-Pilotversuch teilgenommen hat und das System bereits seit September 1994 einsetzt.

Die Kontrolle der DVZ M-V GmbH ergab keinen Anlaß zur Beanstandung. Schwerpunktmäßig habe ich hier die Zugriffsschutzmechanismen und Protokollierungsfunktionen der LAPIS-Komponente Polizeiliche Erkenntnisdatei (PED) geprüft. Die Kontrolle zeigte, daß die geforderten Sicherheitsmaßnahmen vollständig umgesetzt wurden und dem derzeitigen Stand der Technik entsprechen.

In der Polizeiinspektion war demgegenüber festzustellen, daß viele der im Konzept geforderten technischen Maßnahmen nicht umgesetzt waren:

- die Unterbringung des Dienststellenservers entsprach im wesentlichen nicht den Vorgaben,
- als Verteiler im lokalen Netz wurde ein Gerät eingesetzt, das nicht über die geforderten Sicherheitsmerkmale verfügte,
- Verschlüsselungsverfahren, die die Vertraulichkeit der über das Weitverkehrsnetz LAVINE übermittelten Daten sicherstellen sollen, wurden nicht verwendet.

Auch die organisatorischen Rahmenbedingungen entsprachen weitgehend nicht den eigenen Vorgaben. Das dienststellenspezifische Sicherheitskonzept, in dem die Besonderheiten jeder LAPIS-Dienststelle berücksichtigt werden sollen, wurde erst nach der Ankündigung meiner Kontrolle erstellt, obwohl LAPIS in dieser Dienststelle zu diesem Zeitpunkt bereits seit fast zwei Jahren lief. Viele weitere organisatorische Hilfsmittel (zum Beispiel Betriebshandbuch, Datensicherungsrichtlinie, Hinweise zum Umgang mit Paßworten) lagen nicht vor.

Im Ergebnis der Kontrolle bei der Polizeiinspektion habe ich dem Innenminister aufgrund von Verstößen gegen die Bestimmungen des § 17 Abs. 1 und 2 DSG MV eine förmliche Beanstandung gemäß § 28 Abs. 1 Nr. 1 DSG MV ausgesprochen.

Die von mir festgestellten Mängel veranlaßten den Landtag, sich intensiv mit dem Realisierungsstand von LAPIS zu befassen. Der Innenausschuß hat den Innenminister um ausführliche Berichterstattung gebeten.

Schließlich wurde vereinbart, die Zusammenarbeit auf Referentenebene zu intensivieren. Der regelmäßige Informationsaustausch trägt nunmehr dazu bei, Schwachstellen früh zu erkennen und rechtzeitig geeignete und angemessene technische und organisatorische Maßnahmen zu treffen. So wurde beispielsweise ein Maßnahmeplan erstellt, um die bei der Kontrolle festgestellten Mängel möglichst schnell zu beseitigen. Die hierfür erforderliche Sicherheitstechnik (zum Beispiel ein Paßwortmanagementsystem und Verschlüsselungstechnik) befand sich Ende 1997 im Ausschreibungsverfahren. Darüber hinaus wurde die Organisationsstruktur für das

Projekt LAPIS den tatsächlichen Erfordernissen angepaßt und das Projekt sowohl personell als auch finanziell besser ausgestattet.

3.2.5 Zu Unrecht im Polizeicomputer

Aufgrund einer Strafanzeige wegen übler Nachrede ermittelte die Staatsanwaltschaft gegen einen Bürger. Die Polizei legte eine Kriminalakte zu seiner Person an und speicherte seine Daten in der Polizeilichen Erkenntnis Datei (PED MV). Nach Einstellung des Verfahrens wegen Geringfügigkeit sollten die Daten des Betroffenen noch zwei Jahre in der polizeilichen Datei verbleiben. Der Petent äußerte hiergegen Bedenken und bat mich um eine datenschutzrechtliche Prüfung.

Im strafrechtlichen Ermittlungsverfahren wird die Polizei für die Staatsanwaltschaft tätig und erhebt in diesem Zusammenhang personenbezogene Daten. Sie darf die Daten eines Verdächtigen über das Ermittlungsverfahren hinaus auch für präventiv-polizeiliche Zwecke verarbeiten und nutzen. Dies ist jedoch nur unter der Voraussetzung zulässig, daß es sich nicht um Bagatelldelikte handelt, eine Gefahrenprognose hinsichtlich der Begehung weiterer Straftaten vorliegt und die Speicherung zur Aufklärung oder Verhütung künftiger Straftaten erforderlich ist. Ist das Ergebnis des Ermittlungsverfahrens zum Zeitpunkt der Speicherung noch nicht bekannt, so dürfen die Daten zunächst nur maximal zwei Jahre gespeichert werden. Entfällt der zugrunde liegende Verdacht, sind die Daten sofort zu löschen.

Die Polizei teilte mir zunächst mit, daß sie in diesem Fall das Anlegen einer Kriminalakte für erforderlich hielt und nach Kenntnisnahme der Einstellungsverfügung der Staatsanwaltschaft eine Aussonderungsprüffrist von zwei Jahren festgesetzt hatte. Der Fall wurde anschließend nochmals durch das Innenministerium geprüft. Im Ergebnis wurden die Kriminalakte vernichtet und die Daten in der PED MV gelöscht, da die Speicherung der personenbezogenen Daten des Betroffenen weder zur Aufklärung noch zur Verhütung einer künftigen Straftat geeignet waren. Darüber habe ich den Petenten informiert.

Dieser Fall zeigt, daß nach wie vor Unsicherheiten beim Anlegen von Kriminalakten sowie bei der Speicherung in der PED MV bestehen. Unabhängig von diesem Einzelfall beabsichtigt der

Innenminister jetzt, entsprechende Richtlinien zu erarbeiten, um so mehr Rechtssicherheit zu erreichen.

3.3 Verkehr

3.3.1 Blitzen durch Private

In unserem Bundesland ist die Befugnis zur eigenständigen Überwachung des fließenden Verkehrs mittels stationärer Geschwindigkeitsmeßanlagen den Landkreisen und kreisfreien Städten übertragen worden. Da die Überwachungsanlagen teilweise von privaten Unternehmen gemietet werden und Mitarbeiter dieser Unternehmen an Messungen teilnehmen, entsteht der Eindruck, daß Private diese Messungen durchführen. Dagegen äußerten Autofahrer Bedenken.

Die Ordnungsbehörde darf Fotos von Geschwindigkeitsüberschreitungen nur dann für Ordnungswidrigkeitenverfahren verwenden, wenn diese auch rechtmäßig erlangt wurden. Dies setzt voraus, daß die Mitarbeiter der Behörde selbständig und eigenverantwortlich im Rahmen einer Messung den Tatbestand einer Verkehrsordnungswidrigkeit ermittelt haben. Die Inanspruchnahme Privater ist dabei ausschließlich auf Hilfstätigkeiten beschränkt. Zu dieser Frage habe ich mich bereits in meinem Zweiten Tätigkeitsbericht, Punkt 2.4.3, geäußert. Der Wirtschaftsminister unseres Landes hatte seinerzeit die Hinweise aufgegriffen und mit Erlaß vom 22. Dezember 1995 die erforderlichen Regelungen getroffen.

Hiernach obliegt der Ordnungsbehörde die alleinige Verantwortung für die Durchführung der Geschwindigkeitsüberwachung. Sie hat hierfür Mitarbeiter einzusetzen, welche die notwendigen Fachkenntnisse besitzen, die Messungen durchführen und kontrollieren. Mitarbeiter privater Unternehmen, von denen das Meßgerät und das Fahrzeug gemietet werden, sind lediglich für technische Hilfstätigkeiten einzusetzen. Zum Entwickeln der Meßfilme und Anfertigen von Positiven sowie zum Erfassen der Datensätze kann sich die Ordnungsbehörde im Rahmen einer Auftragsdatenverarbeitung eines privaten Anbieters bedienen. Gemäß § 4 DSG MV ist der Auftrag schriftlich zu erteilen. Es sind detaillierte Festlegungen zu treffen, wie der Auftragnehmer mit den Daten umzugehen hat und welche technischen und organisatorischen Maßnahmen gegebenenfalls zu realisieren sind. Die Mitarbeiter des Auftragnehmers sind auf das Datengeheimnis zu verpflichten. Eine Auswertung der Beweismittel durch den Auftragnehmer

ist unzulässig und obliegt allein der Ordnungsbehörde. Darüber hinaus sind bestehende Meldepflichten gegenüber den Aufsichtsbehörden zur Sicherung der datenschutzrechtlichen Kontrolle zu beachten.

Auf meine Anfrage hin erhielt ich im Februar 1996 den bereits verabschiedeten oben genannten Erlaß. Für die Umsetzung der aus § 4 DSG MV resultierenden datenschutzrechtlichen Anforderungen wurde eine Übergangsfrist von einem Jahr eingeräumt. Ich habe darauf hingewiesen, daß § 4 DSG MV unmittelbar zur Anwendung kommt und durch eine untergesetzliche Vorschrift - auch nicht für eine Übergangszeit - keinesfalls außer Kraft gesetzt werden kann. Dies wurde den Ordnungsbehörden zur Kenntnis gegeben.

Nachfragen zur inhaltlichen Ausgestaltung des Auftragsverhältnisses nach § 4 DSG MV habe ich zum Anlaß genommen, den Entwurf einer Mustervereinbarung für den Umgang mit personenbezogenen Daten im Auftrag für diesen Bereich zu erarbeiten und den Landkreisen und kreisfreien Städten im Juni 1996 zur Verfügung zu stellen.

Bei Prüfungen habe ich festgestellt, daß zwar in der überwiegenden Zahl der Fälle bereits schriftliche Verträge existierten, diese aber in keinem Fall den datenschutzrechtlichen Anforderungen entsprachen. So fehlte es an detaillierten Regelungen, die das Auftragsverhältnis und somit den Umgang mit personenbezogenen Daten durch den Auftragnehmer klar umrissen. Über die Beauftragung hatten mich nur einige Ordnungsbehörden informiert, obwohl sie gemäß § 4 Abs. 3 DSG MV dazu verpflichtet gewesen wären. Darüber hinaus waren die privaten Unternehmen ihrer Meldepflichtnach § 32 BDSG nicht nachgekommen.

Meine in diesem Zusammenhang gegebenen Empfehlungen wurden zwischenzeitlich berücksichtigt.

3.3.2 Anhörung des Betroffenen bei straßenverkehrsrechtlichen Ordnungswidrigkeiten

Eine Petentin übersandte mir einen Vordruck zur Prüfung, den sie von einer Bußgeldstelle im Rahmen der Anhörung nach § 55 Ordnungswidrigkeitengesetz (OWiG) erhalten hatte. Neben den Identitätsdaten der Betroffenen sowie den Angaben zum Sachverhalt wurden unter ande-

rem auch Beruf, Einkommen, Telefonnummer, Angaben zur Fahrerlaubnis sowie der Standort bei Wehrpflichtigen erfragt. Bei Nachfragen stellte sich heraus, daß die Bußgeldstellen in diesem Verfahren in unterschiedlichem Maße Daten erheben.

Bevor ein Bußgeldbescheid erlassen wird, ist dem Betroffenen Gelegenheit zur Äußerung zu geben. Zu diesem Zweck erhält er von der Bußgeldstelle einen Anhörungsbogen. Die Datenerhebung ist auf die für die Anhörung erforderlichen Daten zu beschränken.

Der Betroffene hat in jedem Fall die zur Identitätsfeststellung notwendigen Angaben zu seiner Person zu machen. Bei der Festsetzung einer Geldbuße können ferner auch die wirtschaftlichen Verhältnisse des Betroffenen Berücksichtigung finden. Da dieses Kriterium jedoch nicht regelmäßig als Bemessungsfaktor in Betracht kommt, ist eine Erhebung dieser Daten nur im Einzelfall erforderlich. Eine generelle Abfrage des Berufes sowie des Einkommens des Betroffenen bei straßenverkehrsrechtlichen Ordnungswidrigkeiten ist daher nicht zulässig. Die Telefonnummer kann für Rückfragen dienlich sein, sie ist jedoch für das Verfahren selbst nicht erforderlich, so daß es sich hierbei allenfalls um eine freiwillige Angabe handeln kann. Weiterhin ist es nicht generell notwendig, Angaben zur Fahrerlaubnis sowie zum Standort bei Wehrpflichtigen zu machen. Darüber hinaus ist zu beachten, daß für den Betroffenen keine Aussagepflicht zur Sache besteht.

Der Anhörungsbogen ist entsprechend zu gestalten, und es ist eine für den Betroffenen klare Trennung zwischen Pflichtangaben und freiwilligen Angaben vorzunehmen.

Das Wirtschaftsministerium unseres Landes hat diese Hinweise aufgegriffen und mit einem Rundschreiben die Bußgeldstellen darauf aufmerksam gemacht. Ich gehe davon aus, daß inzwischen danach verfahren wird.

3.3.3 Daten aus dem Paß- und Personalausweisregister

Häufig wenden sich Betroffene und Behörden mit der Frage an mich, in welchem Umfang das Paß- bzw. Personalausweisregister genutzt werden darf, um Fahrer bei der Ahndung von Verkehrsordnungswidrigkeiten festzustellen. Die Anfragen zeigen, daß in diesem Bereich noch

eine Reihe von Unsicherheiten besteht. So wies ein Landkreis beispielsweise die für das Register zuständigen Behörden in allgemeiner Form an, im Wege der Amtshilfe mit den Verfolgungsbehörden besser zusammenzuarbeiten, ohne dabei jedoch die maßgeblichen Rechtsgrundlagen zu benennen.

Sofern der Betroffene im Rahmen der Anhörung nach § 55 Ordnungswidrigkeitengesetz (OWiG) keine Angaben zum Sachverhalt macht oder bestreitet, zum maßgeblichen Zeitpunkt mit dem Auto gefahren zu sein, werden weitere Ermittlungen notwendig, um die Identität des Fahrzeugführers festzustellen. Die Paß- und Personalausweisregister werden hierbei regelmäßig als Informationsquelle genutzt. Seitdem die Ordnungsbehörden die Nachermittlungen zur Fahrerfeststellung bei geringfügigen Verkehrsordnungswidrigkeiten grundsätzlich in eigener Regie vornehmen und die Polizei nur noch bei bedeutsamen Ordnungswidrigkeiten einbeziehen, hat die Zahl der Ersuchen an die Paß- und Personalausweisbehörden zugenommen. Aus Kostengründen wird häufig auf eine Fahrerfeststellung vor Ort verzichtet.

Das Paß- bzw. Personalausweisregister ist kein öffentliches Register. Nach § 22 Paßgesetz und § 2 b Gesetz über Personalausweise dürfen an die ersuchende Behörde Daten aus dem Register übermittelt werden, wenn diese

- auf Grund von Gesetzen oder Rechtsverordnungen berechtigt ist, die Daten zu erhalten,
- ohne Kenntnis der Daten nicht in der Lage wäre, ihre Aufgabe zu erfüllen und
- die Daten nicht oder nur mit unverhältnismäßig hohem Aufwand beim Betroffenen erhoben werden können oder wegen der Art der Aufgabe von einer Datenerhebung beim Betroffenen abgesehen werden muß.

Die Verfolgungsbehörde hat ihre Ermittlungstätigkeit so auszugestalten, daß die erforderlichen Daten grundsätzlich beim Betroffenen erhoben werden. Erst wenn dies nicht möglich oder hierfür ein unverhältnismäßig hoher Aufwand erforderlich ist, kann sie ein Ersuchen an die Paß- und Personalausweisbehörde richten, das Lichtbild des Betroffenen oder eine Kopie vorzulegen beziehungsweise zu übersenden. Ein solches Verfahren ist jedoch nicht allein schon dadurch gerechtfertigt, daß ein Ersuchen weniger zeitaufwendig und kostengünstiger ist. Vielmehr bedarf es Tatsachen, die einen unverhältnismäßig hohen Aufwand belegen. Dies ist in jedem Einzelfall zu prüfen.

Das Ersuchen muß sich jedoch immer auf eine konkrete Person beziehen. Eine Übersendung von Beweisfotos durch die Bußgeldstelle an die Paß- und Personalausweisbehörde mit der Bitte, anhand des Paß- bzw. Personalausweisregisters festzustellen, wer der auf dem Foto abgebildete Fahrzeugführer ist, erfüllt diese Forderung nicht und ist datenschutzrechtlich bedenklich. Es zählt nicht zu den Aufgaben der Paß- und Personalausweisbehörde, die Übereinstimmung der Identität zwischen Fahrzeugführer und der im Register vorhandenen Person zu bestätigen. Im Rahmen der Verfolgung von Ordnungswidrigkeiten hat die Verfolgungsbehörde selbst die Tatsachen sowie den Verantwortlichen, der zur Tatzeit das Fahrzeug geführt hat, festzustellen.

Gemäß § 53 OWiG kann die Verfolgungsbehörde auch Familienangehörige, Nachbarn und sonstige Dritte befragen, um den Fahrzeugführer zu ermitteln. Da hierbei unter Umständen eine Vielzahl von Personen Kenntnis vom Ordnungswidrigkeitenverfahren erhält, sollte dies nur dann erfolgen, wenn die Feststellung des Fahrzeugführers anders nicht möglich ist. Unter Verhältnismäßigkeitsgesichtspunkten werden hierbei auch die Schwere des Verkehrsverstoßes und die schutzwürdigen Interessen des Betroffenen zu berücksichtigen sein. Befragungen in der Nachbarschaft sind bei Ordnungswidrigkeiten, die zu einer Eintragung in das Verkehrszentralregister führen, zulässig, wenn die Ermittlungen beim Betroffenen und das Ersuchen an die Paß- und Personalausweisbehörde zu keinem Ergebnis geführt haben.

Bei der Auswahl der einzelnen Maßnahmen ist in Abhängigkeit vom Einzelfall der Verhältnismäßigkeitsgrundsatz zu beachten.

Nur ausdrücklich vom Behördenleiter ermächtigte Mitarbeiter einer Bußgeldstelle dürfen entsprechende Ersuchen stellen. Die Ermächtigung ist schriftlich vorzunehmen. Ferner hat die Bußgeldstelle den Anlaß des Ersuchens sowie die Herkunft der übermittelten Daten und Unterlagen zu dokumentieren, um die Zulässigkeit der Maßnahmen gegebenenfalls auch im weiteren Verfahren nachweisen zu können.

Um die Anwendung der geltenden Bestimmungen zu erleichtern, habe ich der Landesregierung empfohlen, verbindliche Regelungen zur Fahrerfeststellung zu treffen. Das Wirtschaftsministerium hat daraufhin mitgeteilt, daß die Notwendigkeit einer einheitlichen Verfahrensweise gese-

hen wird und daher beabsichtigt sei, zusammen mit dem Innenressort einen entsprechenden Erlaß herauszugeben. Dieser stand bei Redaktionsschluß noch aus.

3.4 Verfassungsschutz

3.4.1 Sicherheitsüberprüfungsgesetz verabschiedet

Im Dezember 1997 hat der Landtag den Entwurf der Landesregierung für ein Sicherheitsüberprüfungsgesetz mehrheitlich angenommen. Damit kehrt für alle an der Sicherheitsüberprüfung Beteiligten Rechtssicherheit ein. Gegenüber den bisher gültigen Sicherheitsüberprüfungsrichtlinien und einem bereits 1995 vorgelegten Referentenentwurf für ein Sicherheitsüberprüfungsgesetz ergeben sich aus datenschutzrechtlicher Sicht folgende wesentliche Verbesserungen:

- Als sicherheitserheblich werden nunmehr „Erkenntnisse“ und nicht mehr „Sachverhalte“ angesehen.

- In der abzugebenden Sicherheitserklärung wird nun nicht mehr undifferenziert nach „Funktionen“ und „Massenorganisationen“ in der ehemaligen DDR gefragt, sondern nur noch nach hauptamtlichen Funktionen in einer Partei oder Massenorganisation.

- Ursprünglich sollten tatsächliche Anhaltspunkte für geistige und seelische Störungen sowie Alkohol-, Drogen- oder Tablettenmißbrauch von Personen, die eine sicherheitsempfindliche Tätigkeit ausüben sollen, zur Sicherheitsakte genommen werden. Da nicht klar war, wer wie beurteilen soll, ob Anhaltspunkte für einen Mißbrauch vorliegen, ist diese Regelung ersatzlos gestrichen worden.

- Die Speicher- bzw. Löschungsfristen wurden für den Fall gekürzt, daß die Sicherheitsüberprüfung vorzeitig abgebrochen wird und bis zu diesem Zeitpunkt keine sicherheitserheblichen Erkenntnisse vorliegen. Die Verpflichtung zur umgehenden Vernichtung der Unterlagen des Betroffenen bei der Verfassungsschutzbehörde wurde in den Gesetzestext aufgenommen. Für den Fall, daß der Betroffene keine sicherheitsempfindliche Tätigkeit aufnimmt, obwohl dies aufgrund der Sicherheitsüberprüfung möglich gewesen wäre, sind die Daten

von der Verfassungsschutzbehörde innerhalb eines Jahres zu löschen, sofern der Betroffene nicht in die weitere Speicherung einwilligt.

Im April 1997 hatte der Innenausschuß eine Expertenanhörung zum Gesetzentwurf der Landesregierung durchgeführt. Dort wurden von verschiedenen Seiten Hinweise, insbesondere hinsichtlich der Unterschiede zwischen dem Sicherheitsüberprüfungsgesetz des Bundes und dem Sicherheitsüberprüfungsgesetz des Landes gegeben.

Letztlich ist der Gesetzentwurf jedoch unverändert verabschiedet worden. So ist es nun unter anderem vorstellbar, daß ein Bewerber für eine sicherheitsempfindliche Tätigkeit in einer Bundesbehörde unseres Landes (beispielsweise Arbeitsämter oder Zoll), in der nach dem Bundesgesetz sicherheitsüberprüft wird, weniger personenbezogene Daten angeben muß, als ein Bewerber für eine sicherheitsempfindliche Tätigkeit in einer Landesbehörde. Ich halte diese Unterscheidung für nicht gerechtfertigt und unnötig.

Darüber hinaus ist die Verfassungsschutzbehörde nach wie vor berechtigt, bei dem von Bund und Ländern betriebenen Nachrichtendienstlichen Informationssystem NADIS anzufragen, ob Erkenntnisse über den Ehegatten, den Lebensgefährten und die Auskunfts- und Referenzperson vorliegen. Die in der Gesetzesbegründung gegebene Erklärung, es handele sich hierbei lediglich um eine „bloße Anfrage“, verharmlost die Tatsache, daß die Anfrage in NADIS ohne Wissen der zu befragenden Personen schon einen erheblichen Eingriff in deren Recht auf informationelle Selbstbestimmung darstellt. Meine Empfehlung, diese NADIS-Abfragen von der Einwilligung der zu befragenden Personen abhängig zu machen, ist nicht berücksichtigt worden.

Außerdem erscheint es mir nicht nachvollziehbar, warum ein von einer Sicherheitsüberprüfung Betroffener grundsätzlich nicht seine Sicherheitsüberprüfungsakte einsehen darf. Meines Erachtens ist nicht zu begründen, warum ein Betroffener, der sich freiwillig einer Sicherheitsüberprüfung unterzogen hat, nicht selbst sehen soll, welche Daten die Verfassungsschutzbehörde zu seiner Person speichert. Überwiegende Geheimhaltungsinteressen oder schwerwiegende schutzwürdige Interessen Dritter, die einer Akteneinsicht entgegenstehen, hätten trotzdem ohne weiteres hinreichend berücksichtigt werden können.

3.4.2 Campingplätze im Visier des Verfassungsschutzes

Im Juni 1996 berichteten Medien über Aktivitäten der Verfassungsschutzbehörde auf einigen Zeltplätzen des Landes. Der Leiter einer Kurverwaltung war demnach von einer Mitarbeiterin der Behörde aufgefordert worden, Camper zu melden, die seiner Meinung nach der links- oder rechtsextremen Szene angehören. Auf seine telefonische Nachfrage zu Erkennungsmöglichkeiten dieses Personenkreises sei ihm gesagt worden, daß damit „Buntgescheckte, Punker und langhaarige Personen“ gemeint wären.

Um die datenschutzrechtlichen Aspekte dieser Maßnahmen zu bewerten, habe ich eine Kontrolle beim Verfassungsschutz durchgeführt. Nach Einblick in die relevanten Unterlagen und aufgrund der Erläuterungen des Leiters der Behörde stellte sich der Vorgang wie folgt dar:

Ausgangspunkt für die Maßnahmen des Verfassungsschutzes waren rechtsextremistisch motivierte Gewalttaten aus den Jahren 1994 und 1995, die vereinzelt auf Campingplätzen in Mecklenburg-Vorpommern begangen wurden.

Mitarbeiter des Verfassungsschutzes hatten deshalb im Frühjahr 1996 ausgewählte Campingplätze Mecklenburg-Vorpommerns besucht. Die Campingplatzbesitzer wurden gebeten, dem Verfassungsschutz das Eintreffen rechtsextremistischer Gruppen parallel zur Benachrichtigung der Polizei mitzuteilen, jedoch ohne personenbezogene Daten einzelner zu übermitteln. Bei gleichzeitigem Vorhandensein einer linksextremistischen Gruppe sollte auch diese Tatsache mitgeteilt werden. Es war beabsichtigt, diese Informationen dann mit den bei der Verfassungsschutzbehörde vorhandenen Erkenntnissen zusammenzuführen, um gegebenenfalls weitere Maßnahmen einzuleiten. Erst beim Vorliegen tatsächlicher Anhaltspunkte für den Verdacht verfassungsfeindlicher Bestrebungen sollten dann in einem zweiten Schritt personenbezogene Daten durch die Verfassungsschutzbehörde erhoben werden. Die in Medien genannten Kriterien „Buntgescheckte, Punks oder langhaarige Personen“ waren im Arbeitsauftrag der zuständigen Mitarbeiter nicht enthalten. Daß diese Begriffe jedoch tatsächlich verwendet wurden, bewies ein Tonbandmitschnitt des Gespräches zwischen dem Leiter der Kurverwaltung und der Mitarbeiterin des Verfassungsschutzes.

Die Campingplatzbesitzer wurden ausdrücklich darauf hingewiesen, daß die erste Meldung in jedem Fall an die Polizei zu gehen hätte und die Möglichkeit der parallelen Mitteilung an die Verfassungsschutzbehörde nur ein zusätzliches Angebot darstelle. Auf die Freiwilligkeit der Mitarbeit wurden sie hingewiesen. Schließlich wurden die Inhaber der Campingplätze gebeten, Diskretion im Hinblick auf das stattgefundene Gespräch zu wahren.

Zur Dokumentation der Maßnahme stellte ich folgendes fest:

Es gab lediglich einen mündlichen Arbeitsauftrag. Dieser Auftrag wurde in den Dienstbesprechungen des Verfassungsschutzes zur Vorbereitung der Maßnahme näher ausgeführt.

In der zur Kontrolle vorgelegten Akte sind auf Formblättern Angaben zu den Campingplätzen (Lage, Anfahrtsweg etc.) sowie Inhabern (Namen, Telefonnummer) enthalten. Darüber hinaus befinden sich in der Akte einzelne Vermerke zu Maßnahmen, welche die Verfassungsschutzbehörde im vorangegangenen Jahr hinsichtlich rechtsextremistisch motivierter Straftaten durchgeführt hatte. Bereits damals wurde mit den Campingplatzinhabern Kontakt aufgenommen, auf deren Plätzen solche Straftaten begangen wurden. In einem Vermerk hieß es dazu unter anderem, daß sogenannte „Nahbeobachter“ angeworben und zur Zusammenarbeit mit dem Verfassungsschutz bewogen werden sollten. Dazu wurde während der Kontrolle mitgeteilt, daß es sich um keine auf Dauer angelegte Zusammenarbeit zwischen dem Verfassungsschutz und den dort genannten Personen handele. Diese Personen erhielten kein Geld für ihre Tätigkeit. Daher sei der dort verwandte Begriff mißverständlich.

Aus datenschutzrechtlicher Sicht war einerseits zu prüfen, ob die Verfassungsschutzbehörde überhaupt in diesem Zusammenhang auf den Campingplätzen des Landes aktiv werden durfte, und andererseits, ob die Art und Weise des Vorgehens geeignet und angemessen war, um für den Verfassungsschutz relevante Erkenntnisse zu gewinnen. Da die Dokumentation nicht aussagekräftig war, habe ich das gesamte Verfahren vorwiegend anhand der Aussagen des Leiters und der zuständigen Mitarbeiter des Verfassungsschutzes wie folgt bewertet:

Eine direkte Einbeziehung von Privaten in die Tätigkeit der Verfassungsschutzbehörde ist im Landesverfassungsschutzgesetz nicht ausdrücklich geregelt. Ich halte sie für grundsätzlich be-

denklich. Es hätte in diesem Fall insbesondere für die angesprochenen Campingplatzinhaber klar und deutlich zum Ausdruck kommen müssen, daß es sich um eine freiwillige Mitwirkung im Sinne einer Unterstützung handelt, wenn sie im Einzelfall bei Vorliegen der Voraussetzungen relevante Sachverhalte übermitteln. Des weiteren mußte klar sein, daß keine auf Dauer angelegte Zusammenarbeit mit der Verfassungsschutzbehörde vorgesehen ist. Da eine gezielte Aufforderung zur Mithilfe erfolgte und darüber hinaus die ausdrückliche Bitte um Diskretion geäußert wurde, könnten sich die Campingplatzbetreiber zur Mitwirkung verpflichtet gefühlt haben. Deshalb blieben Zweifel, ob das Prinzip der Freiwilligkeit jedem Ansprechpartner auch tatsächlich deutlich geworden ist. Ferner hätte die Grenzziehung im Hinblick auf die hier keineswegs beabsichtigte Anwerbung von V-Leuten eindeutig sein müssen. Die in den Vermerken vorgefundenen Aussagen zum Anwerben von sogenannten Nahbeobachtern ließen diese erforderliche präzise Grenzziehung vermissen.

Die Tatsache, daß als Identifizierungsmerkmale Begriffe wie „Buntgescheckte, Punks oder langhaarige Personen“ verwandt werden, ist aus datenschutzrechtlicher Sicht äußerst bedenklich und verstößt gegen das rechtsstaatliche Gebot der Verhältnismäßigkeit. Die genannten Merkmale sind völlig ungeeignet, den gesuchten Personenkreis festzustellen. Allein äußere Merkmale eines Menschen wie Kleidung, Haarlänge und -farbe oder andere Auffälligkeiten als maßgebliches Kriterium zu verwenden, um Personen extremistisch orientierten Gruppen zuzuordnen, ohne weitere Kriterien oder Verhaltensweisen zu berücksichtigen, ist diskriminierend. Die unsachliche Differenzierung aufgrund äußerer Merkmale verstößt gegen § 7 Abs. 2 Landesverfassungsschutzgesetz (LVerfSchG). Darüber hinaus bestand durch die - allerdings vom Arbeitsauftrag nicht gedeckte - Äußerung der eingangs erwähnten Mitarbeiterin des Verfassungsschutzes die Gefahr, daß der Verfassungsschutz personenbezogene Daten erhält, die nicht zu dessen Aufgabenerfüllung erforderlich sind. Derartige Methoden würden zu einem rechtswidrigen Eingriff in das Recht auf informationelle Selbstbestimmung führen, und eine Reihe von Betroffenen würde in das Beobachtungsfeld des Verfassungsschutzes geraten, ohne daß die notwendigen Voraussetzungen dafür vorlägen.

Um eine bessere Transparenz und auch eine nachträgliche datenschutzrechtliche Prüfung gewährleisten zu können, wäre eine lückenlose Dokumentation erforderlich gewesen. Diese Dokumentation hätte Aufschluß über das gesamte Verfahren sowie die Zielstellung des Einsatzes geben müssen. Diese Kritik ergibt sich aus der Notwendigkeit, die von der Exekutive getroffe-

nen Maßnahmen zu kontrollieren (Rechtsstaatsprinzip, Art. 20 Abs. 3 GG) sowie aus der Forderung nach datenschutzrechtlicher Transparenz (Volkszählungsurteil, BVerfGE 65, 1 ff.) und aus der in der Verfassung des Landes Mecklenburg-Vorpommern vorgesehenen Kontrolle durch den Datenschutzbeauftragten.

Die innerbehördliche Organisation muß auch beim Verfassungsschutz so gestaltet sein, daß sie den datenschutzrechtlichen Anforderungen gerecht wird. Die Mitarbeiter müssen die für ihre Aufgaben notwendigen Kenntnisse erlangen und die maßgeblichen Bestimmungen einhalten. Ergibt sich dies nicht unmittelbar und ausreichend aus den geltenden Rechtsvorschriften, so sind Konkretisierungen, zum Beispiel in Einsatzplänen, Dienstanweisungen oder Protokollen, vorzunehmen. Diese Voraussetzungen waren insbesondere für die besagte Mitarbeiterin nicht gegeben, so daß ihr Einsatz aus datenschutzrechtlicher Sicht nicht zulässig war.

Für das Erheben personenbezogener Daten gilt neben den konkret in § 9 LVerfSchG aufgeführten Voraussetzungen ebenso der Grundsatz der Verhältnismäßigkeit. Deshalb wäre das oben beschriebene abgestufte Verfahren, bei dem im ersten Schritt keine personenbezogenen Daten übermitteln werden sollten, aus datenschutzrechtlicher Sicht nicht zu bemängeln gewesen.

Im Ergebnis meiner Kontrolle habe ich dem Innenminister eine förmliche Beanstandung ausgesprochen und die Empfehlungen gegeben,

- Verfahrensabläufe bei solchen oder ähnlichen Einsätzen vorher zu prüfen,
- künftig derartige Verfahren aus den oben genannten Gründen hinreichend zu dokumentieren,
- die Freiwilligkeit bei der Einbeziehung Privater deutlicher darzustellen, insbesondere auch die Bitte um Diskretion wegfallen zu lassen,
- im Hinblick auf die Einbeziehung von Privaten unter dem Gesichtspunkt der Verhältnismäßigkeit eine intensivere Einzelfallprüfung durchzuführen und
- den Vorfall mit den zuständigen Mitarbeitern auszuwerten.

Meinen Empfehlungen wurde gefolgt. Unter anderem wurde eine schriftliche Dienstanweisung für Maßnahmen zur Informationsgewinnung durch den Verfassungsschutz erlassen, die die datenschutzrechtlichen Regelungen berücksichtigt.

3.5 Datenschutz im Landtag

3.5.1 Umgang mit personenbezogenen Daten in Untersuchungsausschüssen

Abgeordnete haben mich gebeten, Empfehlungen zum Umgang mit personenbezogenen Daten durch Untersuchungsausschüsse zu geben. Bei der Arbeit dieser Gremien kommt es in vielen Fällen auch zu Eingriffen in das Grundrecht auf informationelle Selbstbestimmung. Eingriffe in dieses Recht bedürfen jedoch einer verfassungsmäßigen normenklaren Ermächtigungsgrundlage (BVerfGE 65, 1 ff.). Artikel 34 unserer Landesverfassung trifft Regelungen zu den Untersuchungsausschüssen. Dort wird auf das Gesetz verwiesen.

Das Vorläufige Untersuchungsausschußgesetz vom 10. Juli 1991 enthält jedoch keine datenschutzrechtlichen Regelungen.

Auf der Basis der Entscheidung des Hamburgischen Verfassungsgerichts vom 19. Juli 1995 (HVerfG 1/95), die den Umgang mit personenbezogenen Daten durch einen Untersuchungsausschuß zum Gegenstand hat, habe ich ein Arbeitspapier erstellt und den Fraktionen, den Untersuchungsausschüssen sowie den Ministerien unseres Landes zur Verfügung gestellt. Es enthält unter anderem folgende Hinweise:

- Zu prüfen ist zunächst, ob es sich bei den in den Akten enthaltenen Daten um personenbezogene Daten handelt, da das Grundrecht auf informationelle Selbstbestimmung nur Einzelangaben über bestimmte oder bestimmbare natürliche Personen schützt, nicht jedoch Daten juristischer Personen.

- Der Untersuchungsausschuß hat den Grundsatz der Verhältnismäßigkeit zu beachten. Ein Umgang mit personenbezogenen Daten durch den Ausschuß kann nur erfolgen, sofern dies für seine Tätigkeit erforderlich ist. Anderenfalls sind die Daten zu anonymisieren.

- Sensible personenbezogene Daten, deren Schutzbedarf eine vertrauliche Behandlung erfordert, dürfen nur in nichtöffentlicher Sitzung behandelt werden.

- Eine generelle Einstufung von bestimmten Daten im Hinblick auf deren Gefährdung ist unzulässig. Die Abwägung hat immer fallbezogen und individuell zu erfolgen. Die Akten sind beim Untersuchungsausschuß so zu schützen, daß kein Unbefugter Zugang erhalten kann.

Der Präsident des Landtages hat mich darüber informiert, daß er im Ältestenrat anregen werde, über den Entwurf eines Untersuchungsausschußgesetzes zu beraten.

3.5.2 Überprüfung nach dem Abgeordnetengesetz

Nach dem Abgeordnetengesetz unseres Landes überprüft der Landtag seine Mitglieder auf Mitarbeit im Staatssicherheitsdienst. Zu diesem Zweck hatte er mit der Mehrheit seiner Mitglieder eine Bewertungskommission gewählt.

Nach Beendigung ihrer Arbeit war die Bewertungskommission zu dem Ergebnis gekommen, daß keinem Abgeordneten wegen einer Zusammenarbeit mit dem Staatssicherheitsdienst die Niederlegung seines Mandats empfohlen werden muß. Vor der Bekanntgabe dieses erfreulichen Ergebnisses waren allerdings in den Medien bereits Meldungen aufgetaucht, nach denen zwei Abgeordnete durch Stasi-Kontakte belastet sein sollten.

Deshalb habe ich dem Vorsitzenden der Kommission empfohlen, das Überprüfungsergebnis sofort bekanntzugeben und damit nicht bis zu der Pressekonferenz zu warten, die für einige Tage später geplant war. Mir erschien das wichtig, um den Verdächtigungen die Nahrung zu nehmen und die betreffenden Abgeordneten von der psychischen Belastung zu befreien. Aber auch nach Bekanntgabe des Abschlußberichts der Kommission ebbten die Spekulationen nicht gleich ab.

So hatte beispielsweise ein Nachrichtenmagazin Unterlagen über einen Abgeordneten erhalten, aus denen hervorgehen soll, daß er als Informeller Mitarbeiter beim Staatssicherheitsdienst registriert gewesen sei. Von verschiedenen Seiten wurde eine Indiskretion der früheren Beschäftigungsstelle vermutet. Man bat mich, der Sache nachzugehen. Meine daraufhin durchgeführte Kontrolle ergab folgendes:

Im Dezember 1991 war der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes (BStU) vom damaligen Arbeitgeber um Mitteilung gebeten worden, ob Erkenntnisse über eine Zusammenarbeit des Betroffenen mit dem Staatssicherheitsdienst vorliegen. Erst im Dezember 1995 ging die Mitteilung des BStU in der Beschäftigungsstelle ein. Zwischenzeitlich hatte der Betroffene wegen seiner Abgeordnetentätigkeit beantragt, das Arbeitsverhältnis ruhen zu lassen.

Nun wurde die Mitteilung aber nicht - wie sonst üblich - unbearbeitet an den Bundesbeauftragten zurückgeschickt, sondern der Dienststellenleiter befaßte sich selbst mit dem Vorgang und versah die Schriftstücke mit Markierungen. Außerdem führte er ein Gespräch mit dem Betroffenen. Über dieses Gespräch existiert jedoch weder ein Vermerk in den Unterlagen noch ein Protokoll. Im Januar 1996 wurden die Unterlagen vollständig zurückgesandt. Allerdings nicht an die Behörde, sondern an den Bundesbeauftragten, Herrn Gauck, direkt. Im Begleitschreiben wies der Dienststellenleiter ausdrücklich auf folgendes hin: „Aufgrund der kürzlich durch den Landtag beschlossenen neuerlichen Überprüfung aller Landtagsabgeordneten gehe ich davon aus, daß durch Sie weitere Schritte einzuleiten sind." Damit und durch die besondere Vorgehensweise in diesem Fall trifft er eine Wertung und läßt erkennen, daß er die Mitteilung des BStU in gewisser Weise wie einen Beleg für eine Zusammenarbeit des Betroffenen mit dem Staatssicherheitsdienst interpretiert.

Nach dem Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (StUG) sind die Daten aus den Akten zweckgebunden zu verwenden (§ 29 Abs. 1 StUG). In diesem Fall sind sie aber nicht für die gesetzlich normierte Prüfung, sondern für ein Gespräch mit dem Betroffenen verwendet worden, welches der Dienststellenleiter selbst als „privat" bezeichnet und damit auch erklärt, weshalb kein Gesprächsvermerk beziehungsweise Protokoll angefertigt wurde. Es bestand also offensichtlich keine Aufgabe, zu deren Erfüllung die Kenntnis des Inhalts der Unterlagen erforderlich gewesen wäre. Deshalb habe ich den Umgang mit den Daten in diesem Fall förmlich beanstandet und Empfehlungen gegeben, wie in solchen Fällen künftig zu verfahren ist. In seiner Stellungnahme sicherte der Dienststellenleiter zu, meine Empfehlungen künftig zu beachten.

Im Rahmen der Kontrolle hatte der Dienststellenleiter unter anderem versichert, daß er Dritte über den Inhalt nicht informiert hat. Später stellte sich allerdings heraus, daß das nicht den Tat-

sachen entspricht. Nach meiner Bitte um erneute Stellungnahme teilte er mir mit, daß er den Vorstand einer Partei telefonisch über das Vorliegen einer BStU-Akte informiert und dies auch im persönlichen Gespräch dem Betroffenen gegenüber angekündigt habe. Konkrete Inhalte der Akte seien dabei nach seiner Aussage nicht offenbart worden.

Aber allein die Tatsache, daß er von sich aus mit einem Dritten über das Vorliegen einer Mitteilung des BStU spricht, ist datenschutzrechtlich als Übermittlung zu werten. Zumal dies für jedermann erkennbar nur dann sinnvoll erscheint, wenn der Dienststellenleiter seine subjektive Wertung andeutungsweise darlegt. Eine gesetzliche Grundlage für diese Mitteilung an Dritte existiert nicht und eine Einwilligung im Sinne des Datenschutzgesetzes lag nicht vor. Deshalb habe ich diese Übermittlung ebenfalls beanstandet.

Letztendlich hat sich auch der Landesbeauftragte für die Unterlagen des Staatssicherheitsdienstes mit diesem Fall befaßt. Er bewertet die BStU-Mitteilung in diesem Fall nicht als Beleg für eine Mitarbeit des Betroffenen bei der Staatssicherheit. In der Presse wurde er mit den Worten wiedergegeben: „Nur wenige haben sich so mutig gegen die Stasi gewehrt“, und die Stasi hätte nicht arbeiten können, wenn sich alle so verhalten hätten. Angesichts dieses Ergebnisses sind die Verletzungen des Rechts auf informationelle Selbstbestimmung durch den Dienststellenleiter besonders schwerwiegend. Aber selbst bei einem anderen Ergebnis wäre sein Vorgehen zweifellos als gesetzeswidrig einzustufen gewesen.

3.6 Einwohnerwesen

3.6.1 DDR-Meldedaten - ein altes Problem

Das polizeiliche Meldewesen der DDR umfaßte eine Vielzahl von Datensammlungen. Neben den auch für die heutige Aufgabenerfüllung der Meldebehörden erforderlichen Daten wurden in der örtlichen Meldekartei und in der Kreismeldekartei weitere Angaben des Betroffenen gespeichert. Hierzu zählen unter anderem der Beruf, die Tätigkeit, die Personenkennzahl, Auslandsaufenthalte, Besuch aus dem Ausland, die Ausschreibung zur Fahndung, die Tätigkeit als freiwilliger Helfer der Polizei, der Besitz von Jagdwaffen, die Auflage staatlicher Kontrollmaßnahmen, Eintragungen aus dem Strafregister und die kriminalistische Registrierung bestimmter Personen.

Bei der Übernahme der Daten aus dem Zentralen Einwohnerregister der DDR für die heutigen Melderegister fehlten zum Teil Daten, wie Vornamen, frühere Namen und frühere Anschriften. Die Meldebehörden sind daher verpflichtet, das aktuelle Melderegister im Rahmen der täglichen Arbeit anhand der alten örtlichen Meldekartei und Kreismeldekartei zu ergänzen. Dieser Verpflichtung sind die Meldebehörden bisher mit unterschiedlicher Intensität nachgekommen. Aufgrund der noch unvollständigen Daten in den Registern der Meldebehörden und der bisher nur teilweise erfolgten Nacherfassung der melderechtsrelevanten Daten aus den alten Karteien ist es nach wie vor nötig, auf diese Altdatenbestände zurückzugreifen. So bedarf es beispielsweise bei Anträgen für Leistungen nach dem Vertriebenenzuwendungsgesetz eines lückenlosen Nachweises der Wohnsitze des Betroffenen. Ferner ist ein Rückgriff auf diese Daten für Ersuchen von Betroffenen notwendig, um Verbindungen zu Eltern und Verwandten herzustellen.

Die weitere Aufbewahrung der alten Karteien und der Zugriff auf diese Daten wurden zwischen dem Innenministerium und meiner Behörde beraten. Im Ergebnis hat das Innenministerium einen Erlaß herausgegeben. Für eine Übergangszeit können die Meldekarteien unter folgenden Maßgaben noch bei den Meldebehörden verbleiben:

- Die alten Meldekarteien sind räumlich getrennt vom aktuellen Melderegister aufzubewahren und durch technische und organisatorische Maßnahmen nach § 17 Landesdatenschutzgesetz von Mecklenburg-Vorpommern zu sichern.

- Auskünfte über melderechtsfremde Daten dürfen nur dem Betroffenen selbst oder zur Behebung einer Beweisnot seinem Rechtsnachfolger erteilt werden.

- Beim Erteilen von Auskünften aus den alten Meldekarteien dürfen keine neuen Datenbestände, beispielsweise durch Aufbewahren von Kopien der Karteien in Akten, angelegt werden.

- Ein Umgang mit diesen Karteien ist nur dem Amtsleiter sowie von ihm schriftlich besonders ermächtigten Mitarbeitern erlaubt.

– Im aktuellen Melderegister noch fehlende Daten sind anhand der alten Karteien nachzuerfassen.

Um einen Überblick zu erhalten, in welchen Fällen Betroffene noch Auskünfte zu ihren Daten aus den alten Karteien benötigen, ist den Meldebehörden eine jährliche Berichtspflicht auferlegt worden. Mit dem Ziel, die alten Karteien zu archivieren beziehungsweise - soweit keine Übernahme durch ein Archiv erfolgt - die melderechtsfremden Daten zu löschen, wird im Jahre 2000 erneut geprüft, ob weiterhin ein Auskunftsbedarf der Betroffenen besteht.

3.6.2 Personenstandsgesetz contra Familienforschung

Das Interesse einzelner an der Vergangenheit und an familiären Verknüpfungen über Generationen hinweg beschäftigt in zunehmendem Maße auch den Datenschutz. So erreichen mich immer häufiger Anfragen und Beschwerden von Privatpersonen zu der Auskunftspraxis der Standesämter in unserem Land.

Gemeinsames Anliegen der Petenten ist die Familienforschung anhand alter Dokumente wie der Kirchen- und Personenstandsbücher. Die Informationen werden von den Familienforschern in mühsamer Recherche zusammengetragen und dann wie ein Puzzle zusammengesetzt. In Einzelfällen lehnen die Standesämter es jedoch ab, Auskünfte zu geben. Dies stößt bei den Anfragenden, insbesondere wenn die betroffenen Personen bereits seit langem verstorben sind, auf Unverständnis.

§ 61 Abs. 1 des Personenstandsgesetzes regelt, unter welchen Voraussetzungen Privatpersonen Einsicht in Personenstandsbücher (Heirats-, Familien-, Geburten- und Sterbebuch) gewährt werden darf. Zunächst steht dieses Recht nur Personen zu, auf die sich der Eintrag in diesen Büchern bezieht. Ferner dürfen auch der Ehegatte sowie die Vorfahren und Abkömmlinge des Betroffenen Einsicht erhalten. Dieses „abgeleitete Benutzungsrecht“ ist auf die Verwandten in gerader aufsteigender oder absteigender Linie beschränkt. Soweit der Antragsteller nicht zu diesem Personenkreis zählt, erhält er nur Einsicht, wenn er ein rechtliches Interesse glaubhaft machen kann. Das rechtliche Interesse erfordert das Vorliegen eines besonderen Rechtsgrundes, etwa daß der Auskunftssuchende die Daten zur Durchsetzung von Rechtsansprüchen benötigt. Da die Familienforschung nicht hierunter fällt, bleibt der Weg zu den Daten in diesen

Fällen versperrt. In den von mir geprüften Einzelfällen waren die hinterfragten Entscheidungen der Verwaltung aufgrund der geltenden Gesetzeslage nicht zu beanstanden.

Allerdings gibt es seitens der Bundesregierung mittlerweile seit Jahren Überlegungen zur Änderung des Personenstandsgesetzes. So ist beabsichtigt, die Einsichtnahme bereits bei Glaubhaftmachen eines berechtigten Interesses zuzulassen, wenn seit dem Tod des Betroffenen mindestens 30 Jahre oder, falls der Todestag nicht bekannt ist, seit der Geburt mindestens 120 Jahre vergangen sind. Als berechtigtes Interesse wird jedes auf sachlichen Erwägungen beruhende ideelle und wirtschaftliche Interesse anerkannt, das mit der Rechtsordnung im Einklang steht. Hierunter fallen in diesem Zusammenhang auch Auskunftsersuchen für Zwecke der Familien- oder Ahnenforschung. Mit der Verabschiedung eines Änderungsgesetzes durch den Bundestag wird jedoch nicht mehr in dieser Legislaturperiode zu rechnen sein. Es bleibt zu hoffen, daß dieses Vorhaben nicht weiter auf die lange Bank geschoben wird, um die unter datenschutzrechtlichen Gesichtspunkten unproblematischen und aus meiner Erfahrung zum Teil verständlichen Anliegen der Familienforschung angemessen berücksichtigen zu können.

3.6.3 Datenschutz für Gastgeber ausländischer Besucher

Ein Petent informierte mich darüber, daß die Ausländerbehörde für die Erteilung einer Aufenthaltsgenehmigung für einen ausländischen Besucher von ihm die Offenlegung seiner wirtschaftlichen Verhältnisse verlangte. So sollte er neben seinem Einkommen aus Erwerbstätigkeit Name und Anschrift des Arbeitgebers, sonstige Einkünfte, monatliche Belastungen und Angaben über die zum Haushalt gehörenden Personen machen. Dies löste bei ihm Verwunderung aus, da bisher eine einfache Erklärung nach § 84 Ausländergesetz (AuslG) genügte, daß er für die mit dem Besuch anfallenden Kosten aufkommen werde.

Ich habe gegenüber der Ausländerbehörde kritisiert, daß sie Daten erhebt, die für die Bonitätsprüfung nicht erforderlich sind, und daß ein Hinweis auf die Rechtsgrundlagen beziehungsweise die Freiwilligkeit der Angaben fehlt. Die Ausländerbehörde berief sich in ihrer Stellungnahme auf die Hinweise der Fachaufsichtsbehörde. Daher habe ich meine Bedenken auch dem Innenministerium dargelegt und die landesweite Praxis erfragt. Das Innenministerium teilte mir dazu mit, daß zwischenzeitlich mit Erlaß vom 13. November 1996 ein bundeseinheitliches,

weitgehend fälschungssicheres Formular für Verpflichtungserklärungen nach § 84 AuslG in Mecklenburg-Vorpommern eingeführt wurde, das die ursprünglich von den Ausländerbehörden benutzten Vordrucke abgelöst hat. In dem neuen Formular werden die für die Bonitätsprüfung erhobenen Daten aufgenommen. Das Original der Erklärung erhält der Gastgeber und leitet es an seinen ausländischen Gast weiter, damit dieser die Unterlagen der Auslandsvertretung vorlegen kann.

Gegen die Verwendung dieses Vordruckes und das Verfahren habe ich gegenüber dem Innenministerium unseres Landes folgende Bedenken geltend gemacht:

- Für die Erteilung eines Visums für Besuchszwecke eines ausländischen Gastes wird eine Verpflichtungserklärung des Gastgebers nach § 84 AuslG verlangt. Eine Aufenthaltsgenehmigung wird regelmäßig dann versagt, wenn der ausländische Besucher seinen Lebensunterhalt einschließlich Krankenversicherungsschutz nicht aus eigenen Mitteln, Unterhaltsleistungen Dritter etc. bestreiten kann. Vor Abgabe einer Verpflichtungserklärung wird die Bonität des Erklärenden geprüft. Der Umfang der zu erhebenden Daten hat sich am konkreten Zweck zu orientieren. Die Fragen nach dem Beruf, zum Arbeitgeber, zur Wohnung (Größe, Eigentum oder Miete) sowie sonstigen Angaben zu Wohn-, Einkommens- und Vermögensverhältnissen sind zu weitgehend beziehungsweise zu unbestimmt und in diesem Zusammenhang nicht erforderlich. Für die Aufgabenerfüllung der Ausländerbehörde genügt es festzustellen, daß der Gastgeber über ausreichend Mittel verfügt, um für die anfallenden Kosten zu haften. Dazu genügt in der Regel die Vorlage eines entsprechenden Nachweises. Die Ausländerbehörde dokumentiert dies in einem Aktenvermerk. Eine weitere Aufbewahrung der entsprechenden Belege beziehungsweise etwaiger Kopien ist für diesen Zweck nicht erforderlich.

- Durch die Aufnahme dieser Daten in die Verpflichtungserklärung erhalten Dritte (Gast, Auslandsvertretung) Kenntnis über die Vermögens- und Einkommensverhältnisse des Gastgebers, ohne daß dies für die Wirksamkeit der Verpflichtungserklärung erforderlich ist. Vielmehr genügt es, wenn in der Erklärung das Prüfungsergebnis der Ausländerbehörde vermerkt wird.

– Die Verpflichtung des Betroffenen, für die Kosten des Besuches aufzukommen, bezieht sich auf den Zeitraum der Einladung. Nach Ablauf dieser Zeit sind die Unterlagen nur noch für eine Übergangszeit, etwa drei Monate, aufzubewahren, um sie für gegebenenfalls noch kommende Erstattungsansprüche öffentlicher Stellen zu nutzen.

Das Innenministerium hat meine Bedenken anerkannt und mit Erlaß vom 1. September 1997 die Ausländerbehörden des Landes angewiesen, entsprechend diesen Empfehlungen zu verfahren.

3.6.4 Allgemeine Verwaltungsvorschriften zum Ausländergesetz

Im Juli 1997 erhielt ich einen Referentenentwurf der Allgemeinen Verwaltungsvorschriften zum Ausländergesetz zur Stellungnahme. Die im Entwurf enthaltenen Regelungen, Hinweise und Erläuterungen zum Ausländergesetz, zur Durchführungsverordnung zum Ausländergesetz, zum Asylverfahrensgesetz, zu der Genfer Flüchtlingskonvention sowie zum Schengener Durchführungsabkommen sollen insbesondere den Ausländerbehörden, aber auch sonstigen mit Ausländerangelegenheiten betrauten Institutionen und Behörden die Anwendung der ausländerrechtlichen Vorschriften erleichtern. Für die Ausländerbehörden sollen sie ermessensbindenden Charakter haben, um eine bundeseinheitliche Anwendung des Ausländergesetzes zu gewährleisten.

Ein Teil der im Entwurf vorgesehenen Bestimmungen entsprach nicht den datenschutzrechtlichen Anforderungen.

- Hinsichtlich der Maßnahmen zur Identitätsprüfung von Ausländern war aus Klarstellungsgründen noch zu ergänzen, daß körperliche Untersuchungen (§ 81 a StPO) und DNA-Analysen (molekular genetische Untersuchungen - § 81 e StPO) nicht erlaubt sind.

- In Ausweisungsverfahren darf die Ausländerbehörde nur solche Verurteilungen verwerten, die im Bundeszentralregister eingetragen und noch nicht zu tilgen sind. Ich habe vorgeschlagen zu ergänzen, daß gleiches auch für länger zurückliegende Einstellungen von Strafverfahren gelten soll, sofern im Fall einer Verurteilung aller Voraussicht nach bereits Til-

gungsreife eingetreten wäre. In derartigen Fällen sollte ein Ausländer nicht strenger behandelt werden als bei einer Verurteilung.

- Zu den Pflichten eines Flughafenunternehmers gehört es, den Aufenthalt von schon bei der Einreise zurückgewiesenen Ausländern in der Unterkunft per Hausordnung zu regeln und zu überwachen. Ich hatte hierzu empfohlen, den Ausländern die Hausordnung in einer ihnen verständlichen Sprache bekanntzugeben. Die Regeln der Hausordnung dürfen die Ausländer nur insoweit in ihrer persönlichen Freiheit beschränken, als es für den Zweck der Unterbringung oder für die Ordnung auf dem Flughafen erforderlich ist.

- Im Verfahren der Bonitätsprüfung des Gastgebers eines ausländischen Besuchers sollte der Umfang der zu erhebenden Daten auf das erforderliche Minimum reduziert werden. Auf die Vorlage eines Mietvertrages könnte beispielsweise verzichtet werden (siehe dazu auch Punkt 3.6.3).

Das Innenministerium unseres Landes hat meine Empfehlungen aufgegriffen und in die Stellungnahme an das Bundesministerium des Innern mit aufgenommen.

3.7 Kommunalrecht

3.7.1 Bürgerdaten in öffentlicher Sitzung von Gemeindevertretungen

Gemeindevertreter fragen häufig an, was zu beachten ist, wenn Anträge mit personenbezogenen Daten in den Sitzungen der Gemeindevertretungbehandelt werden sollen.

Bei der Tätigkeit der Gemeindevertretung ist ein Umgang mit personenbezogenen Daten nur zulässig, soweit dieser für ihre Aufgabenerfüllung erforderlich ist. Kann eine Gemeindevertretung ohne Kenntnis personenbezogener Daten nicht sachgerecht beraten und entscheiden, so dürfen die Unterlagen diese Daten enthalten.

Der Grundsatz der Öffentlichkeit von Gemeindevertretersitzungen gemäß § 29 Abs. 5 Satz 1 Kommunalverfassung für das Land Mecklenburg-Vorpommern (KV MV) ist Ausfluß des De-

mokratieprinzips. Die Öffentlichkeit ist bei den Sitzungen grundsätzlich zugelassen und soll somit jederzeit die Möglichkeit einer „Kontrolle“ gegenüber den gewählten Vertretern haben. Das Handeln der Gemeindevertreter soll für den Bürger transparent sein. Die Öffentlichkeit ist jedoch nach § 29 Abs. 5 Satz 2 KV MV auszuschließen, wenn überwiegende Belange des öffentlichen Wohls oder berechtigte Interessen einzelner dies erfordern. Ein solches berechtigtes Interesse ist regelmäßig anzunehmen, wenn es sich um Sachverhalte handelt, die mit sensiblen personenbezogenen Daten verbunden sind, so etwa bei Personal- und Grundstücksangelegenheiten, bei Bescheiden des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR, bei Entscheidungen über Stundung beziehungsweise Erlaß von Forderungen und ebenso bei der Behandlung von Bauanträgen. In diesen Fällen hat der Betroffene ein schutzwürdiges Interesse daran, daß beispielsweise seine biographischen Daten, Vermögensverhältnisse, Grundstücksdaten und Geschäftsabsichten nicht in öffentlicher Sitzung behandelt und somit einer breiten Öffentlichkeit bekanntwerden. Im Einzelfall sind die Interessen sorgfältig zu prüfen und abzuwägen. Die oben genannten Angelegenheiten sollten grundsätzlich in nichtöffentlicher Sitzung behandelt werden.

3.7.2 Ausübung des gemeindlichen Vorkaufsrechtes

Der Käufer eines Grundstückes hat gegenüber dem Grundbuchamt unter anderem nachzuweisen, daß für das Grundstück ein gemeindliches Vorkaufsrecht nicht existiert oder nicht ausgeübt wird. Erst dann wird der Eintrag in das Grundbuch vollzogen. Zu diesem Zweck müssen die Vertragsparteien der Gemeinde den Verkauf eines Grundstückes anzeigen. Die Gemeinde prüft, ob sie ein Vorkaufsrecht hat und ob sie dieses gegebenenfalls wahrnehmen will. Besteht kein Vorkaufsrecht oder soll dieses nicht ausgeübt werden, erteilt die Gemeinde dem Antragsteller hierüber unverzüglich einen Bescheid, der zur Vorlage beim Grundbuchamt dient.

Bei der Prüfung des Vorkaufsrechtes ist der Grundsatz der Verhältnismäßigkeit zu beachten. Der Gemeinde sind deshalb nur die Daten zu übermitteln, die tatsächlich für ihre Entscheidung erforderlich sind. Bisher wurden jedoch häufig die vollständigen Verträge übersandt. Somit ist der Gemeinde in den Fällen, in denen kein Vorkaufsrecht bestand, eine Vielzahl von Daten bekanntgeworden, die sie nicht zur Aufgabenerfüllung benötigte. Weil es datenschutzrechtlich unzulässig ist, unabhängig vom Bestehen eines Vorkaufsrechtes die Übersendung des voll-

ständigen Kaufvertrages zu verlangen, habe ich mich gegen dieses Verfahren ausgesprochen. § 28 Abs. 1 Satz 1 Baugesetzbuch (BauGB) verpflichtet die Vertragsparteien lediglich, den Inhalt des Kaufvertrages mitzuteilen.

Einige Notare haben darauf hingewiesen, daß bis zu einer Entscheidung der Gemeinde unter Umständen mehrere Monate vergehen und dies zu erheblichen Verzögerungen bei der Vertragsabwicklung führen kann. Die Gemeinde darf ihr Vorkaufsrecht nur innerhalb von zwei Monaten nach Übersendung des vollständigen rechtswirksamen Kaufvertrages ausüben. Daher seien in der Vergangenheit gleich vollständige Kaufverträge an die Gemeinde gesandt worden, um so die Gemeinde zu einer schnellen Entscheidung zu bewegen. Datenschutzrechtlich ist es bedenklich, wenn Notare sich durch das zögerliche Verwaltungshandeln einer Gemeinde zu einer solchen Verfahrensweise gezwungen sehen. Die Gemeinde ist verpflichtet, in der Sache unverzüglich zu entscheiden.

Ich habe empfohlen, ein zweistufiges Verfahren zu nutzen, um so dem Recht auf informationelle Selbstbestimmung der Betroffenen einerseits und dem berechtigten Informationsinteresse der Gemeinden andererseits zu entsprechen. In einem ersten Schritt übersenden die Vertragsparteien der Gemeinde eine Veräußerungsanzeige mit den Daten, die für die Feststellung, ob für dieses Grundstück ein gemeindliches Vorkaufsrecht besteht, erforderlich sind. Existiert kein Vorkaufsrecht beziehungsweise soll ein bestehendes Vorkaufsrecht nicht wahrgenommen werden, so erteilt die Gemeinde unverzüglich ein sogenanntes Negativattest. Anderenfalls bittet sie den Notar, den vollständigen Kaufvertrag zu übersenden. Zur Verfahrensbeschleunigung kann ein von der Notarkammer erstelltes Musterformular beitragen.

Das Innenministerium beabsichtigt, hierzu einen Erlaß herauszugeben. Der Entwurf lag mir bereits vor. Ich habe dazu Stellung genommen.

3.7.3 Gebührenfestsetzung bei Einleitung von Niederschlagswasser

Die Wasser- und Abwasserzweckverbände sowie die Stadtwerke erheben Gebühren, wenn Niederschlagswasser über die öffentliche Kanalisation abgeleitet wird und dies in einer entsprechenden Satzung geregelt ist. Zu diesem Sachverhalt erhielt ich Anfragen von Bürgern.

Ein Bürger sandte mir einen „Erfassungsbogen zur Niederschlagsmengenermittlung“ zu und bat mich zu prüfen, ob die detaillierte Erhebung von Grundstücksdaten zulässig sei. Er befürchtete, daß die Stadtwerke damit ein eigenes Grundstückskataster anlegen könnten.

Für die Mengenberechnung sind Angaben über einzelne Flächen erforderlich, von denen Niederschlagswasser abgeleitet wird. Ohne daß es näher erläutert wurde, sollten aber in diesem Fall neben versiegelten Flächen auch solche für den Garten und die Außenanlagen angegeben werden. Im Formular oder einem Informationsblatt hätte darauf hingewiesen werden müssen, daß Flächen, auf denen Regenwasser üblicherweise versickert, nur dann anzugeben sind, wenn dieses Wasser von einer Drainage gesammelt und in die öffentliche Kanalisation abgeleitet wird.

Im übrigen ergab sich aus der Satzung über die Abwasserbeseitigung, daß auch solche Flächen in die Kalkulation nicht einzubeziehen sind, von denen das Niederschlagswasser vollständig für eigene Zwecke genutzt wird. Auch darauf hätte im Formular aufmerksam gemacht werden müssen.

Der datenerhebenden Stelle habe ich empfohlen, einen erklärenden Satz in den Erbebungsbogen oder in das Anschreiben aufzunehmen. Weiterhin sollten die Betroffenen, die entsprechende Angaben bereits gemacht hatten, erneut angeschrieben und auf diese Erklärung hingewiesen werden. Dies war vor allem deshalb erforderlich, weil möglicherweise Flächen angegeben worden sind, die bei sachgerechter Aufklärung nicht angegeben worden wären.

Die datenerhebende Stelle hat die Betroffenen in der erforderlichen Weise aufgeklärt und wird in den Anschreiben künftig einen entsprechenden Hinweis geben. Des weiteren wird sie zukünftig auf die Erhebung von Gartenflächen sowie Flächen für Außenanlagen gänzlich verzichten. Bei allen Betroffenen, die die Größe solcher Flächen bereits mitgeteilt hatten, wird der Gebührenbescheid entsprechend korrigiert, und sie werden darüber informiert.

In einem anderen Fall erhielt ich von einem Bürger einen Erhebungsbogen zur Prüfung, mit dem neben den Angaben zum Grundstück und zur Abwasserbeseitigung sowie Regenwasserableitung auch die Art und die Nutzung des Grundstückes erfaßt werden sollte. Beispiels-

weise wurde hier gefragt, ob das Grundstück für Wohn- oder Gewerbezwecke genutzt und welches Gewerbe gegebenenfalls betrieben wird. Darüber hinaus wurden Angaben zur Anzahl der vorhandenen und geplanten Gästebetten gefordert.

Ich habe empfohlen, den Erhebungsbogen zu ändern, so daß nunmehr nur solche Daten erhoben werden, die unmittelbar für die Abwasser- und Regenwassermengenberechnung relevant sind.

3.7.4 Grenzenlose Rechnungsprüfung?

Ein Petent wandte sich in folgender Angelegenheit an mich und bat um eine datenschutzrechtliche Bewertung:

Das Rechnungsprüfungsamt hatte bei einem Amt einer Stadt eine unvermutete Kassenbestandsaufnahme vorgenommen. Dabei wurden Verstöße gegen haushalts- und kassenrechtliche Bestimmungen, beispielsweise das Fehlen von Quittungen für Auszahlungen an Privatpersonen, Formfehler und unklare Leistungsumfänge in Verträgen, festgestellt. Das Rechnungsprüfungsamt bezweifelte die Ordnungsmäßigkeit der nachgereichten Quittungen und Belege des Amtes. Deshalb sandte es die Unterlagen an das Sozialamt der Stadt mit der Bitte, anhand der Leistungsakten zu prüfen, ob die Zahlungsempfänger auch Sozialleistungen beziehen und ob sie gegebenenfalls Nebeneinkünfte angegeben haben. Das Sozialamt veranlaßte Anhörungen der Betroffenen, bei denen auch Mitarbeiter des Rechnungsprüfungsamtes anwesend waren. Das Rechnungsprüfungsamt erhielt die Protokolle der Anhörungen, die teilweise auch sensible personenbezogene Daten der Betroffenen enthielten.

Personenbezogene Daten dürfen zum Zwecke der Rechnungsprüfung in dem dafür erforderlichen Umfang genutzt werden, soweit dies unerläßlich oder unvermeidbar ist.

Die Einbeziehung des Sozialamtes durch das Rechnungsprüfungsamt, um neue Erkenntnisse für die Rechnungsprüfung des anderen Amtes zu gewinnen, war jedoch zu weitgehend. Im Ergebnis der Rechnungsprüfung wurden zwar Unstimmigkeiten festgestellt, die im weiteren Verfahren zu klären waren. Jedoch war nicht von vornherein klar, daß es sich in allen Fällen

um Bezieher von Sozialleistungen handelte. Ferner hätte vom Sozialamt berücksichtigt werden müssen, daß die Nutzung von Sozialdaten auf Zwecke der Rechnungsprüfung beim jeweiligen Sozialleistungsträger beschränkt ist und demnach eine Nutzung für Rechnungsprüfungen bei anderen öffentlichen Stellen nicht in Frage kommt.

Der allgemeine Verdacht des Sozialleistungsmißbrauchs rechtfertigt ein solches Verfahren ebenfalls nicht. Die Übermittlung von personenbezogenen Daten an das Sozialamt, die dem Rechnungsprüfungsamt im Rahmen einer Prüfung bei einem anderen Amt zur Kenntnis gelangt sind, stellt eine Zweckdurchbrechung dar. Diese wäre nur erlaubt gewesen, wenn in konkreten Einzelfällen tatsächliche Anhaltspunkte dafür vorgelegen hätten, daß Betroffene unrichtige Angaben gemacht haben. Pauschale Überprüfungen, etwa in Form eines Datenabgleichs, sind unzulässig, da hierbei den beteiligten Ämtern eine Vielzahl von Daten Betroffener zur Kenntnis gelangt, die zu deren Aufgabenerfüllung nicht erforderlich ist. Auch Erfahrungswerte über Häufungen von Leistungsbetrug in bestimmten Bereichen genügen nicht. Vielmehr bedarf es konkreter Tatsachen in jedem Einzelfall.

In diesem Zusammenhang ist es äußerst bedenklich, bei Prüfungen einer öffentlichen Stelle festgestellte Verstöße gegen kassen- und haushaltsrechtliche Bestimmungen regelmäßig den Zahlungsempfängern zuzurechnen. Schließt eine Privatperson mit einer öffentlichen Stelle einen Vertrag, so hat die öffentliche Stelle dafür Sorge zu tragen, daß dieser und sonstige kassenbegründende Unterlagen einschließlich der Quittungen den gesetzlichen Anforderungen entsprechen. Die Tatsache, daß diesbezüglich Angaben fehlten und daher Unterlagen nachgereicht wurden, sowie die vom Rechnungsprüfungsamt allgemein in Frage gestellte Glaubwürdigkeit ließen eine Zweckdurchbrechung und somit eine Verarbeitung und Nutzung der Daten - wie in diesem Fall geschehen - nicht zu.

Der Umgang mit den Daten, insbesondere die Übermittlung zwischen dem Rechnungsprüfungsamt und dem Sozialamt der Stadt, verstößt insofern gegen datenschutzrechtliche Bestimmungen. Die Stadt hat mir mitgeteilt, daß sie meine Bedenken teilt und meiner Rechtsauffassung folgt. In einem abschließenden Gespräch konnte ich mich davon überzeugen, daß sich die betreffenden Mitarbeiter inzwischen mit den datenschutzrechtlichen Vorschriften vertraut gemacht haben und nunmehr auch für das informationelle Selbstbestimmungsrecht sensibilisiert sind.

3.8 Bau-, Wohnungs- und Liegenschaftswesen

3.8.1 Kontrolle eines Wohnungsamtes

Am 1. Januar 1996 ist das Landesbelegungsbindungsgesetz in Kraft getreten. Die Neuregelung der Belegungsbindung des im kommunalen und genossenschaftlichen Eigentum stehenden Wohnraumes hat datenschutzrechtliche Auswirkungen. Zum einen haben sich die Voraussetzungen für die Erteilung eines Wohnberechtigungsscheines und damit auch der Umfang der zu diesem Zweck zu erhebenden Daten geändert. Zum anderen sind nur noch maximal 50 % der kommunalen und genossenschaftlichen Wohnungen belegungsgebunden, so daß eine Speicherung von Mieterdaten zum Zwecke der Kontrolle der Belegungsbindung auf diese Wohnungen beschränkt ist.

Wegen der neuen Regelungen habe ich im Frühjahr 1997 den Umgang mit personenbezogenen Daten im Rahmen der Belegungsbindung in einem Wohnungsamt geprüft:

Wohnberechtigungsschein

Eine belegungsgebundene Wohnung darf einem Wohnungssuchenden grundsätzlich nur dann überlassen werden, wenn dieser vor dem Einzug im Besitz eines Wohnberechtigungsscheines ist und die darin angegebene Wohnungsgröße nicht überschritten wird. Den Wohnberechtigungsschein muß er beim Wohnungsamt beantragen.

Mit dem Antragsformular wurden neben den für die Erteilung eines Wohnberechtigungsscheines erforderlichen Daten folgende weitere Angaben des Antragstellers und seiner Familie generell erhoben:

- Erst- oder Wiederholungsantrag,
- Staatsangehörigkeiten des Antragstellers und seiner Familienmitglieder,
- Gründe für die Antragstellung,
- Telefonnummer,

– Entbindungstermin bei Schwangeren sowie
– Datum der Eheschließung bei allen Verheirateten.

Personenbezogene Daten dürfen nur erhoben werden, soweit sie zur Prüfung der sachlichen Voraussetzungen für einen Wohnberechtigungsschein erforderlich sind. Entsprechend präzise sind die Angaben des Betroffenen zu erfragen. Der Antrag muß grundsätzlich nicht begründet werden. In Abhängigkeit von der Personenzahl ist eine angemessene Wohnungsgröße zu gewähren. Wird jedoch ein zusätzlicher Raumbedarf, zum Beispiel aus beruflichen oder familiären Erfordernissen, geltend gemacht, hat der Antragsteller die Gründe darzulegen. Ebenso bedarf es einer Begründung, wenn aufgrund der Einkommensverhältnisse kein Wohnberechtigungsschein erteilt werden darf, es sich aber um einen sozialen Härtefall handelt.

Der Vordruck ist daher so zu gestalten, daß der Betroffene klar erkennen kann, welche Daten für die Prüfung der Voraussetzungen erforderlich sind. Ferner ist der Betroffene umfassend darüber aufzuklären, was mit seinen Daten geschieht und auf welcher Rechtsgrundlage die Behörde tätig wird. Das Wohnungsamt hat den Vordruck auf der Basis meiner Hinweise überarbeitet.

Die Anträge der Betroffenen wurden seit 1991 aufbewahrt und die Daten seit 1993 in automatisierten Dateien gespeichert. Eine Löschung war bis zum Zeitpunkt meiner Kontrolle nicht vorgesehen. Ein Wohnberechtigungsschein gilt für die Dauer eines Jahres. Nach Ablauf dieses Zeitraumes ist eine weitere Aufbewahrung der Unterlagen und die Speicherung der Daten in einer automatisierten Datei nicht erforderlich. Die Daten wurden inzwischen gelöscht.

Erfassen und Kontrolle der Belegungsbindung

Die Speicherung personenbezogener Daten zur Sicherung der Zweckbestimmung des belegungsgebundenen Wohnraumes ist zulässig. Jedoch dürfen hierzu nur Daten von Betroffenen gespeichert werden, die in einer solchen Wohnung leben. Zum Zeitpunkt der Kontrolle waren jedoch auch Daten von Personen gespeichert, die in einer kommunalen oder genossenschaftlichen Wohnung ohne Belegungsbindung leben. Die Verwaltung hatte es versäumt, nach der

Neufestlegung des belegungsgebundenen Wohnraumes die personenbezogenen Daten dieser Mieter zu löschen. Dies wurde umgehend nachgeholt.

Übermittlung von Einwohnermeldedatenan das Wohnungsamt

Das Wohnungsamt hatte vom Einwohnermeldeamt regelmäßig Listen mit den Daten aller verstorbenen oder weggezogenen Einwohner der Stadt mit folgenden Angaben erhalten: Name, Vorname, (alte und gegebenenfalls neue) Anschrift, Geburtsname, Staatsangehörigkeit, Geburtsdatum, Geschlecht, Geburtsort und Familienstand. Diese Daten wurden für die Prüfung von Wohngeldzahlungen und die Kontrolle der Belegungsbindung genutzt. Die Notwendigkeit der Nutzung personenbezogener Daten im Einzelfall rechtfertigt ein solches Verfahren nicht, da hier dem Wohnungsamt eine Vielzahl von Daten Betroffener zur Kenntnis gelangt, ohne daß diese zu dessen Aufgabenerfüllung erforderlich ist.

Für die Kontrolle der Belegungsbindung ist in § 14 Meldedaten-Übermittlungsverordnung des Landes Mecklenburg-Vorpommern ein Verfahren festgelegt, wonach die Meldebehörde dem Wohnungsamt Daten von in belegungsgebundenen Wohnungen lebenden Einwohnern übermitteln darf. Der Datensatz umfaßt weitaus weniger Daten, als bisher in der Liste von der Meldebehörde übermittelt wurden, und beschränkt sich auf den Personenkreis, der tatsächlich in einer solchen Wohnung lebt. Diese Datenübermittlung setzt jedoch die Kenntnis des belegungsgebundenen Wohnraumes durch die Meldebehörde voraus. Dies war zum damaligen Zeitpunkt noch nicht realisiert worden. Die Stadt ist meiner Rechtsauffassung gefolgt und verfährt nunmehr nach den geltenden Bestimmungen.

Technische und organisatorische Maßnahmen nach § 17 DSG MV

Während der Kontrolle habe ich neben Mängeln beim baulichen Datenschutz unter anderem die fehlenden Möglichkeiten einer sicheren Aufbewahrung von Akten und anderen Datenträgern sowie die Nutzung von Trivialpaßwörtern kritisiert.

Das Wohnungsamt hat meine Bedenken aufgegriffen und die erforderlichen Maßnahmen zum Schutz der personenbezogenen Daten verwirklicht.

3.8.2 Öffentliche Bauleitplanung

Eine Stadt hatte im Rahmen der Bürgerbeteiligung den Entwurf eines Bebauungsplanes öffentlich ausgelegt. Hierzu äußerte sich ein Bürger gegenüber der Stadtverwaltung schriftlich. In diesem Schreiben kritisierte er auch das von der Stadt beauftragte Planungsbüro. Er wies aber ausdrücklich darauf hin, daß seine Kritik am Planungsbüro für das Verfahren nicht relevant und lediglich für die Verwaltung bestimmt sei. Das Schreiben sollte daher nicht vollständig an das Planungsbüro weitergeleitet werden. Trotzdem übersandte die Stadt das Schreiben in ungekürzter Fassung an das Planungsbüro mit der Begründung, daß das Planungsbüro zur Mitwirkung bei der städtebaulichen Planung verpflichtet sei und deshalb auch Kenntnis von allen eingegangenen Bedenken und Anregungen erhalten müsse. Dies sei auch im Rahmen des Umganges mit personenbezogenen Daten im Auftrag nach § 4 DSG MV zulässig. Das Planungsbüro seinerseits hatte nach Kenntnis des Schreibens den Petenten unter Androhung einer Zahlung von 10.000,- DM aufgefordert, künftig solche Äußerungen zu unterlassen. Der Petent bat um eine datenschutzrechtliche Prüfung der Angelegenheit.

Die Gemeinden planen eigenverantwortlich für ihren Bereich die örtliche Bebauung und stellen hierzu Bauleitpläne auf. Im Planverfahren sind die Bürger sowie die Träger öffentlicher Belange zu beteiligen. Zu diesem Zweck sind beispielsweise die Entwürfe der Bauleitpläne öffentlich auszulegen, um den Beteiligten Gelegenheit zu geben, ihre Anregungen und Bedenken vorzubringen. Diese werden von der Stadtvertretung in öffentlicher Sitzung geprüft. Sie wägt die öffentlichen und privaten Belange gemäß § 1 Abs. 6 Baugesetzbuch (BauGB) ab und trifft eine verbindliche Entscheidung, inwieweit Bedenken und Anregungen berücksichtigt werden. Der Verwaltung obliegt es lediglich, die Beschlüsse vorzubereiten und die entsprechenden Bauleitpläne zu erarbeiten. Für diese Zwecke können auch externe Stellen, zum Beispiel Planungsbüros, hinzugezogen werden. Gehört es zu den Aufgaben des Planungsbüros, die im Ergebnis der öffentlichen Auslegung eingegangenen Stellungnahmen der Bürger für die Stadtvertretung aufzubereiten, ist - da hierbei mit personenbezogenen Daten umgegangen wird - § 4 DSG MV zu beachten.

Im vorliegenden Fall ergaben sich die Schwierigkeiten dadurch, daß die Kritik am Planungsbüro mit der Stellungnahme zum Bebauungsplanverfahren verknüpft war, jedoch nicht in die Abwägung der öffentlichen und privaten Belange nach § 1 Abs. 6 BauGB einfließen sollte. Das Recht auf informationelle Selbstbestimmung wird durch das vom Gesetzgeber vorgesehene Verfahren eingeschränkt. Der einzelne muß grundsätzlich damit rechnen, daß seine Einwände zur Vorbereitung auch dem Bauamt sowie einem eventuell beauftragten Planungsbüro in diesem Zusammenhang zur Kenntnis gelangen und von der Stadtvertretung in öffentlicher Sitzung behandelt werden. Ungeachtet dessen war in diesem atypischen Fall jedoch zu beachten, daß der Betroffene selbstbestimmend in seinem Schreiben differenziert hatte. Die Verwaltung hätte die datenschutzrechtlichen Aspekte beachten müssen und nur die Äußerungen, die den Bebauungsplanentwurf betrafen, im weiteren Verfahren nutzen und an das Planungsbüro weitergeben dürfen. So wäre sichergestellt gewesen, daß die Bedenken des Petenten in den gemeindlichen Abwägungsprozeß eingeflossen und keine darüber hinausgehenden Daten dem Planungsbüro zur Kenntnis gelangt wären. Im Zweifelsfall hätte man sich nochmals an den Petenten wenden sollen.

Das Planungsbüro hat mit der Nutzung der Daten für privatrechtliche Auseinandersetzungen gegen das Gebot der Zweckbindung verstoßen. Der Hinweis der Stadt, das Planungsbüro habe hierbei eigenmächtig gehandelt und Datenschutzvorschriften verletzt, trifft zwar zu, entläßt die Stadt jedoch nicht aus ihrer datenschutzrechtlichen Verantwortung. Als Auftraggeber ist sie in jedem Fall für die Einhaltung der datenschutzrechtlichen Bestimmungen zuständig. Deshalb hätte sie auch die weiteren Voraussetzungen für den Umgang mit personenbezogenen Daten im Auftrag nach § 4 DSG MV schaffen müssen. So wäre der Auftragnehmer unter anderem auf das Datengeheimnis nach §5 DSG MV zu verpflichten gewesen.

Den Petenten habe ich über diesen Sachverhalt informiert. Die Stadt hat versichert, künftig den gesetzlichen Bestimmungen entsprechend zu verfahren.

In einem anderen Fall hatte ein Bürgermeister allen Gemeindevertretern in Vorbereitung der Abwägung der öffentlichen und privaten Belange nach § 1 Abs. 6 BauGB die erforderlichen Sitzungsunterlagen übersandt. In der Anlage befand sich auch eine Namenliste der Bürger, die Einwände gegen den Entwurf des Bebauungsplanes geltend gemacht hatten. Ein Gemeindevertreter war wegen Befangenheit gemäß § 24 Kommunalverfassung Mecklenburg-Vorpommern

von der Mitwirkung ausgeschlossen. Dieser Gemeindevertreter setzte sich mit einigen Einwohnern in Verbindung, um mit ihnen über ihre Beweggründe für die Einwände zu diskutieren. Ein Petent äußerte Bedenken gegen die Übersendung der Liste an den befangenen Gemeindevertreter sowie dessen anschließendes Auftreten.

Die Unterlagen werden der Gemeindevertretung zweckgebunden für die Beratung und Entscheidung im Rahmen der Abwägung der öffentlichen und privaten Belange übersandt. Soweit ein Gemeindevertreter als befangen gilt, hat er diese Tatsache unaufgefordert gegenüber dem Vorsitzenden der Gemeindevertretung anzuzeigen. Dies hat für ihn zur Folge, daß weder eine beratende noch eine entscheidende Mitwirkung oder ein sonstiges Tätigwerden in diesem Verfahren zulässig ist.

Hat ein Gemeindevertreter seine Befangenheit mitgeteilt, ist es aus datenschutzrechtlicher Sicht nicht notwendig, ihm Sitzungsunterlagen mit personenbezogenen Daten zu übersenden. Da der betroffene Gemeindevertreter im vorliegenden Fall dem Mitwirkungsverbot unterlag, war ein Umgang mit personenbezogenen Daten in der Sache durch ihn nicht erforderlich. Das Mitwirkungsverbot steht einer weiteren Verarbeitung und Nutzung personenbezogener Daten durch den befangenen Gemeindevertreter entgegen. Er hätte somit auf jeden Fall nicht in der beschriebenen Art und Weise tätig werden dürfen. Der Bürgermeister der Gemeinde hatte, nachdem ihm dies ein betroffener Bürger zur Kenntnis gab, den Gemeindevertreter aufgefordert, dies unverzüglich zu unterlassen. Ergänzend hierzu habe ich dem Bürgermeister empfohlen, in der Gemeindevertretung auf die datenschutzrechtlichen Aspekte hinzuweisen, um künftig ähnliche Fälle auszuschließen.

Wegen der grundsätzlichen Bedeutung dieser Frage habe ich die Kommunalaufsicht informiert.

3.9 Statistik

3.9.1 EU-Volkszählung 2001

Für das Jahr 2001 ist in der Europäischen Union (EU) eine Volks- und Wohnungszählung vorgesehen. Dazu existiert bereits ein Vorschlag für eine Verordnung der EU. Tritt diese Verordnung in Kraft, so gilt sie unmittelbar in jedem Mitgliedstaat. Alle nationalen Behörden haben

sie zu beachten und zu vollziehen. Der Verordnungsvorschlag sieht in seinem Artikel 1 - Allgemeine Bestimmungen und Referenzzeitraum - vor:

„Die Mitgliedstaaten und die Kommission, jeweils innerhalb ihres Kompetenzbereichs handelnd, erstellen auf der Grundlage einer allgemeinen Zählung der Bevölkerung und der Wohnungen gemeinschaftliche Statistiken. Diese Zählungen werden an einem zwischen dem 1. März und dem 31. Mai 2001 liegenden Referenzdatum durchgeführt. (Erhebung 2001)."

Unter anderem sollen folgende personenbezogene Daten erfaßt werden:

- Aufenthaltsort,
- genaues Geburtsdatum,
- Art der Erwerbstätigkeit,
- Stellung im Beruf,
- Niveau der erfolgreich abgeschlossenen Bildung,
- Besitzverhältnisse an Wohnungen.

Diese Merkmale gehen teilweise über die Daten hinaus, die für die in der Bundesrepublik 1987 durchgeführte Volkszählung gesammelt wurden.

Die Bundesregierung hat sich wegen der sehr hohen zu erwartenden Kosten und der Vorgabe, statistische Vorhaben auf den unbedingt notwendigen Umfang zu reduzieren, gegen die geplante Zählung ausgesprochen. Da jedoch die Kommission und die anderen Mitgliedstaaten dem Vorhaben positiv gegenüberstehen, ist es wahrscheinlich, daß eine Verordnung zur Volkszählung 2001 verabschiedet wird. Es wäre aber auch möglich, daß der Verordnungsvorschlag nicht weiter verfolgt wird. Die Bundesregierung sucht nun nach kostengünstigen Alternativen zu den aufwendigen Haushaltsbefragungen.

Im Oktober 1996 hat das Bundesministerium des Innern (BMI) eine Problemskizze entworfen, in der drei Bereiche angesprochen werden:

1. Nutzung der Melderegister für statistische Zwecke,
2. Bereinigung der Melderegister zur besseren Nutzbarkeit,

3. Erweiterung der Melderegister um diejenigen Daten, die für die EU-Zählung benötigt werden.

Die Innenministerien der Länder wurden gebeten, gemeinsam diese Punkte zu erörtern. Gegenüber unserem Innenministerium habe ich eine Stellungnahme zu der Problemskizze mit folgenden Schwerpunkten abgegeben:

Zu 1.: Die Nutzung des Datenbestandes der Melderegister (der den Meldebehörden amtlich bekanntgewordenen Daten) für statistische Zwecke durch das Statistische Landesamt - als die für Mecklenburg-Vorpommern zuständige „Sammelstelle“ für EU- und Bundesstatistiken - ist zulässig, wenn dafür eine entsprechende Rechtsverordnung geschaffen wird.

Zu 2.: Eine Melderegisterbereinigung bedingt den Umgang mit personenbezogenen Daten. Die Meldebehörden sind nach dem Landesmeldegesetz verpflichtet, die Melderegister von Amts wegen oder auf Antrag eines Betroffenen im Rahmen des Verwaltungsvollzugs zu bereinigen. Eine darüber hinausgehende Verpflichtung zur Melderegisterbereinigung allein darauf zu stützen, daß die bereinigten Daten für künftige, etwa alle zehn Jahre stattfindende Zensen gebraucht würden, weil eine Volkszählung im Wege einer Vollerhebung politisch nicht durchsetzbar erscheint, läßt Zweifel an der Erforderlichkeit und damit an der datenschutzrechtlichen Zulässigkeit aufkommen.

Zu 3.: Die Melderegister sollen um Angaben zu Haushalt, Erwerbstätigkeit, Schulbildung sowie Pendlerverhalten ergänzt werden. Die Erweiterung der Melderegister um solche personenbezogenen Daten, die dem Meldewesen systemfremd sind, trägt tendenziell dazu bei, eine umfangreiche Datensammlung über jeden einzelnen Bürger zu realisieren, und es wäre somit möglich, Persönlichkeitsprofile zu bilden. Allein politische Gründe oder die zu erwartenden Kosten vermögen einen solch schweren Eingriff in das Recht auf informationelle Selbstbestimmung nicht zu rechtfertigen.

Darüber hinaus würde die in Betracht gezogene Melderegistererweiterung das Prinzip der Trennung von Statistik und Verwaltungsvollzug verletzen. Denn die Erhebung dieser zusätzlichen personenbezogenen Daten darf nach dem Volkszählungsurteil und den

Statistikgesetzen nur durch die Statistikämter oder abgeschottete Statistikstellen erfolgen, nicht jedoch durch Stellen des Verwaltungsvollzugs. Da die Meldebehörden jedoch Stellen des Verwaltungsvollzugs sind, ist eine solche Erweiterung des Melderegisters auch in statistikrechtlicher Hinsicht unzulässig.

Wenn man wie das BMI von einer Vollerhebung für eine Volkszählung absehen will, bleibt nach meiner Auffassung aus datenschutz- und statistikrechtlicher Sicht nur die Möglichkeit zu versuchen, die statistische Nutzung der Melderegister in ihrer derzeitigen Gestalt mit der ständig laufenden einprozentigen Stichprobe nach dem Mikrozensusgesetz in zusammengefaßter Form zu kombinieren.

Derzeit gibt es Überlegungen, neben dem Melderegister weitere bereits bestehende Datenbestände zu nutzen und eine Befragung der Gebäudeeigentümer durchzuführen. Da alle dabei anfallenden Daten personenbezogen verknüpft werden sollen, gibt es auch gegen diese Erwägungen Bedenken. Nunmehr ist abzuwarten, welche konkreten Vorgehensweisen von Seiten des BMI vorgeschlagen werden.

3.9.2 Kommunalstatistiken ohne Auskunftspflicht

Einige Kommunen haben im Berichtszeitraum zu verschiedenen Themen Befragungen der Bevölkerung durchgeführt. So wurde beispielsweise um freiwillige Beantwortung von Fragen zur Wohnsituation oder zur Naherholung gebeten. Oftmals wurde dabei der statistische Bezug des Vorhabens und damit auch die Geltung des Landesstatistikgesetzes übersehen, welches wichtige Vorschriften zum Schutz personenbezogener Daten enthält. Ein solcher, datenschutzrechtlich relevanter Bezug ist gegeben, wenn zwar als Ergebnis nicht-personenbezogene Informationen benötigt werden, diese aber durch die Erhebung personenbezogener Daten gewonnen werden sollen.

Im Rahmen einer Sitzung mit den behördlichen Datenschutzbeauftragten der Landkreise und der kreisfreien Städte habe ich hierfür folgende Empfehlungen gegeben:

1. Allgemeine Voraussetzungen

- Die Erhebung personenbezogener Daten muß erforderlich sein. Dies ist nicht der Fall, wenn die benötigten Angaben vom Statistischen Landesamt zur Verfügung gestellt oder aus öffentlichen Quellen gewonnen werden können.
- Es muß eine kommunale Statistikstelle vorhanden sein, die räumlich und personell von den anderen Verwaltungsstellen abgeschottet ist.
- Inhalt, Zeitraum, betroffener Personenkreis sowie Art und Weise der Befragung müssen durch Satzung oder Anordnung des (Ober-)Bürgermeisters oder des Landrates geregelt werden.
- Die Vergabe statistischer Arbeiten an private oder öffentliche Stellen ist nur unter den folgenden Voraussetzungen möglich:
  (-) Eignung des Auftragnehmers,
  (-) Einhaltung aller für die Erhebungsstellen geltenden Rechtsvorschriften,
  (-) schriftliche Auftragserteilung und Anzeige der Beauftragung beim Landesbeauftragten für den Datenschutz,
  (-) bei privaten Stellen: Verbot der Unterbeauftragung und Pflicht zur Unterwerfung unter die Kontrolle des Landesdatenschutzbeauftragten.

2. Der Fragebogen

- Es sind nur Fragen aufzunehmen, die für die Aufgabenerfüllung erforderlich sind.
- Zur Beantwortung sollten - möglichst grobe - anzukreuzende Kategorien vorgegeben werden. Nur in Ausnahmefällen kommen Textfelder in Betracht.
- Der Fragebogen darf keinen Platz für Adreßangaben des Befragten oder des Interviewers sowie für Bemerkungen des Interviewers vorsehen.

3. Auswahl des zu befragenden Personenkreises

- Es ist festzulegen, wie viele Anworten aus dem Personenkreis vorliegen müssen, damit die Ergebnisse aussagekräftig sind.

- Unter Berücksichtigung des zu erwartenden Rücklaufprozentsatzes ist zu entscheiden, wie viele Adressen benötigt werden, um die oben bestimmte Zahl an Antworten zu erreichen.
- Die Stelle, der die entsprechenden Adressen des für die Befragung relevanten Personenkreisese vorliegen (Adreßstelle) - meist das Einwohnermeldeamt -, wählt daraus per Zufallsverfahren die anzuschreibenden Personen aus.

4. Vorbereitung der Befragung

- Die anzuschreibenden Personen sind ausführlich über die Befragung zu unterrichten, insbesondere darüber, daß die Teilnahme an der Befragung sowie die Beantwortung jeder einzelnen Frage freiwillig ist. Die Adreßstelle verschickt dazu Informationsmaterial, ein Antwortformular und ein Anschreiben, das etwa folgenden Passus enthält:

  „Wenn Sie an der Befragung teilnehmen möchten, kreuzen Sie bitte auf dem beiliegenden Antwortformular an, ob Sie schriftlich oder einem Interviewer gegenüber antworten möchten, und schicken Sie das Formular im ebenfalls beiliegenden Freiumschlag innerhalb von zwei Wochen an die kommunale Statistikstelle (Anschrift ist vorgedruckt)."

  Die zu versendenden Unterlagen hat die Adreßstelle zuvor von der zuständigen Fachbehörde oder der kommunalen Statistikstelle erhalten.
- Die Interviewer (Erhebungsbeauftragten) müssen sorgfältig ausgewählt werden. Als Interviewer darf nicht eingesetzt werden, bei wem unter anderem aufgrund seines Berufes, etwa Makler, zu befürchten ist, daß er die erhaltenen Informationen anderweitig verwendet. Die Interviewer sind schriftlich auf die Wahrung der statistischen Geheimhaltung und auf die Einhaltung des Datengeheimnisses zu verpflichten.

5. Durchführung der Befragung

- Die Personen, welche schriftlich antworten möchten, erhalten den Fragebogen mit dem Hinweis, weder auf ihm noch auf dem Rückumschlag ihre Adresse zu schreiben.
- Die Personen, welche mündlich antworten möchten, werden von einem Interviewer befragt, der sich auszuweisen hat und den Zweck sowie die Freiwilligkeit der Befragung erläutert.

6. Auswertung

- Die kommunale Statistikstelle wertet die Fragebögen statistisch aus und vernichtet sie anschließend, um eine gegebenenfalls mögliche Reidentifizierung zu verhindern.
- Sie übermittelt nur die zusammengefaßten Ergebnisse, getrennt nach jeder einzelnen Frage, an die fachlich zuständige Stelle. Eine Ausnahme kann bei Fragen gemacht werden, die sich direkt auf das Ergebnis der vorangehenden Frage beziehen.
- Die empfangende Stelle wertet die Ergebnisse fachlich aus.

In den Abschnitten 3 bis 5 wird das datenschutzfreundliche Adreßmittlungsverfahren angewandt. So wird erreicht, daß die kommunale Statistikstelle nur Kenntnis von Daten derjenigen Personen erhält, die an der Befragung teilnehmen möchten. Falls andere Methoden zur Durchführung der Erhebung eingesetzt werden sollen, muß sorgfältig geprüft werden, in welchen der vorstehenden Punkte es zu einer Aufweichung des Schutzes personenbezogener Daten kommt und ob diese Einschränkungen des Rechts auf informationelle Selbstbestimmung gerechtfertigt werden können.

Beabsichtigt eine Kommune, Personenbefragungen durchzuführen, sollte sie möglichst frühzeitig unter Berücksichtigung der oben genannten Empfehlungen mit der datenschutzgerechten Gestaltung des Verfahrens beginnen.

3.10 Telekommunikation

3.10.1 Die ISDN-Datenschutzrichtlinie der Europäischen Union

Nachdem 1990 ein erster Entwurf vorgelegt worden war, ist im Dezember 1997 nach mehr als sieben Jahren die „Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, insbesondere im Diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in digitalen Mobilfunknetzen“ (ISDN-Richtlinie) verabschiedet worden. Die ersten Entwürfe der ISDN-Richtlinie waren noch auf digitale Telekommunikations(TK)-Netze beschränkt. Daher

rührt auch diese allgemein übliche Kurzform. Die Richtlinie gilt jetzt jedoch für den gesamten Bereich der Telekommunikation. Dies ergibt sich schon aus ihrer oben aufgeführten vollständigen Bezeichnung. Die ISDN-Richtlinie ist die erste und bisher einzige bereichsspezifische europäische Datenschutzrichtlinie, welche die allgemeine EU-Datenschutzrichtlinie konkretisiert und ergänzt. Die Mitgliedstaaten der Europäischen Union sind verpflichtet, die Vorgaben der ISDN-Richtlinie wie die EU-Datenschutzrichtlinie (siehe Punkt 2.4) bis zum 24. Oktober 1998 umzusetzen. Auch auf das deutsche TK-Recht wird die ISDN-Richtlinie Auswirkungen haben. Vor allem bei der TK-Datenschutzverordnung (siehe Punkt 3.10.4) ist sie zu berücksichtigen.

Die wichtigsten Regelungen der ISDN-Richtlinie sind:

- Ziel und Geltungsbereich: Die Richtlinie dient der Schaffung eines gemeinschaftsweit gleichwertigen Schutzes der Grundrechte hinsichtlich personenbezogener TK-Daten, insbesondere des Rechts auf Privatsphäre. Neben dem TK-Bereich gilt sie auch für das interaktive Fernsehen und Video auf Abruf (Video on demand). Behörden- und unternehmensinterne Netze sind zwar nicht erfaßt, jedoch wurde vereinbart, daß jeder Mitgliedstaat die Bestimmungen der Richtlinie auch auf nicht-öffentliche TK-Netze und auf nicht öffentlich zugängliche TK-Dienste anwenden kann.

- Sicherheit: TK-Unternehmer müssen technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der TK-Dienste und -Netze ergreifen. Die in früheren Entwürfen enthaltene Verpflichtung zum Anbieten von Verfahren zur Gesprächsverschlüsselung findet sich leider nicht mehr im verabschiedeten Richtlinientext. Besteht ein besonderes Risiko der Verletzung der Netzsicherheit, so muß der Teilnehmer darüber und über mögliche Abhilfen einschließlich deren Kosten unterrichtet werden.

- Vertraulichkeit: Die Mitgliedstaaten müssen die Vertraulichkeit der Telekommunikation gewährleisten. Sie haben insbesondere das unbefugte Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens der Telekommunikation zu untersagen.

- Verkehrs- und Gebührendaten: Verkehrsdaten sind nach Verbindungsende zu löschen oder zu anonymisieren. Gebührendaten dürfen nur mit Einwilligung des TK-Teilnehmers zu Vermarktungszwecken verwendet werden.

- Rufnummernanzeige: Neu für das deutsche TK-Recht (siehe hierzu TK-Datenschutzverordnung Punkt 3.10.4) ist, daß dem Angerufenen eingeräumt werden muß, die Anzeige seiner Nummer beim Anrufer sowie die Anzeige der Rufnummer des Anrufers bei ihm zu unterdrücken und eingehende Anrufe bei vom Anrufer unterdrückter Rufnummernanzeige abzuweisen.

- Anrufweiterschaltung: Jeder Teilnehmer muß die automatische Anrufweiterschaltung auf sein Endgerät gebührenfrei ablehnen können.

- Direktmarketing: Das Senden von Telefaxen mit Werbung ist nur bei vorheriger Einwilligung des empfangenden Teilnehmers erlaubt. Unerbetene Anrufe dürfen die Mitgliedstaaten nur zulassen, wenn die Angerufenen eingewilligt oder zumindest nicht widersprochen haben.

Mit den notwendigen Anpassungen des TK-Rechts an die Forderungen der ISDN-Richtlinie muß umgehend begonnen werden, damit die oben genannte Umsetzungsfrist bis zum 24. Oktober 1998 eingehalten werden kann.

3.10.2 Das Telekommunikationsgesetz

Am 1. August 1996 ist das Telekommunikationsgesetz (TKG) in Kraft getreten. Es schließt die Liberalisierung im Bereich der Telekommunikation (TK) ab und schafft die Voraussetzungen, um die Entwicklung der Telekommunikation von einer staatlichen Versorgungsleistung zu einem im wesentlichen den Gesetzen des Marktes unterliegenden Dienstleistungsangebot privater Unternehmen zu Ende zu bringen.

Das TKG sieht für den freien Wettbewerb im TK-Bereich allerdings eine staatliche Regulierung vor, deren wichtigste Ziele folgende sind:

- Wahrung der Interessen der TK-Teilnehmersowie des Fernmeldegeheimnisses,
- Gewährleistung eines chancengleichen und funktionsfähigen Wettbewerbs,
- Sicherstellung einer flächendeckenden und bezahlbaren TK-Grundversorgung
- Wahrung der Belange der öffentlichen Sicherheit

Darüber hinaus enthält das TKG auch die zentralen datenschutzrelevanten Bestimmungen für den TK-Bereich. Die für den Datenschutz wichtigsten Aspekte des TKG sind:

- Der Begriff Telekommunikation ist sehr weit definiert. Eine eindeutige Abgrenzung zu den Multimedia-Diensten ist nicht ohne weiteres möglich. Die Geltungsbereiche des TKG einerseits und des Teledienstegesetzes (TDG) sowie des Teledienstedatenschutzgesetzes (TDDSG) andererseits fließen ineinander über. Bei verschiedenen Diensten ist nicht klar, für wen welche Datenschutzbestimmungen gelten. Der Kooperationskreis IuK-Datenschutz (siehe Punkt 2.2) versucht daher, den einzelnen TK-, Tele-, Medien- und rundfunkähnlichen Diensten die passenden Datenschutzbestimmungen und die zuständige Datenschutzkontrollstelle zuzuordnen.

- Wer geschäftsmäßig - nicht notwendig gewinnorientiert - TK-Dienste erbringt, ist zur Wahrung des Fernmeldegeheimnisses verpflichtet. Er darf mit TK-Daten nur insoweit umgehen, als es für die geschäftsmäßige Erbringung der TK-Dienste erforderlich ist.

- Die Bundesregierung ist verpflichtet, eine Rechtsverordnung zu erlassen, in der der Umgang mit den Daten der TK-Teilnehmer durch die TK-Diensteanbieter geregelt wird (siehe Punkt 3.10.4).

- Geschäftsmäßige TK-Diensteanbieter dürfen personenbezogene Daten, die sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erhoben haben, für Zwecke der Werbung, Kundenberatung oder Marktforschung nur verarbeiten oder nutzen, wenn der Kunde eingewilligt hat.

- Die Datenschutzkontrollstelle für alle TK-Unternehmen, für deren Tätigkeit das TKG gilt, ist grundsätzlich der Bundesbeauftragte für den Datenschutz. Öffentliche Stellen der Länder unterliegen aber weiterhin auch dann der Kontrollkompetenz der Landesbeauftragten für

den Datenschutz, wenn sie TK-Dienstleistungen anbieten; dies gilt insbesondere für behördliche Nebenstellenanlagen.

- Diensteanbieter dürfen Kundendaten in öffentliche gedruckte oder elektronische Verzeichnisse eintragen, soweit der Kunde dies beantragt hat. Bereits eingetragene Kunden haben ein Widerspruchsrecht (siehe Punkt 3.18.8).

- Geschäftsmäßige TK-Diensteanbieter müssen personenbezogene Daten, die sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erhoben haben, im Einzelfall an die Sicherheitsbehörden übermitteln, soweit sie für die Erfüllung der Aufgaben dieser Behörden erforderlich sind. Kunden und Dritten darf die Datenübermittlung nicht mitgeteilt werden.

  Kommentar: Insbesondere das absolut formulierte Verbot der Unterrichtung des Betroffenen ist meines Erachtens bedenklich, da nicht einmal eine nachträgliche Mitteilung in den Fällen vorgesehen ist, in denen die Aufgabenerfüllung durch die Unterrichtung nicht gefährdet wäre.

- Geschäftsmäßige TK-Diensteanbieter müssen Kundendateien führen, in die Name und Anschrift der Inhaber von Rufnummern und Rufnummernkontingenten aufzunehmen sind, auch wenn diese nicht in öffentliche Verzeichnisse eingetragen sind. Diese Dateien müssen von der Regulierungsbehörde jederzeit in einem von ihr vorgegebenen automatisierten Verfahren für die Sicherheitsbehörden abgerufen werden können. Die genannten Diensteanbieter müssen durch technische und organisatorische Maßnahmen sicherstellen, daß ihnen Abrufe nicht zur Kenntnis gelangen können. Eine Beschränkung der Abrufe auf konkrete Zwecke ist nicht vorgesehen.

  Kommentar: Es stellt sich die Frage, ob bei TK-Dienstleistungen, zu deren Erbringung keine personenbezogenen Daten benötigt werden, dennoch Adreßdaten des Kunden zu führen sind. Dies ist wegen des auch im TKG formulierten Grundsatzes der Erforderlichkeit für die Diensteerbringung abzulehnen.

– Betreiber von TK-Anlagen haben technische Vorkehrungen unter anderem zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten zu treffen. Es besteht eine Ermächtigung, die Umsetzung durch Rechtsverordnung zu regeln. Leider wurde von ihr bisher kein Gebrauch gemacht. Es gibt lediglich einen von der Regulierungsbehörde erstellten Katalog von Sicherheitsanforderungen, der aber Belange des Datenschutzes nur unzureichend berücksichtigt.

Es ist zu hoffen, daß im Zuge der Anpassung an die Vorgaben der ISDN-Richtlinie (siehe Punkt 3.10.1) auch

– die Begriffsdefinitionen überarbeitet,
– die Auskunftsansprüche der Sicherheitsbehörden auf das notwendige Maß beschränkt,
– Unterrichtungspflichten eingeführt,
– Klarstellungen zur Gewährleistung anonymer Nutzungen getroffen und
– bei den Sicherheitsanforderungen auch die nötigen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung einbezogen

werden.

3.10.3 Das Begleitgesetz zum Telekommunikationsgesetz

Das Begleitgesetz zum Telekommunikationsgesetz (siehe Punkt 3.10.2) schafft die Voraussetzungen zur Umsetzung der Vorschriften des TKG und paßt Regelungen des Bundesrechts an das TKG an. Es ist wie das Informations- und Kommunikationsdienste-Gesetz (IuKDG) ein Artikelgesetz (siehe dazu Punkt 2.2). In seinem ersten Teil regelt das TKG-Begleitgesetz die personalrechtlichen Erfordernisse für die Errichtung der Regulierungsbehörde, die zum 1. Januar 1998 ihre Arbeit aufnehmen soll, sowie für die Auflösung des Bundesministeriums für Post und Telekommunikation zum Ende des Jahres 1997. Der zweite Teil ändert zahlreiche Vorschriften des Bundes, zum Beispiel das Bundesdatenschutzgesetz, das Gesetz zu Artikel 10 Grundgesetz und die Strafprozeßordnung (StPO). Damit werden einerseits begriffliche Unstimmigkeiten ausgeräumt, andererseits wird auch die materielle Rechtslage verändert, beispielsweise werden die Strafvorschriften erweitert.

Gegenüber der Landesregierung habe ich im Entwurfsstadium des Gesetzes zu verschiedenen datenschutzrelevanten Normen Stellung genommen. Die meisten der von meinen Amtskollegen und mir kritisierten Vorschriften sind in das nunmehr geltende Gesetz nicht übernommen worden, darunter auch die beiden folgenden Regelungsvorschläge:

- Eine Befugnisnorm zur Erfassung der von den Mobiltelefonen abgegebenen Aktivmeldungen zur Standortermittlung und Bildung von Bewegungsprofilen ist von der Bundesregierung abgelehnt worden, da die Untersuchungen zur Erforderlichkeit einer solchen Vorschrift noch nicht abgeschlossen sind.

- Eine vom Bundesrat vorgeschlagene Ermächtigung für die Sicherheitsbehörden zur Ermittlung von Rufnummern mit neuartigen Abhörgeräten (ausführlich dazu Punkt 3.20.1) hat ebenfalls keinen Eingang in das TKG-Begleitgesetz gefunden.

Negativ ist zu vermerken, daß es nicht zu der geplanten und auch dringend nötigen Ablösung des § 12 Fernmeldeanlagengesetz (FAG) kam. Nach dieser Vorschrift können Gerichte und Staatsanwaltschaften in jeder strafgerichtlichen Untersuchung Auskunft über Verbindungsdaten verlangen. Im Gegensatz zu § 100a StPO, der die Überwachung der Telekommunikation, also der Inhaltsdaten, im Strafverfahren regelt, sind die Auskunftsrechte des § 12 FAG nicht auf einen Katalog schwerwiegender Straftaten beschränkt. Dies ist vor allem deshalb besonders bedenklich, weil die Information darüber, mit welchen Personen man Gespräche geführt hat, oft wichtiger sein kann als der Inhalt dieser Gespräche. Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb schon im März 1994 in einer Entschließung die längst überfällige Änderung der Regelungen des § 12 FAG angemahnt (siehe Zweiter Tätigkeitsbericht, 4. Anlage). Daß nun auch das TKG-Begleitgesetz den § 12 FAG nicht durch eine datenschutzgerechtere Auskunftsregelung ersetzt, ist bedauerlich. Es bleibt zu hoffen, daß die Aufforderung des Bundestags-Innenausschusses an die Bundesregierung, bis spätestens April 1998 eine Regelung zur Ablösung des § 12 FAG zu finden, auch umgesetzt wird und die Anforderungen an die Auskunftserteilung über die Verbindungsdaten konkretisiert und erhöht werden. Als Ersatz für den § 12 FAG ist die Einfügung eines § 99a in die StPO geplant.

3.10.4 Die Telekommunikationsdienstunternehmen-Datenschutzverordnung

Maßgeblich für den Datenschutz in der Telekommunikation waren bis Mitte 1996 die für die Deutsche Telekom geltende Telekom-Datenschutzverordnung und die auf die privaten TK-Unternehmer anzuwendende Teledienstunternehmen-Datenschutzverordnung (UDSV). Diese beiden Vorschriften wurden durch die im Juli 1996 in Kraft getretene Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV) ersetzt. Aber auch das seit August 1996 geltende TKG (siehe Punkt 3.10.2) enthält zentrale Datenschutzbestimmungen. Dies führt einerseits dazu, daß für denselben Sachverhalt unterschiedliche Regelungen bestehen. Zum Beispiel können Bestandsdaten der Kunden nach dem TKG nur mit deren Einwilligung für Werbung des TK-Unternehmers genutzt werden, wohingegen die TDSV lediglich ein Widerspruchsrecht der Kunden vorsieht. Andererseits unterscheiden sich auch die Anwendungsbereiche der beiden Regelungswerke. So gilt das TKG auch für sogenannte Corporate Networks, also behörden- und unternehmensinterne Netze, und Nebenstellenanlagen, sofern sie von den Beschäftigten privat genutzt werden dürfen, während die TDSV diese TK-Netze ausdrücklich von ihrem Geltungsbereich ausschließt. Bei Problemen, die sich aus dem Verhältnis von TKG und TDSV ergeben, ist jeweils die für den Kunden, also für den Betroffenen, günstigere Regelung anzuwenden. Im Jahr 1998 werden diese Schwierigkeiten ausgeräumt sein, da dann die Bundesregierung aufgrund der Verpflichtung des TKG eine Rechtsverordnung zum Datenschutz im TK-Bereich erlassen wird, deren Anwendungsbereich mit dem TKG identisch ist und die die TDSV ablöst. Um die Vorgaben der mittlerweile verabschiedeten EU-ISDN-Richtlinie (siehe Punkt 3.10.1) mit berücksichtigen zu können, wurde mit dem Erlaß der Rechtsverordnung gewartet.

Die TDSV enthält folgende wichtige Regelungen:

- Die Diensteanbieter sind verpflichtet, ihre Kunden über den Umgang mit deren Daten und über besondere Gefährdungen der Netzsicherheit durch unbefugte Eingriffe Dritter zu unterrichten.

- Alle für die Entgeltberechnung nicht benötigten Verbindungsdaten sind unverzüglich zu löschen. Die übrigen Daten dürfen unter Kürzung der Zielrufnummer um die letzten drei Ziffern bis zu achtzig Tage nach Rechnungsversand gespeichert werden. Auf Verlangen des

Teilnehmers sind die Daten vollständig zu speichern oder spätestens mit Versendung der Rechnung vollständig zu löschen.

- Der Kunde kann gegen Entgelt einen Einzelverbindungsnachweis verlangen. Schwangerschafts-, Gesundheits- und Familienberatungsstellen, die Telefonseelsorge sowie vergleichbare Institutionen können beantragen, daß Verbindungen zu Telefonanschlüssen ihrer Mitarbeiter auf Einzelverbindungsnachweisen nicht herausgelesen werden können.

- Bietet der TK-Unternehmer dem Angerufenen die Anzeige der Telefonnummer des Anrufers an, so muß er diesem kostenlos die Wahl einräumen zwischen dauerndem Ausschluß der Anzeige, fallweisem Ausschluß der Anzeige - soweit technisch möglich - oder ständiger Anzeige. Der Kunde kann kostenfrei einen Anschluß beantragen, bei dem die Rufnummernanzeige eingehender Verbindungswünsche ausgeschlossen ist. Er kann verlangen, daß dieser Anschluß im Teilnehmerverzeichnis entsprechend gekennzeichnet wird.

- Bei Polizei, Feuerwehr und vergleichbaren Einrichtungen, die Notrufe bearbeiten, haben die Diensteanbieter sicherzustellen, daß die Rufnummernanzeige nicht ausgeschlossen wird.

- Bietet der TK-Unternehmer die Option der Anrufweiterschaltung an, so muß er dem Inhaber des Anschlusses, an den weitergeleitet werden soll, die Möglichkeit gewährleisten, dies zu unterbinden. Eine Anrufweiterschaltung muß dem Anrufer mitgeteilt werden, soweit dies technisch möglich ist.

- Der Kunde, der nur in bestimmten Kundenverzeichnissen erscheinen will, beispielsweise in gedruckten, aber nicht in elektronischen Teilnehmerverzeichnissen, kann beantragen, daß die Eintragung seiner Daten gesondert gekennzeichnet wird (siehe auch Punkt 3.18.8).

- Hat der Teilnehmer der Eintragung in das Kundenverzeichnis widersprochen, darf keine Rufnummernauskunft erteilt werden, sofern er nichts Gegenteiliges erklärt hat.

Es ist davon auszugehen, daß die meisten der oben stehenden Regelungen auch in die aufgrund des TKG zu erlassende Rechtsverordnung übernommen werden.

Bei der Umsetzung der TDSV gibt es verschiedene Probleme, von denen im folgenden einige zusammen mit den Wertungen und Empfehlungen der Datenschutzbeauftragten dargestellt werden:

- Bis auf die oben genannten Institutionen können die Kunden der Aufnahme ihrer Rufnummer in den Einzelverbindungsnachweis desjenigen, der sie angerufen hat, nicht widersprechen.

  Die Datenschutzbeauftragten werden sich dafür einsetzen, daß in die neue Rechtsverordnung das sogenannte Holländische Modell aufgenommen wird, wonach der Kunde ein Wahlrecht hat, ob seine Nummer auf Einzelverbindungsnachweisen erscheinen soll.

- Zielrufnummern im Ausland werden generell vollständig in Einzelverbindungsnachweise eingetragen.

  Diese Vorgehensweise steht nicht im Einklang mit der TDSV, die eine Kürzung der Rufnummern um die letzten drei Ziffern verlangt, wenn der Kunde nicht ausdrücklich die vollständige Speicherung oder Löschung der Daten wünscht.

- Die Telekom unterläßt die Kennzeichnung der Eintragungen der Kunden, die in bestimmten Verzeichnissen nicht erscheinen möchten.

  Sie hat der ihr obliegenden Kennzeichnungspflicht nachzukommen (siehe auch Punkt 3.18.8).

- Die Pflicht des Diensteanbieters, einem Kunden unter bestimmten Voraussetzungen Auskunft über die Anschlüsse zu geben, von denen er angerufen worden ist („Fangschaltung"), wurde teilweise mißbraucht, etwa um die Adresse eines Frauenhauses herauszufinden, in welchem Familienmitglieder untergebracht waren.

An den in der Regelung verlangten schlüssigen Vortrag des Auskunftsbegehrenden über ihn bedrohende oder belästigende Anrufe sowie an die Dokumentationspflicht sind einheitliche und hohe Anforderungen zu stellen.

– Die Unterrichtung des Anrufers darüber, daß sein Anruf an einen anderen Anschluß weitergeleitet wird, erfolgt auch dann, wenn der Inhaber dieses Anschlusses ebenfalls der Angerufene ist.

  Diese Mitteilung ist unnötig und beeinträchtigt das Recht auf informationelle Selbstbestimmung des Angerufenen, da der Anrufer dadurch Informationen über den Aufenthaltsort des Angerufenen erhält. Sie sollte daher unterbleiben.

– Beim Erwerb einer Mobiltelefonkarte werden teilweise Kopien von amtlichen Ausweisen des Kunden angefertigt.

  Dieses Verhalten steht eindeutig im Widerspruch zur TDSV, die dem Diensteanbieter nur das Recht auf Vorlage der Dokumente einräumt. Es ist daher sofort einzustellen.

3.11 Finanzwesen

3.11.1 Änderung der Abgabenordnung

Seit Jahren bemühen sich die Datenschutzbeauftragten um eine Anpassung der Abgabenordnung (AO) an die Datenschutzgesetzgebung. Entsprechende Änderungs- und Ergänzungsvorschläge zu dem Entwurf des Gesetzes zur Änderung der Abgabenordnung hat das Bundesministerium der Finanzen (BMF) nicht berücksichtigt (siehe Erster Tätigkeitsbericht, Punkt 2.8.1).

Im Frühjahr 1996 übermittelte der Bundesbeauftragte für den Datenschutz dem BMF den zwischen den Datenschutzbeauftragten abgestimmten Katalog aller Änderungs- und Ergänzungsvorschläge zur datenschutzrechtlichen Überarbeitung der AO. Zeitgleich haben auch die Da-

tenschutzbeauftragten der Länder den Katalog den zuständigen Ministerien zur Kenntnis zugeleitet und um Unterstützung ihres Anliegens gebeten.

Ende 1996 wurden die Vorschläge in einer Besprechung zwischen dem BMF, den für Fragen der AO zuständigen Vertretern der obersten Finanzbehörden der Länder, Vertretern des Bundesministeriums der Justiz (BMJ), dem Bundesbeauftragten für den Datenschutz sowie einem Vertreter der Landesbeauftragten für den Datenschutz erörtert. Insbesondere die Vertreter der obersten Finanzbehörden des Bundes und der Länder vertraten die Ansicht, eine Änderung der AO sei im Hinblick auf datenschutzrechtliche Belange nicht erforderlich. Die derzeitigen Regelungen seien in dieser Hinsicht ausreichend.

Zwischenzeitlich hat das BMJ zu den datenschutzrechtlichen Änderungs- und Ergänzungsvorschlägen schriftlich Stellung genommen und diese im wesentlichen abgelehnt.

Die Datenschutzbeauftragten des Bundes und der Länder werden sich auch weiterhin für die Änderung der AO einsetzen.

3.11.2 Automatisierter Abruf von Steuerdaten

Personenbezogene Daten, die dem Steuergeheimnis nach der Abgabenordnung (AO) unterliegen, dürfen nur unter den in § 30 Abs. 6 Satz 1 AO normierten Voraussetzungen in einem automatisierten Verfahren abgerufen werden. Das Bundesministerium der Finanzen (BMF) kann durch Rechtsverordnung bestimmen, welche technischen und organisatorischen Maßnahmen gegen den unbefugten Abruf der Steuerdaten zu treffen sind (§ 30 Abs. 6 Satz 2, 3 AO).

Vor diesem rechtlichen Hintergrund erarbeitete das BMF 1994 den Entwurf einer Verordnung über den automatisierten Abruf von Steuerdaten des Bundesamtes für Finanzen, der Finanzämter sowie der Gemeinden durch hierzu besonders berechtigte Amtsträger (Steuerdaten-Abruf-Verordnung). Im Rahmen der Abstimmungsgespräche zwischen dem BMF und den obersten Finanzbehörden der Länder wurde jedoch kein Konsens im Hinblick auf mögliche Regelungen für den Abruf von Steuerdaten der Gemeinden gefunden. Das BMF rückte daher zunächst von seiner Absicht ab, die erforderlichen Einzelheiten in einer Rechtsverordnung zu regeln. Es be-

absichtigt nunmehr im Einvernehmen mit den obersten Finanzbehörden der Länder, eine bundeseinheitliche Verwaltungsvorschrift, die „Steuerdaten-Abruf-Verwaltungsregelung“, zu schaffen. Dazu wurde der bisherige Verordnungsentwurf überarbeitet und an die neueren technischen Entwicklungen angepaßt. Die Verwaltungsregelung soll durch Erlasse gegenüber dem Bundesamt für Finanzen und den Finanzbehörden der Länder umgesetzt werden, regelt jedoch nicht den Abruf von Steuerdaten der Gemeinden. Das BMF beabsichtigt gleichwohl, mittelfristig ebenfalls eine einvernehmliche und einheitliche Regelung des Abrufs von Steuerdaten der Gemeinden zu erreichen.

Der Bundesbeauftragte für den Datenschutz hat in Abstimmung mit den Landesbeauftragten für den Datenschutz gegenüber dem BMF zu dem Entwurf der „Steuerdaten-Abruf-Verwaltungsregelung“ Stellung genommen. Die datenschutzrechtlichen Bedenken richten sich insbesondere gegen die Einrichtung von automatisierten Steuerdaten-Abrufverfahren durch eine Verwaltungsvorschrift. Denn mehrere Landesdatenschutzgesetze, wie auch das DSG MV, verlangen, daß automatisierte Abrufverfahren durch Rechtsverordnung geregelt werden. Die Einrichtung solcher Verfahren mittels bloßer Verwaltungsvorschriften wäre danach unzulässig. Des weiteren ist nach der Gesetzesbegründung der Erlaß der Rechtsverordnung auch nicht in das Ermessen des BMF gestellt, wie der Wortlaut des § 30 Abs. 6 Satz 2 AO vermuten läßt. Der Bundesminister der Finanzen ist nach dem Willen des Gesetzgebers vielmehr verpflichtet, eine entsprechende Verordnung zu erlassen (siehe Bundestags-Drucksache 10/1636). Überdies entspricht die Einrichtung eines automatisierten Abrufverfahrens in einer Verwaltungsvorschrift auch nicht den verfassungsrechtlichen Anforderungen.

Es bleibt nun abzuwarten, ob das BMF mit den kommunalen Spitzenverbänden eine Einigung über die Einbeziehung der Gemeinden in das automatisierte Abrufverfahren erzielt. In diesem Fall stünde dem Erlaß der geforderten Rechtsverordnung nichts mehr im Wege.

3.11.3 PROfiskal

Unter Federführung des Finanzministeriums war 1994 damit begonnen worden, das bisher im Haushalts-, Kassen- und Rechnungswesen (HKR) eingesetzte Programm durch das Softwareprodukt PROfiskal zu ersetzen. Die Aufgabe und Durchführung dieses Vorhabens, meine

Teilnahme bei der Projektgruppe sowie die bisherigen datenschutzrechtlichen Empfehlungen habe ich im Zweiten Tätigkeitsbericht, Punkt 2.17.3, dargestellt.

Mittlerweile läuft PROfiskal unter Produktionsbedingungen und wird damit zur Echtdaten-Verarbeitung eingesetzt. Während der gesamten Einführungsphase war ich beteiligt. Die folgenden Aspekte bildeten den Schwerpunkt der Beratungstätigkeit in dieser Phase.

Datenschutz- und IT-Sicherheitskonzept

Die Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) hat im Auftrag des Finanzministeriums das Datenschutz- und IT-Sicherheitskonzept entworfen. Zu diesem Konzept habe ich unter anderem folgende Hinweise gegeben:

- Im Abschnitt „IT-Einsatzanalyse“ wurden alle in PROfiskal anfallenden Daten nach ihrer Schutzwürdigkeit klassifiziert. Die dafür verwendeten Begriffe „Verfügbarkeit“, „Integrität“ und „Vertraulichkeit“ sind wesentliche Kategorien des Datenschutzes und ermöglichen eine differenzierte Betrachtung gerade auch hinsichtlich personenbezogener Daten. Die bisher eigens für die Bewertung dieser Daten vorgesehene Rubrik „Sensibilität“ ist deshalb überflüssig und sollte entfallen.

- Der Abschnitt „Risikoanalyse“ basiert auf dem IT-Strukturrahmen für Mecklenburg-Vorpommern. Die Gefahren, die für das Recht auf informationelle Selbstbestimmung bestehen, werden aber darin nur zum Teil berücksichtigt. Es reicht nicht, lediglich die Vorgaben des IT-Strukturrahmens an die Besonderheiten von PROfiskal anzupassen.

  In dem Unterabschnitt „Schadensqualität“ sollte der Punkt „Verletzung(en) des informationellen Selbstbestimmungsrechts“ aufgenommen werden. Er ist dann in der Werteskala sowie in den Unterabschnitten „Schadenshäufigkeit“ und „Risikowert“ zu berücksichtigen. Auch die folgenden Abschnitte und Kapitel sollten auf einen sich eventuell daraus ergebenden Änderungs- bzw. Erweiterungsbedarf hin überprüft werden.

Das Finanzministerium will die Empfehlungen berücksichtigen.

Testdatenbank

Neben der Datenbank für den Produktionsbetrieb existiert eine Testdatenbank, auf die jeder mit PROfiskal arbeitende Mitarbeiter Zugriff hat und in die er auch Daten eingeben kann. Die Testdatenbank dient zur Schulung der Mitarbeiter und zur Untersuchung des Ablaufverhaltens der einzelnen Prozesse. Dafür wurden auch personenbezogene Daten genutzt.

Die Verwendung von personenbezogenen Echtdaten zu Testzwecken ist grundsätzlich unzulässig, da sie eine Zweckdurchbrechung darstellt und die Integrität der Daten gefährdet. Nachdem ich auf die Unrechtmäßigkeit der Nutzung von Echtdaten für allgemeine Testzwecke hingewiesen hatte, wurden umgehend sämtliche in der Testdatenbank gespeicherten personenbezogenen Daten gelöscht. Gleichzeitig wurden die Mitarbeiter angewiesen, künftig keine personenbezogenen Daten in die Testdatenbank einzugeben.

Test mit Echtdaten im Einzelfall

Das Finanzministerium bat zu prüfen, ob ein Test einer bestimmten Programmfunktion mit Echtdaten durchgeführt werden kann. Das zu testende Modul weist eine so hohe Komplexität auf, daß allein mit Testdaten wichtige Aspekte des Programmlaufes, wie die Leistungsfähigkeit, nicht aussagekräftig getestet werden können. Unter folgenden Voraussetzungen wäre im vorliegenden Einzelfall der geplante Test mit Echtdaten vertretbar:

- Das zu testende Programm/Modul muß nach den Regeln der Softwaretechnik umfassend mit (nicht personenbezogenen) Testdaten getestet worden sein. Das gilt insbesondere für die möglichen Programmverzweigungen, die Fehlerrobustheit, etwa bei falschen Eingaben, die Fehlerbehandlung und das Zusammenspiel mit den übrigen Programmen/Modulen.

- Die Gründe, warum ein Test mit Testdaten nicht ausreicht und Echtdaten benötigt werden, sind detailliert zu dokumentieren.

- Der Test ist zeitlich auf das notwendige Minimum zu beschränken.

- Die Originaldatenbank darf nur dann für die Testzwecke verwendet werden, wenn eine vollständige Sicherungskopieunmittelbar vor Testbeginn angelegt worden ist.

- Der Test muß unter Produktionsbedingungen ablaufen, die personenbezogenen Daten müssen also genauso gegen unberechtigte Zugriffe und Manipulation geschützt sein wie im Echtbetrieb.

- Zugriffsrechte für den Test dürfen nur solche Personen erhalten, die auch im Echtbetrieb mit PROfiskal arbeiten. Ihre Zugriffsrechte für den Test dürfen die ihnen für den Echtbetrieb eingeräumten Rechte nicht übersteigen. Andere Personen dürfen nur unter Aufsicht Zugriff auf die Anlage haben. Fernzugriff, etwa Fernwartung, ist für diese Personengruppe ausgeschlossen.

- Unverzüglich nach Testende müssen alle beim Test eingesetzten personenbezogenen Daten gelöscht und der ursprüngliche Zustand durch Einspielen der Sicherungskopie wiederhergestellt werden.

Ich habe das Finanzministerium gebeten, mir mitzuteilen, wie unter Berücksichtigung meiner Empfehlungen verfahren wird. Die Antwort steht noch aus.

Lesender Fernzugriff durch die Softwarefirma

Die DVZ M-V GmbH teilte mir mit, daß sie es aus Gründen der Effektivität für sinnvoll halte, der Softwarefirma im Einzelfall zu ermöglichen, auf PROfiskal-Datenbestände lesend zuzugreifen. In meiner Stellungnahme zur Zulässigkeit dieses Fernzugriffs wies ich darauf hin, daß der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe „Forderungen an Wartung und Fernwartung“ herausgegeben hat und daß die darin aufgeführten Anforderungen einer datenschutzgerechten Fernwartung auch für nur lesende Zugriffe gelten. Ich bat die DVZ M-V GmbH, alle in Frage kommenden Forderungen der Orientierungshilfe umzusetzen und dies zu dokumentieren.

Die DVZ M-V GmbH sicherte mir zu, daß kein Fernzugriff stattfinde, bevor nicht die erforderlichen Maßnahmen ergriffen sowie dokumentiert worden sind und ich zugestimmt habe.

Die meisten meiner im vorangehenden und im aktuellen Berichtszeitraum gegebenen Empfehlungen zu PROfiskal wurden berücksichtigt. Die Zusammenarbeit mit dem Finanzministerium, welches die datenschutzrechtliche Verantwortung für das Verfahren hat, und mit der Projektgruppe, in der unter der Leitung der DVZ M-V GmbH das Finanzministerium und die Softwarefirma vertreten sind, ist weiterhin konstruktiv.

3.12 Soziales

3.12.1 Wahrung des Sozialgeheimnisses

Ein Sozialhilfeempfänger hatte beim Ordnungsamt einen Antrag auf Schadensersatz nach dem Staatshaftungsgesetz gestellt. Bei einer Einsichtnahme in seine Sozialhilfeakte stellte er fest, daß diese eine Kopie seines Antrages enthielt. Warum sie dort aufbewahrt wurde, wurde ihm nicht erklärt. Daraufhin wandte er sich an mich.

Auf meine Anfrage teilte mir der Leitende Verwaltungsbeamte mit, daß für den vom Petenten eingereichten Antrag auf Schadensersatz der Landkreis zuständig ist. Die Prüfung der Zuständigkeit erfolgte durch den Leiter des Ordnungs- und Sozialamtes. Da die beantragte Summe im Falle einer Bewilligung als Vermögen im Sinne des Bundessozialhilfegesetzes zu werten wäre, wurde eine Kopie des Antrages vorsorglich in die Sozialhilfeakte übernommen.

Aus datenschutzrechtlicher Sicht handelt es sich in diesem Fall um eine Datenerhebung auf Vorrat, die grundsätzlich unzulässig ist. Die Daten hätten erst erhoben werden dürfen, wenn sie zur Erfüllung einer konkreten Aufgabe des Sozialamtes erforderlich gewesen wären. Das bedeutet, daß der Betroffene erst dann im Rahmen seiner Mitwirkung im Sozialverfahren zur Vorlage entsprechender Beweismittel hätte verpflichtet werden können, wenn seinem Antrag stattgegeben worden wäre. Dies habe ich dem Amt mitgeteilt und gefordert, die Kopie des Antrages auf Schadensersatz aus der Sozialhilfeakte zu entfernen. Dieser Aufforderung wurde entsprochen.

3.12.2 Formulare zur Eingliederungshilfe für Behinderte

Ein freier Träger hat mich gebeten, ein Antragsformular eines Sozialamtes auf Eingliederungshilfe für behinderte Kinder zu prüfen (§§ 39 ff. Bundessozialhilfegesetz - BSHG). Die Daten sollten insbesondere als Entscheidungsgrundlage für die Frühförderung der Kinder verwendet werden. Dazu waren der vollständige Name, das Geburtsdatum und der Wohnort des Kindes, Name und Anschrift des Hausarztes, Diagnose beziehungsweise die Art der Behinderung und der vollständige Name der Eltern gefordert. Des weiteren sollten die sorgeberechtigten Eltern drei Einverständniserklärungen unterschreiben.

Nach der ersten sollten sie sich damit einverstanden erklären, daß die Erzieher in der Kindereinrichtung durch ihre Unterschrift die Teilnahme des Kindes an der Frühförderung bestätigen dürfen. Eine Alternative war nicht angegeben, und es wurde darüber hinaus nicht erläutert, welche Folgen es hat, wenn nicht eingewilligt wird. Aufgrund meiner Empfehlung hat das Sozialamt sie so geändert, daß die Betroffenen zunächst erklären, ob sie mit dieser Regelung einverstanden sind oder nicht. Des weiteren werden sie nun auf die Folgen hingewiesen, wenn sie die Einwilligung nicht geben. In diesem Fall kann eine Frühförderung in der Kindereinrichtung nicht stattfinden.

In der zweiten Erklärung wurde das Einverständnis erbeten, daß vorhandene ärztliche Berichte, Gutachten und Befunddokumentationen dem Gesundheitsamt/Sozialamt beziehungsweise dem Medizinischen Dienst zur Verfügung gestellt werden. Das Sozialamt benötigt für seine Entscheidungen jedoch nur das Ergebnis des amtsärztlichen Gutachtens. Hierauf hatte bereits der freie Träger in seinem Schreiben hingewiesen. Ferner war die Erklärung zu unbestimmt und ihr Zweck wurde nicht erläutert. Deshalb hat das Sozialamt auf meinen Vorschlag hin einen geänderten Text aufgenommen. Nunmehr erklären die Eltern sich damit einverstanden, daß die von ihnen benannten Ärzte oder Krankenhäuser ärztliche Berichte, Gutachten oder Befunddokumentationen, soweit sie mit der Behinderung in einem medizinischen Sachzusammenhang stehen, dem Gesundheitsamt beziehungsweise dem Medizinischen Dienst zur Verfügung stellen dürfen. Die Ärzte werden insofern von der Schweigepflicht entbunden. Die Erklärung wird mit dem Hinweis abgeschlossen, daß bei einer Verweigerung der Einwilligung eine amtsärztliche

Untersuchung erforderlich ist, deren Ergebnis dem Sozialamt zur Entscheidung über die Eingliederungshilfe mitgeteilt wird.

Schließlich sollten sich die Betroffenen im dritten Punkt damit einverstanden erklären, daß andere Fachämter über die im Gutachten vorgeschlagenen Maßnahmen zur individuellen Förderung des Kindes informiert werden. Weder waren die Fachämter näher bezeichnet, noch ist erläutert worden, ob den Betroffenen Nachteile entstehen, wenn sie dies nicht unterzeichnen. Ich habe empfohlen, die Einwilligung so zu ändern, daß die im amtsärztlichen Gutachten vorgeschlagenen weiteren Maßnahmen zur individuellen Förderung des Kindes an das Jugendamt und an das Schulamt übermittelt werden dürfen oder nicht. Die Betroffenen sollten außerdem darauf hingewiesen werden, daß ihnen bei einer Verweigerung dieser Einwilligung keine Nachteile entstehen, da sie selbst entsprechende Anträge bei den Fachämtern stellen können. Das Sozialamt hat auch diese Empfehlung übernommen.

3.12.3 Hilfe bei drohendem Verlust der Wohnung

Sozialhilfeträger, kommunale Wohnungsunternehmen und das Sozialministerium baten um Beratung, wie Bürgern unter Einhaltung datenschutzrechtlicher Bestimmungen schnell geholfen werden kann, wenn ihnen der Verlust der Wohnung droht, weil sie hohe Mietrückstände nicht mehr begleichen können.

Mit dem Gesetz zur Reform des Sozialhilferechts vom 23. Juli 1996 wurde eine Rechtsgrundlage für die Datenübermittlung an die Sozialhilfeträger geschaffen, die eine rechtzeitige Hilfe in einem solchen Fall ermöglicht. Danach dürfen Gerichte im Falle der Kündigung des Mietverhältnisses nach § 554 Bürgerliches Gesetzbuch (BGB) dem zuständigen örtlichen Träger der Sozialhilfe folgende Daten bei Eingang einer Räumungsklage mitteilen (§ 15 a Abs. 2 BSHG):

- Tag des Eingangs der Klage,
- Namen und Anschriften der Parteien,
- Höhe des monatlich zu entrichtenden Mietzinses,
- Höhe des geltend gemachten Mietzinsrückstandes und der geltend gemachten Entschädigung und den

- Termin der mündlichen Verhandlung, sofern dieser bereits bestimmt ist.

Wenn allerdings offensichtlich ist, daß die Mietrückstände nicht wegen Zahlungsunfähigkeit entstanden sind, dann dürfen diese Daten nicht an den Sozialhilfeträger übermittelt werden.

In den Beratungen habe ich auf diese Rechtsvorschrift hingewiesen. Die Sozialhilfeträger meinten jedoch, daß diese Mitteilung durch die verzögerte Bearbeitung bei den Gerichten meist zu spät erfolgt, so daß nicht mehr ausreichend Zeit verbleibt, um die Räumung der Wohnung tatsächlich zu verhindern. Deshalb habe ich dem Sozialministerium empfohlen, die Gerichte in geeigneter Form darauf hinzuweisen, daß sie diese Mitteilung, wie es die Rechtsvorschrift vorsieht, unverzüglich an die Sozialhilfeträger geben - also unmittelbar nach Eingang der Klage und Prüfung der Zulässigkeit der Datenübermittlung. Selbstverständlich wäre den Sozialhilfeträgern nicht damit gedient, wenn eine solche Klage im Geschäftsgang eines Gerichtes hängenbleibt und sie erst kurz vor der Verhandlung die Information erhalten.

Darüber hinaus haben die Sozialhilfeträger die Möglichkeit, im Rahmen ihrer Öffentlichkeitsarbeit in allgemeiner Form ihre Beratung und Unterstützung anzubieten, so daß Betroffene von sich aus den Kontakt zum Sozialamt suchen.

Das Sozialministerium hat bei einer Besprechung des Sachverhaltes im August 1997 mitgeteilt, daß es nach dieser Empfehlung verfahren wird.

3.12.4 Viele Fragen zu den neuen Regelungen im Kita-Gesetz

Im Januar 1996 wurde in Medien berichtet, daß im Entwurf einer Satzung zum Gesetz zur Förderung von Kindern in Tageseinrichtungen und Tagespflege (KitaG) vorgesehen ist, dem Antragsformular auf einen Kindertagesstättenplatz einen Arbeitszeitnachweis beizufügen. In diesem Nachweis war der Beginn und das Ende der täglichen Arbeitszeit anzugeben und vom Arbeitgeber zu bestätigen. Darüber hinaus wurde auch nach dem Beschäftigungsverhältnis („beschäftigt als“) gefragt. Ein Hinweis auf die Rechtsgrundlage dieser Datenerhebung fehlte.

Die Anspruchsvoraussetzungen für einen Platz in einer Kindertageseinrichtung sind im KitaG normiert. Demnach hat jedes Kind ab dem vollendeten dritten Lebensjahr ohne Einschränkungen Anspruch auf einen Platz in einer Kindertageseinrichtung von bis zu sechs Stunden täglich. Wird jedoch ein Ganztagsplatz beansprucht, müssen die Eltern mindestens vier Stunden täglich berufstätig oder an der Ausübung des Personensorgerechts ganz oder teilweise gehindert sein.

Der von der Gemeinde erarbeitete Erhebungsbogen entsprach somit nicht den gesetzlichen Bestimmungen. Deshalb habe ich folgende Empfehlungen gegeben:

Zunächst sollte der Antrag so strukturiert werden, daß die Eltern klar erkennen können, welche Daten für einen Halbtags- beziehungsweise Ganztagsplatz anzugeben sind. Die Kenntnis der täglichen Arbeitszeit ist beispielsweise nur erforderlich, wenn ein Ganztagsplatz beantragt wird. Aber auch dann ist eine detaillierte Angabe zur täglichen Arbeitszeit (Beginn und Ende) nicht erforderlich. Nach der Rechtsvorschrift ist eine pauschale Bestätigung des Arbeitgebers ausreichend.

Die Frage nach dem Beschäftigungsverhältnis („beschäftigt als“) ist für die Entscheidung der Gemeinde ebenfalls nicht erforderlich und somit nicht zulässig. Dieses Datum darf also künftig auch nicht mehr erhoben werden. Weiterhin sollte der Erhebungsbogen um die Angabe der einschlägigen Rechtsvorschrift ergänzt werden.

Die Gemeinde hat den Arbeitszeitnachweis entsprechend meinen Empfehlungen überarbeitet.

Unklarheiten zum KitaG auch bei den Trägern der Einrichtungen

In einem anderen Fall übersandte mir der Träger einer Kindertagesstätte den vom zuständigen Landkreis erarbeiteten „Antrag auf Ermäßigung des Elternbeitrages - Ermittlung des Familien-Netto-Einkommens“ zur datenschutzrechtlichen Prüfung.

Das Einkommen der Eltern war untergliedert nach der Einkommensart anzugeben, zum Beispiel Kindergeld, Unterhalt, Arbeitslosenhilfe, Sozialhilfe. Dieser Antrag sollte von den Personensorgeberechtigten ausgefüllt und in der Kindertagesstätte abgegeben werden.

Im KitaG ist geregelt, daß die Anträge auf Ermäßigung des Elternbeitrages bei den örtlichen Trägern der öffentlichen Jugendhilfe zu stellen sind und nicht - wie hier vorgesehen - beim Träger der Einrichtung. Fraglich war auch, ob der verlangte detaillierte Einkommensnachweis notwendig war, zumal das Gesetz lediglich die Glaubhaftmachung des Familiennettoeinkommens verlangt (§ 18 Abs. 2 KitaG). Mittel der Glaubhaftmachung sind beispielsweise die Vorlage von Belegen oder die Versicherung an Eides Statt. Letzteres kam in diesem Fall nicht in Betracht, da die Behörde nur dann befugt ist, eidesstattliche Versicherungen abzunehmen, wenn dies durch Gesetz oder Rechtsverordnung vorgesehen und die Behörde durch eine Rechtsvorschrift für zuständig erklärt worden ist. Glaubhaftmachung bedeutet aber nicht, daß die einzelnen Einkommensbestandteile wie Sozialhilfe oder Wohngeld erhoben und gespeichert werden. Bei diesem Verfahren würde bei den Trägern der Einrichtungen eine zweite „Sozialhilfeakte“ angelegt, die zum Teil sogar noch mehr Daten enthalten würde, als eine übliche Akte.

Dem Landkreis habe ich folgendes Verfahren empfohlen:

1. Auf dem Erhebungsbogen sollte darauf hingewiesen werden, daß der Antrag auf Ermäßigung des Elternbeitrages grundsätzlich beim örtlichen Träger der öffentlichen Jugendhilfe zu stellen ist.

2. Die Eltern sollten ihr Einkommen beim Träger der öffentlichen Jugendhilfe im Rahmen der Antragstellung durch Vorlage der entsprechenden Unterlagen glaubhaft machen. Der örtlich zuständige Träger der öffentlichen Jugendhilfe kann dann in seiner Unterlage festhalten, welche Eltern die Ermäßigung erhalten und wie hoch diese ist.

Der Landkreis hat meine Empfehlungen umgesetzt.

3.12.5 Von teuren Versicherten und ungesicherten Sozialdaten

Im Dezember 1996 wurde ich über eine besonders unerfreuliche Sache unterrichtet. Im Namen von Ersatzkassen waren an mehrere Dialysepatienten, die Mitglied einer Krankenkasse unseres Landes sind, Briefe verschickt worden. Sie enthielten ein Informationsblatt über die nunmehr mögliche freie Wahl der Krankenkasse und auch gleich einen Aufnahmeantrag der betreffenden Ersatzkasse. Es entstand der Eindruck, daß sie abgeworben werden sollten.

Die Briefe waren nicht ausreichend frankiert, und der Absender fehlte. Deshalb wurden sie von den Adressaten nicht angenommen. Die Zentrale Briefermittlungsstelle der Deutschen Post AG hat sie dann geöffnet und jeweils den Ersatzkrankenkassen übergeben, deren Aufnahmeantrag beilag. Solche Formulare liegen üblicherweise in den Geschäftsstellen von Krankenkassen zur freien Verfügung aus und können daher von jedem Besucher mitgenommen werden.

Die Recherchen der Ersatzkassen ergaben, daß die Briefe nicht von ihnen versandt worden waren und daß sich die Adressaten ausnahmslos als Dialysepatienten in Behandlung befinden. Vor diesem Hintergrund haben die Ersatzkrankenkassen vermutet, daß die Versichertendaten von der betreffenden Krankenkasse unseres Landes entweder unbefugt an Dritte weitergegeben worden sind oder von ihr nicht ausreichend gegen unbefugten Zugriff gesichert waren. Der Bundesverband der betreffenden Ersatzkrankenkassen hat mich über diesen Sachstand informiert und mir eine Liste der betroffenen Versicherten zur Verfügung gestellt. Aus ihr ging hervor, daß die Angeschriebenen überwiegend in einer Stadt beziehungsweise deren näherer Umgebung wohnen.

Ich habe die Krankenkasse um eine Stellungnahme gebeten und den Sozialminister über den Sachverhalt unterrichtet. Der Vorstandsvorsitzende hat mitgeteilt, daß man bei den Recherchen über das Stadium der Spekulation nicht hinausgekommen sei und in seinem Hause keine Anhaltspunkte dafür vorliegen würden, daß Sozialdaten unberechtigt an Dritte übermittelt oder diese Briefe von seiner Kasse verschickt worden seien.

Bei einer ersten Kontrolle der zuständigen Geschäftsstelle stellte sich heraus, daß von 14 der angeschriebenen Personen 12 bei der Krankenkasse unseres Landes versichert sind. Bei den zwei anderen Personen war aufgrund der vorliegenden Angaben nicht eindeutig nachweisbar,

wo sie versichert sind oder waren. Wie sich aus den gespeicherten Leistungsdaten weiter ergab, wurden die Versicherten von verschiedenen Dialysezentren beziehungsweise niedergelassenen Dialyseärzten behandelt. Eine zweckentfremdete Nutzung der Patientendaten durch die Behandlungseinrichtungen oder durch die Beförderungsunternehmen war deshalb recht unwahrscheinlich.

Die Krankenkasse berichtete von weiteren Recherchen: Eine Anfrage bei dem Rechenzentrum ergab keine Hinweise darauf, daß Mitarbeiter einen Auftrag zur Zusammenstellung von Adressen ausgewählter Dialysepatienten ausgelöst hatte. Die Daten aus Standardbildschirmmasken des Datenverarbeitungssystems zusammenzustellen, sei nur mit unverhältnismäßig großem Aufwand möglich und komme daher kaum in Betracht. Eine Befragung von Mitarbeitern sei ebenfalls erfolglos gewesen. Man sei schließlich zu der Auffassung gelangt, daß die zweckentfremdete Datennutzung aufgrund des Einzelwissens eines Mitarbeiters zustande gekommen sei. Der Personenkreis ließe sich jedoch nicht weiter eingrenzen.

Eine weitere Kontrolle der Zugriffsrechte auf den Datenbestand erschien mir deshalb erforderlich. Die verantwortlichen Mitarbeiter der Krankenkasse bestätigten, daß das Datenverarbeitungssystem die Vergabe differenzierter Schreib- und Leserechte zwar prinzipiell ermöglicht, aber diese unterschiedlichen Zugriffsrechte nicht eingerichtet worden waren. Folglich konnte jeder Beschäftigte mit einer Zugangsberechtigung zum System den gesamten Datenbestand, also die gespeicherten Beitrags- und Leistungsdaten aller Versicherten dieser Krankenkasse im Land Mecklenburg-Vorpommern, bearbeiten und die Standardbildschirmanzeigen auswerten. Dies steht im Widerspruch zu der Rechtsvorschrift, nach der die datenverarbeitenden Stellen technische und organisatorische Maßnahmen zu treffen haben, die erforderlich sind, um die Ausführung der Vorschriften des Sozialgesetzbuches zu gewährleisten (§ 78 a SGB X). Ich habe diesen Zustand beanstandet und differenzierte Zugriffsrechte gefordert.

In ihrer Stellungnahme hat die Krankenkasse ausgeführt, daß sie in der Zwischenzeit eine Arbeitsgruppe eingerichtet hat, die die Zugriffsberechtigungsprofile für Nutzer festlegen wird. Anfang Dezember 1997 teilte sie mit, daß bis Ende des Monats die Zugriffsbeschränkungen nach entsprechenden Berechtigungsprofilen technisch realisiert sein werden.

Weiter war der Sachverhalt mit den mir zur Verfügung stehenden gesetzlichen Möglichkeiten nicht aufzuklären.

3.12.6 Prüfung des Medizinischen Dienstes der Krankenversicherung in Krankenhäusern

Aus verschiedenen Krankenhäusern des Landes erreichten mich Anfragen zu den Prüfungsrechten des Medizinischen Dienstes der Krankenversicherung (MDK).

Ich habe darauf hingewiesen, daß es im wesentlichen drei unterschiedliche Aufträge von gesetzlichen Krankenkassen sein können, die den MDK zur Prüfung von Krankenhausbehandlungen berechtigen:

1. gutachtliche Stellungnahme wegen der Art, Schwere, Dauer oder Häufigkeit der Erkrankung oder wegen des Krankheitsverlaufs (Sozialgesetzbuch Fünftes Buch § 275 Abs. 1 - SGB V),
2. gutachtliche Stellungnahme über die Notwendigkeit und Dauer der stationären Behandlung eines Versicherten mit der Befugnis des MDK, die Räume der Krankenhäuser in der Zeit zwischen 08.00 und 18.00 Uhr zu betreten, um dort Krankenunterlagen einzusehen und, soweit erforderlich, den Versicherten zu untersuchen (§ 276 Abs. 4 SGB V),
3. gutachtliche Stellungnahme, um Fehlbelegungen zu vermeiden oder bestehende Fehlbelegungen abzubauen (§ 17 a Krankenhausfinanzierungsgesetz).

Der erste Prüfungsfall ist ein allgemeiner Auftrag, der alle Leistungserbringer einbezieht. Er kann dadurch erfüllt werden, daß der MDK vom Krankenhaus einzelne Unterlagen anfordert, zum Beispiel einen Arztbericht, Operationsbericht oder dergleichen. Die Zusendung der vollständigen Originalakte an den MDK läßt sich damit allerdings nicht begründen. Dies wäre auch aus medizinischen Gründen nicht zu rechtfertigen, denn in Notfällen oder für eventuell erforderliche weitere Behandlungen dieser Krankheit müssen diese Unterlagen im Krankenhaus jederzeit verfügbar sein.

Der zweite Fall bezieht sich ausschließlich auf die gutachtliche Stellungnahme bei einer stationären Behandlung. Wesentlich ist dabei, daß der MDK das Krankenhaus in der Zeit von 08.00 bis 18.00 Uhr betreten darf, dort Krankenunterlagen einsehen und gegebenenfalls den Versicherten auch untersuchen kann. Die Grenze der Einsichtnahme in Krankenunterlagen richtet sich nach dem Krankheitsfall. Der MDK darf nur die Unterlagen einsehen, allerdings auch solche aus vorhergehenden Behandlungen, die mit dem zu prüfenden Fall in einem medizinischen Sachzusammenhang stehen. Krankenunterlagen, auf die das nicht zutrifft, sind nach dem Landeskrankenhausgesetz gesperrt (§ 19 LKHG M-V).

Für den dritten Prüfauftrag müssen Anhaltspunkte dafür vorliegen, daß bei einem Krankenhaus Fehlbelegungen an bestimmten Tagen gehäuft auftreten, zum Beispiel Krankenhausaufnahmen vor Wochenenden oder Feiertagen. Die Einsichtnahme in Krankenunterlagen und die Nutzung von Patientendaten ohne einen solchen Anhaltspunkt ist nach dieser Rechtsvorschrift jedenfalls nicht zulässig.

Im Jahr 1996 hatten die Krankenkassen den MDK beauftragt, sogenannte Stichtagserhebungen in allen Krankenhäusern des Landes durchzuführen. Dazu wurden willkürlich mehrere Tage eines Jahres ausgewählt und die Akten aller Patienten, die an einem solchen Tag im Krankenhaus behandelt worden sind, eingesehen und ausgewertet. Die Krankenkassen nahmen an, durch dieses Vorgehen auch Fehlbelegungen feststellen zu können, doch konkrete Hinweise darauf waren nicht vorhanden. Solche Hinweise aber hätte jede Krankenkasse aus den von den Krankenhäusern zu übermittelnden Daten erhalten können, wie Institutskennzeichen des Krankenhauses, Tag, Uhrzeit und Grund der Aufnahme (§ 301 Abs. 1 Sozialgesetzbuch Fünftes Buch - SGB V). Deshalb war die Stichtagserhebung so nicht zulässig.

Allerdings kann der MDK auch bei abgeschlossenen Behandlungsfällen mit einer gutachtlichen Stellungnahme beauftragt werden, wenn und soweit dies zur Erfüllung einer Aufgabe nach dem Sozialgesetzbuch erforderlich ist. Er kann sich dann gegenüber dem Krankenhaus auf dessen gesetzliche Mitteilungspflicht berufen (§ 276 Abs. 2 Satz 1 SGB V), die die Sperrung der Patientendaten im erforderlichen Umfang aufhebt (§ 19 Abs. 2 Satz 5 LKHG M-V). Der MDK muß den Auftrag jedoch begründen, damit dieser vom Krankenhaus geprüft und die Aufhebung der Sperrung für diesen Zweck in den Krankenunterlagen vermerkt werden kann (§ 19 Abs. 2 Satz 6 LKHG M-V).

Den Krankenhäusern habe ich diese Rechtslage erläutert und auch die Landeskrankenhausgesellschaft sowie den MDK darüber informiert.

3.12.7 Prüfung der Versicherungsfreiheit/Versicherungspflicht durch das Landesbesddungsamt

Ein Petent bat mich, das Formular „Erklärungen zur Prüfung der Versicherungsfreiheit beziehungsweise Versicherungspflicht in der Kranken-, Renten- und Arbeitslosenversicherung“ zu prüfen, weil er Bedenken hinsichtlich der Menge der geforderten Daten hatte (siehe auch Punkt 3.12.7).

Zunächst war zweifelhaft, ob alle Angaben für die Überprüfung der Versicherungsfreiheit beziehungsweise Versicherungspflicht überhaupt erforderlich waren. Beispielsweise sollte beantwortet werden, ob der Betroffene „... künftig berufsmäßig als Arbeitnehmer oder Beamter tätig sein will“ oder ob er „... die Absicht habe, Mitglied bei einer Ersatzkasse zu werden.“ Ich habe dem Finanzministerium als der für das Landesbesoldungsamt zuständigen Stelle folgende Empfehlungen gegeben:

1. Die auf dem Erhebungsbogen geforderten Angaben sollten dahingehend überprüft werden, ob sie für die Überprüfung der Versicherungsfreiheit/Versicherungspflicht erforderlich sind.

2. Im Erhebungsbogen sollte auf die für die Datenerhebung einschlägigen Rechtsvorschriften hingewiesen werden.

3. Sollten darüber hinausgehende Daten erhoben werden, ist auf die Freiwilligkeit der Angaben hinzuweisen.

In dem überarbeiteten Entwurf wurden diese Empfehlungen umgesetzt.

Über das Ergebnis habe ich den Petenten informiert. Durch seine Anfrage hat er zu einer datenschutzgerechten Gestaltung des Formulars beigetragen.

3.12.8 Schwarzarbeiter-Hotline

Im Frühjahr 1997 berichteten die Medien über eine sogenannte Schwarzarbeiter-Hotline. Bürger und Behörden wurden darüber informiert, daß Anzeigen über illegale Beschäftigung und Schwarzarbeit bei den Arbeits- und Hauptzollämtern unter speziell eingerichteten Rufnummern entgegengenommen würden.

Eine Regionalzeitung stellte erste Ergebnisse der Hotlines dar und berichtete, daß über 90 Prozent der Anrufer anonym bleiben wollten. Im Wege der Amtshilfe würden die zuständigen Stellen benachrichtigt, sofern sich ein Anruf auf einen Fall beziehe, für den das Arbeitsamt nicht zuständig sei. Besorgte Bürger unseres Landes befürchteten, daß hiermit der Denunziation Tür und Tor geöffnet werde. Einige praktische Beispiele zeigten, daß diese Sorge durchaus berechtigt war. So habe beispielsweise ein Arbeiter zu unrecht seinen Chef angeschwärzt, um sich auf diese Weise an ihm wegen einer betrieblichen Angelegenheit zu rächen.

Arbeitsämter sind Dienststellen der Bundesanstalt für Arbeit. Sie unterliegen der Kontrolle des Bundesbeauftragten für den Datenschutz (BfD). Deshalb bat ich den BfD, die Rechtmäßigkeit der Schwarzarbeiter-Hotline zu prüfen. Er unterrichtete mich, daß er bei seiner Kontrolle in einem Arbeitsamt keine Verstöße gegen datenschutzrechtliche Bestimmungen festgestellt hat. Es seien dort jedoch fast ausschließlich anonyme Anzeigen registriert worden.

Folgende Fragen sind damit jedoch bis zum gegenwärtigen Zeitpunkt noch nicht beantwortet:

- Auf welcher gesetzlichen Grundlage kann ein Arbeitsamt quasi als zentrale Meldestelle fungieren und personenbezogene Daten entgegennehmen und sie an andere Stellen übermitteln, wenn es nicht zuständig ist?
- Wie lange dürfen solche Daten gespeichert werden, wenn den Hinweisen mangels tatsächlicher Anhaltspunkte nicht nachgegangen wird beziehungsweise wenn sie sich im Laufe der Prüfung als unrichtig erweisen?

- Werden Betroffene darüber informiert, daß Hinweise über sie vorliegen, und welche Möglichkeit haben sie, sich gegen nachweislich ungerechtfertigte Angriffe zur Wehr zu setzen?

Der Wirtschaftsminister unseres Landes hat die Einrichtung der Schwarzarbeiter-Hotlines in Interviews verteidigt. Wie einem Pressebericht zu entnehmen war, haben die zuständigen Minister anderer Bundesländer jedoch derartige Maßnahmen aus gutem Grund abgelehnt.

Ich gehe davon aus, daß es geeignetere staatliche Mittel als eine sogenannte Schwarzarbeiter-Hotline gibt, um Leistungsmißbrauch zu bekämpfen.

3.13 Gesundheitswesen

3.13.1 Fragebogen zur Erhebung von Praxiskosten

Im August 1996 wurde ich über ein Schreiben der Kassenärztlichen Vereinigung (KV) und einen beigefügten Fragebogen zur Erhebung von Praxiskosten informiert und um datenschutzrechtliche Bewertung gebeten.

Als Ziel der Datenerhebung war angegeben, daß durch die Kenntnis individueller Praxisbudgets die Berechnung und Festlegung der fachgruppenspezifischen Praxiskosten besser beeinflußt werden kann. Außerdem wollte die KV hiermit eine Datengrundlage zur betriebswirtschaftlichen Beratung der Ärzte schaffen. Die Angaben sollten anonym erfolgen, und es wurde zugesichert, daß sie ohne Zuordnungsmöglichkeit erfaßt und weiterverarbeitet werden. Unklar blieb zunächst, ob die Ärzte verpflichtet sind die Daten anzugeben, oder ob die Erhebung auf freiwilliger Basis erfolgen sollte.

Darüber hinaus waren einige der abgefragten Daten so detailliert, daß ohne weiteres eine Zuordnung zu einem bestimmten Arzt möglich war. So wurde beispielsweise nach der Höhe des Honorars der Kassenärztlichen Vereinigung und anderen einzelnen Praxiseinnahmen gefragt. Ich habe die KV darauf hingewiesen, daß es sich hier nicht um eine anonyme Erhebung handelt, und empfohlen, entweder einen Erhebungsbogen zu verwenden, der die zugesicherte Anonymität tatsächlich gewährleistet, oder die Betroffenen entsprechend aufzuklären.

Daraufhin hat die KV die Datenerhebung insbesondere mit § 285 SGB V begründet. Danach dürfen Einzelangaben über die persönlichen und sachlichen Verhältnisse der Ärzte erhoben und gespeichert werden, soweit dies beispielsweise zur Sicherstellung und Vergütung der vertragsärztlichen Versorgung erforderlich ist. Insofern wäre gegen die Datenerhebung nichts einzuwenden gewesen, wenn sie mit Hinweis auf die Rechtsvorschrift beziehungsweise die Freiwilligkeit erfolgt wäre. Dann hätte die KV aber zwischen den beiden unterschiedlichen Zwecken der Datenerhebung - Festlegung fachgruppenspezifischer Praxiskosten und betriebswirtschaftliche Beratung - deutlich trennen sowie durch technische und organisatorische Maßnahmen die zweckgebundene Nutzung der jeweiligen Daten gewährleisten müssen.

Die KV hat meine Empfehlungen aufgenommen und sie bei der 1997 durchgeführten Erhebung berücksichtigt.

3.13.2 Einsichtsrecht nach dem Gesetz über Hilfen und Schutzmaßnahmen für psychisch Kranke

Eine psychiatrische Klinik verweigerte einer ehemaligen Patientin und deren Hausarzt Einsicht in ihre Krankenunterlagen. Deshalb wandte sie sich an mich und bat um Unterstützung.

Das Akteneinsichtsrecht für psychisch kranke Personen ist im „Gesetz über Hilfen und Schutzmaßnahmen für psychisch Kranke (PsychKG)“ unseres Landes geregelt (§ 44 PsychKG). Danach ist Betroffenen und ihren gesetzlichen Vertretern unentgeltlich Auskunft über die zu ihrer Person gespeicherten Daten zu geben und Einsicht in die über sie geführten Akten zu gewähren. Dieses Recht kann nur verweigert werden, wenn eine Verständigung mit den Betroffenen aufgrund ihres Gesundheitszustandes nicht möglich ist.

Des weiteren ist in dieser Rechtsvorschrift geregelt, daß der behandelnde Arzt die entsprechenden Inhalte vermitteln soll, wenn bei einer vollständigen Auskunft oder Einsichtnahme mit schwerwiegenden gesundheitlichen Nachteilen für den Betroffenen zu rechnen ist. Hiermit hat der Gesetzgeber beabsichtigt, daß auch unter diesen Bedingungen eine Auskunft oder Einsichtnahme nicht generell verweigert werden kann, sondern der Arzt die Inhalte so vermitteln

soll, daß keine gesundheitlichen Nachteile für den Betroffenen entstehen. Wenn der Patient allerdings geheilt ist und folglich nicht mehr mit entsprechenden Nachteilen zu rechnen ist, kann er vollständige Auskunft und Einsicht verlangen.

Die Rechtsvorschrift war offensichtlich in der psychiatrischen Klinik noch nicht in ihrem vollen Umfang bekannt, deshalb habe ich den Ärztlichen Direktor darauf aufmerksam gemacht. Der Patientin wurde schließlich Auskunft gegeben und Akteneinsicht in die mehr als 20 Jahre alten Patientenunterlagen gewährt.

3.13.3 Patientendaten in Krankenhäusern

Kontrollen in Krankenhäusern haben gezeigt, daß die datenschutzrechtlichen Bestimmungen des Landeskrankenhausgesetzes für das Land Mecklenburg-Vorpommern (LKHG M-V) nicht immer eingehalten wurden. Die Schwerpunkte der festgestellten Mängel beziehungsweise vorgeschlagenen Verbesserungen lagen im wesentlichen in den Bereichen

- Datenerhebung bei der Aufnahme der Patienten,
- Datenübermittlungen an anderes Fachpersonal und an Dienstleister,
- Aufbewahrung der Patientenunterlagen.

In einem Krankenhaus wurden beispielsweise die Daten für die stationäre Behandlung vom Personal im Empfangsbereich erhoben. Dabei war weder eine ausreichende akustische noch eine optische Trennung zum Wartebereich vorhanden. Außerdem wurden vom Verwaltungspersonal auch medizinische Daten, wie die Aufnahmediagnose, erfragt und in das Datenverarbeitungssystem eingegeben. Das Personal konnte in diesen Datensätzen umfassend recherchieren, weil die Daten abgeschlossener Behandlungsfälle nicht gesperrt waren. Das Landeskrankenhausgesetz schreibt jedoch vor, daß Patientendaten nach Abschluß der Behandlung zu sperren und spätestens nach 30 Jahren beziehungsweise dann zu löschen sind, wenn ihre Nutzung nicht mehr erforderlich ist (§ 19 Abs. 1 LKHG M-V).

Häufig wird in der Patientenaufnahme oder unmittelbar im Eingangsbereich eine Liste oder eine Datei mit Patientennamen, Station und Zimmernummer genutzt, um Besuchern Auskunft

geben zu können. Eine Datensammlung zu diesem Zweck ist jedoch nur zulässig, wenn der Patient seine Einwilligung hierzu gegeben hat. Weiter ist dabei zu beachten, daß diese Einwilligung nur für die Dauer des Krankenhausaufenthalts gilt. Folglich sind die Daten sofort nach Entlassung des Patienten zu löschen. Dies wurde jedoch nicht in jedem Fall so realisiert. In einigen Fällen waren die Daten mehrere Tage bis Wochen nach der Entlassung des Patienten noch verfügbar.

Ständig an Bedeutung gewinnt auch die Übermittlung von Patientendaten innerhalb und an Stellen außerhalb des Krankenhauses. Vermehrt wird das Fachwissen von anderen Abteilungen und Spezialisten genutzt. Dabei besteht die Gefahr, daß der Patient selbst nicht mehr überblikken kann, wer was wann konkret über ihn weiß und an Daten gespeichert hat. Deshalb empfiehlt sich zum Beispiel beim Datenaustausch im Zusammenhang mit Labordienstleistungen, anstelle personenidentifizierender Daten (wie Name, Vorname und Geburtsdatum) Pseudonyme zu nutzen, beispielsweise die krankenhausinterne Patientennummer. Es handelt sich dann nach der Definition im Landeskrankenhausgesetz zwar immer noch um Patientendaten (§ 14 Abs. 1 LKHG M-V), doch die eindeutige Zuordnung zu einem bestimmten Patienten ist nur noch dem behandelnden Krankenhaus möglich (siehe auch Punkt 2.1). Der Empfehlung wurde vom ärztlichen Personal häufig entgegen gehalten, daß damit die Verwechslungsgefahr zunehme. Dieses Argument ist vor allem deshalb nicht nachvollziehbar, da gerade durch zunehmende Automatisierung der Informationsflüsse auch geeignete Kontrollmechanismen entwickelt worden sind, so daß eine fehlerhafte Zuordnung von Daten nahezu ausgeschlossen werden kann. Die fortschreitende Anwendung von Telemedizin sowie von neuen Kommunikations- und Informationstechnologien erfordert gerade deshalb die Pseudonymisierung der Patientendaten, um auch unter diesen Bedingungen ein angemessenes Datenschutzniveau sicherzustellen.

Es war festzustellen, daß die Patientendaten in den Krankenunterlagen nicht so aufbewahrt werden, wie es das Landeskrankenhausgesetz vorschreibt (§ 19 Abs. 2 Satz 4 LKHG M-V). Die wesentliche Kritik an der bisherigen Praxis läßt sich in folgenden Punkten zusammenfassen:

- Die Behandlungsunterlagen eines Patienten aus verschiedenen Krankenhausaufenthalten und der Behandlung in verschiedenen Fachabteilungen werden in einer Patientenakte aufbewahrt, ohne daß ein medizinischer Sachzusammenhang erkennbar ist.

- Die Behandlungsunterlagen werden in den Archiven nach dem Geburtsdatum und bei gleichen Geburtsdaten alphabetisch nach den Namen der Patienten abgelegt, so daß auch Dritte ohne Schwierigkeiten den Datenbestand erschließen können.

Patientendaten aus verschiedenen Behandlungen können praktisch nur zusammengeführt werden, wenn dazu die Sperrung der Daten eines abgeschlossenen Behandlungsfalles aufgehoben wird. Dies ist jedoch nur zulässig, wenn beide Behandlungen in einem medizinischen Sachzusammenhang stehen (§ 19 Abs. 2 Satz 5 LKHG M-V). Ob ein solcher Zusammenhang vorliegt, ergibt sich im wesentlichen aus der Anamnese. Nur wenn der Patient nicht in der Lage ist, entsprechende Angaben zu machen, könnte anhand der Daten aus früheren Aufenthalten in verschiedenen Fachabteilungen das Vorliegen eines Zusammenhanges geprüft werden. Ist dagegen zwischen zwei oder mehreren Behandlungen kein medizinischer Sachzusammenhang gegeben, dürfen die Daten nicht zusammengeführt und auch nicht in einer Patientenakte aufbewahrt werden.

Weiter regelt das Landeskrankenhausgesetz, daß zur Erschließung der Akten im Archiv ein Nachweis zu führen ist, zu dem andere Bereiche keinen Zutritt haben dürfen (§ 19 Abs. 2 Satz 4 LKHG M-V). Deshalb müssen die Akten so aufbewahrt werden, daß ein Behandlungsfall nur über diesen Nachweis einem Patienten zugeordnet werden kann und andere Bereiche des Krankenhauses ohne Zugriff auf den Nachweis den Bestand nicht erschließen können. Die häufig noch praktizierte Aufbewahrung nach dem Geburtsdatum entspricht nicht dieser Norm. Bei Kenntnis des Geburtsdatums und des Namens ist es für jedermann ohne weiteres möglich, die Akte im Archiv aufzufinden.

Die Krankenhäuser haben zugesagt, die Mängel zu beheben und meine Empfehlungen zu realisieren. In einem Fall steht die abschließende Stellungnahme noch aus.

3.13.4 Ungeschützte Blutspenderdaten im Universitätsnetz

Ein anonymer Anrufer informierte mich darüber, daß ein Rechner, mit dem Daten der Blutbank der medizinischen Fakultät einer Universität verarbeitet werden, nicht ausreichend gegen Zugriff durch Unbefugte gesichert wäre. Er behauptete, diese Datenbestände jederzeit lesen und

verändern zu können. Die für den Zugriff erforderlichen Voraussetzungen (zum Beispiel Hostname und Paßwort) beschrieb er detailliert.

Damit die zu vermutenden Mängel in der Systemgestaltung und -administration so schnell wie möglich beseitigt werden konnten, informierte ich umgehend die Universität. In der Abteilung Transfusionsmedizin wurden tatsächlich solche Mängel ermittelt und sofort beseitigt. Unbefugte Zugriffe auf den Datenbestand der Blutbank wurden nicht festgestellt. Der Rechner, der manipuliert werden konnte, wurde lediglich als Printserver benutzt. Die Blutbankanwendung selbst lief schon seit geraumer Zeit auf einem anderen Gerät. Vorsorglich habe ich empfohlen, in Zusammenarbeit mit dem Universitätsrechenzentrum das lokale Netz der Blutbank besser gegen das übrige Universitätsnetz abzuschotten und so die Sicherheit gegen Manipulationsversuche zu erhöhen.

Um detaillierter zu einzelnen technischen und organisatorischen Maßnahmen beraten zu können, führte ich in der Abteilung Transfusionsmedizin einen Kontrollbesuch durch. Ich wurde darüber informiert, daß in dieser Abteilung verschiedene Blutprodukte hergestellt, geprüft und bereitgehalten werden. Zur Unterstützung der einzelnen Verfahrensschritte in dieser Blutbank dient ein lokales Rechnernetz, welches mit dem Universitätsnetz verbunden ist. An die Integrität und die Verfügbarkeit der dort verarbeiteten Daten werden höchste Anforderungen gestellt, da fehlerhafte Daten zur Gefahr für Leben und Gesundheit von Patienten werden können. Darüber hinaus werden im Blutbanksystem auch Daten der Spender verarbeitet.

Vor diesem Hintergrund waren folgende Feststellungen von Bedeutung:

- Die Verbindung zum Universitätsnetz dient vor allem der Datenübertragung zwischen zwei Standorten, an denen die Blutbankdaten benötigt werden. Daneben gibt es auch eine Verbindung zur zentralen Patientendatei. Detaillierte Analysen zum Kommunikationsbedarf waren jedoch bisher nicht erfolgt.

- Auf die Informationsdienste des Internet wird von separaten PC aus zugegriffen. Damit sind Hard- und Software für diese beiden Anwendungen wirkungsvoll voneinander getrennt. Mit dieser Konfiguration allein ist die erforderliche logische Netztrennung allerdings noch nicht sichergestellt.

- Die lokale Administration der Anwendung wies keine Schwachstellen mehr auf, die Anlaß zur Beanstandung gegeben hätten. Der Fernwartungzugang war jedoch noch nicht ausreichend gegen Zugriffsversuche durch Unbefugte gesichert.

- Die Grundsicherungsmaßnahmen des Universitätsrechenzentrums für den Netzwerkbetrieb erwiesen sich für eine derart sensible Anwendung als nicht ausreichend. Das Blutbanknetz wurde jedoch schon vor meinem Kontrollbesuch durch zusätzliche Abschottungsmaßnahmen (Firewalls) gesichert (siehe auch Zweiter Tätigkeitsbericht, Punkt 2.18.3).

- Bestimmte Dienste, die das Universitätsrechenzentrum zur Verfügung stellt beziehungsweise fordert, sind für den Betrieb sensibler Anwendungen ungeeignet. So sind MAC-Adressen (Media Access Control) von Ethernetkarten zur Authentifikation nicht ausreichend wirksam. Das gleiche gilt für die Sicherungsverfahren, die im Netzwerkmanagementprotokoll SNMP Version 1 (Simple Network Management Protocol) implementiert sind. Auch ein zentrales Backup von unverschlüsselten personenbezogenen Daten durch das Rechenzentrum ist nicht tragbar.

Auf der Basis dieser Feststellungen habe ich die folgenden Empfehlungen gegeben, um die Datensicherheit speziell für das Blutbanksystem zu verbessern:

- Der Kommunikationsbedarf der Blutbankanwendung mit anderen Systemen sollte geprüft werden. Dies ist notwendig, um diese Systeme sowie das Netzwerk so zu implementieren, daß von ihnen kein untragbares Risiko, insbesondere für die Integrität der Blutbankdaten, ausgeht.

- PC in der Abteilung Transfusionsmedizin, die zum Zugriff auf die Informationsdienste des Internet bestimmt sind, sollten in einem anderen logischen Netz betrieben werden als die Blutbankrechner.

- Wegen der besonders hohen Anforderungen an die Datenintegrität ist vor allem darauf zu achten, daß ausschließlich die zur Aufgabenerfüllung erforderliche Software installiert ist und nur tatsächlich notwendige Kommunikationsmöglichkeiten eingerichtet sind.

- Zur Sicherung der Integrität und der Vertraulichkeit der Blutbankdaten sollte zumindest bei der Übertragung über das Universitätsnetz eine Verschlüsselungslösung in Erwägung gezogen werden.

- Die Fernwartungszugänge sollten gleichfalls mit kryptographischen Mitteln gesichert werden.

Ich habe darauf hingewiesen, daß eine enge Zusammenarbeit mit dem Universitätsrechenzentrum erforderlich ist, um diese Empfehlungen umzusetzen. Gegebenenfalls müßten die technischen Sicherungsmaßnahmen des Rechenzentrums um weitere anwendungsbezogene Maßnahmen ergänzt werden.

Ich bin mit der Universität weiter im Gespräch und habe weitere Beratung angeboten.

3.14 Personalwesen

3.14.1 Personal- und Organisationsdatensystem in der Oberfinanzdirektion

Ein Landesbediensteter der Oberfinanzdirektion (OFD) teilte mir mit, daß die OFD das Personal- und Organisationsdatensystem (PODS) eingeführt hat, ohne die Betroffenen darüber zu informieren. Somit würden sie im unklaren gelassen, welche ihrer Daten automatisiert verarbeitet werden.

Auf meine Anfrage hin erhielt ich von der OFD die Auskunft, daß sie den Einsatz des PODS plant und dazu gemeinsam mit dem Personalrat eine Dienstvereinbarung entwickelt. Ob dieses System die gleichen Datenschutz- und Datensicherheitsanforderungen erfüllt wie das zu diesem Zweck als Landesstandard empfohlene Personal- und Stellenverwaltungssystem PERSYS (siehe Zweiter Tätigkeitsbericht, Punkt 2.13.3), konnte zunächst nicht beantwortet werden. Nachdem ich den Petenten darüber informierte, bekräftigte er, daß das PODS bereits eingesetzt wird. Dies habe ich zum Anlaß genommen, den Umgang mit Personalakten und Personaldaten bei der OFD zu kontrollieren.

Ich stellte fest, daß dieses System tatsächlich im Personalreferat bereits genutzt wurde. Die zuständigen Mitarbeiter erklärten, daß es sich im Teststadium befinde und noch nicht die Daten aller Bediensteten gespeichert seien. Der Personalrat habe der automatisierten Personaldatenverarbeitung grundsätzlich zugestimmt. Eine entsprechende Dienstvereinbarung werde vorbereitet. Vor diesem Hintergrund beanstandete ich den Umgang mit Personaldaten in der OFD und begründete dies wie folgt:

- PODS ist entgegen der Auskunft, daß seine Anwendung beabsichtigt sei, bereits genutzt worden.
- Die Betroffenen wurden nicht über die Art der über sie gespeicherten Daten informiert.
- Es lag keine Dienstvereinbarung zum Einsatz des Systems vor.
- Die technischen und organisatorischen Maßnahmen zum Schutz der Daten waren nicht ausreichend.

Die Finanzministerin teilte mir zu dem Kontrollbericht mit, daß die datenschutzrechtlichen Vorschriften künftig beachtet werden. Die beanstandeten Sachverhalte würden gemäß der empfohlenen Maßnahmen geändert. Darüber hinaus wird PODS in absehbarer Zeit durch das als Landesstandard empfohlene PERSYS ersetzt.

3.14.2 Aufbewahrung von Personalakten

Aus der Tagespresse hatte ich erfahren, daß Personalakten einer Amtsverwaltung auf der Straße gefunden worden waren. Zu diesen Unterlagen gehörten unter anderem Stellenbeschreibungen, Zeugnisse sowie Überprüfungsergebnisse des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU). Der Pressemeldung war weiter zu entnehmen, daß die Personalakten gestohlen waren. Ich forderte daraufhin die zuständige Amtsverwaltung auf mitzuteilen, welche technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten im Hause getroffen worden sind.

Das gesamte Gebäude der Amtsverwaltung ist durch eine Alarmanlage, die einem Wachdienst zugeschaltet ist, gesichert. Die Personalakten sowie die BStU-Bescheide wurden zum Zeit-

punkt des Diebstahls in einer verschlossenen Stahlkassette, die sich in einem Panzerschrank befand, aufbewahrt. Eine Mitteilung aller Betroffenen über den Diebstahl ihrer Personalakte sei zwischenzeitlich erfolgt. Da bei dem Einbruch nur die Unterlagen gestohlen wurden, die sich in der verschlossenen Kassette befanden, werde man diese künftig nicht mehr verschließen.

Eine derart leichtfertige Einstellung ist datenschutzrechtlich recht bedenklich und sie veranlaßte mich erneut, an den Amtsleiter heranzutreten und darauf hinzuweisen, daß diese Unterlagen einem besonderen Vertrauensschutz (Personalaktengeheimnis) unterliegen. Der Gesetzgeber hat diesem besonderen Schutzbedürfnis durch bereichsspezifische Regelungen zum Umgang mit personenbezogenen Daten bei Dienst- und Arbeitsverhältnissen Rechnung getragen. So sind die §§ 100 ff. Landesbeamtengesetz Mecklenburg-Vorpommern und für die Arbeiter und Angestellten die Vorschriften des Landesdatenschutzgesetzes von Mecklenburg-Vorpommern (§ 31 DSG MV) zu beachten.

Demzufolge ist der Dienstherr beim Umgang mit Personalakten verpflichtet, alle Vorkehrungen zu treffen, um diese Unterlagen vor dem Zugriff und der Einsichtnahme durch Dritte zu schützen. Eine Aufbewahrung in unverschlossenen Kassetten genügt diesen Anforderungen nicht. Es gehört zu den Aufgaben des Dienstherren, die Gefahren eines möglichen Datenmißbrauchs zu minimieren und zumindest die vorhandenen Sicherungsmöglichkeiten zu nutzen. Das bedeutet, daß die Amtsverwaltung die Kassetten auch dann zu verschließen hat, wenn sie in einem Stahlschrank aufbewahrt werden.

Ergänzend habe ich noch darauf hingewiesen, daß die Anfragen sowie die Bescheide des BStU nicht in der Personalakte aufbewahrt werden sollten, sondern in einer besonderen Sachakte.

Die Amtsverwaltung hat diese Hinweise berücksichtigt.

3.14.3 Umgang mit Bewerbungsunterlagen

Ein Behördenangestellter hatte sich für eine Stelle beworben, die im Zuständigkeitsbereich des Ministeriums liegt, bei dem er beschäftigt ist. Seine Bewerbung wurde abgelehnt. Das Ablehnungsschreiben und seine Bewerbung wurden ihm auf dem Dienstweg zurückgesandt. Dadurch

erhielt sein Dienstvorgesetzter von dieser Bewerbung Kenntnis. Der Angestellte fragte nun an, ob dieses Verfahren aus datenschutzrechtlicher Sicht zulässig ist.

Das Ministerium hat auf meine Frage nach der Rechtsgrundlage für diese Art der Zusendung mitgeteilt, daß die Beschäftigten gebeten worden sind, grundsätzlich in allen Belangen den Dienstweg einzuhalten. Darüber hinaus seien Beamte nach dem Landesbeamtengesetz (LBG M-V) und Angestellte nach dem Bundesangestelltentarifvertrag-Ost (BAT-O) verpflichtet, ihre Amtspflichten gewissenhaft zu erfüllen und den dienstlichen Anordnungen nachzukommen. Überdies sind alle Vorgesetzten nach der Gemeinsamen Geschäftsordnung der Ministerien des Landes Mecklenburg-Vorpommern (GGO I M-V) über wesentliche Angelegenheiten ihres Verantwortungsbereiches rechtzeitig auf dem Dienstwege zu informieren.

Weder das LBG M-V noch der BAT-O oder die GGO I M-V enthalten jedoch eine normenklare Rechtsgrundlage, die die Zusendung des Ablehnungsschreibens und anderer Bewerbungsunterlagen auf dem Dienstweg rechtfertigen würden. Nach dem Landesdatenschutzgesetz dürfen öffentliche Stellen mit den Daten ihrer Beschäftigten nur umgehen, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher organisatorischer, sozialer und personeller Maßnahmen erforderlich ist beziehungsweise andere Rechtsvorschriften oder eine Dienstvereinbarung das vorsehen (§ 31 Abs. 1 DSG MV). Der Umgang mit den Bewerbungsunterlagen des Betroffenen durch den Dienstvorgesetzten war zu keinem der genannten Zwecke erforderlich. Diese Beurteilung würde auch bei einer erfolgreichen Bewerbung zutreffen, denn es obliegt zunächst einmal dem Beschäftigten selbst, seinen Vorgesetzten rechtzeitig über den geplanten Wechsel zu informieren. Rechtzeitig und damit erforderlich ist eine solche Information aber erst dann, wenn beide Seiten übereinkommen, ein Beschäftigungsverhältnis aufzunehmen. Bei einer erfolgreichen Bewerbung wäre eine Information auf dem Dienstweg schon allein deshalb verfrüht, da der Betroffene sich immer noch anders entscheiden kann und die Stelle letztlich doch nicht annimmt.

Ich habe deshalb empfohlen, bei Bewerbungsverfahren auf die Einhaltung des Dienstweges zu verzichten und Schreiben sowie Unterlagen zu einem solchen Vorgang an die Privatadresse des Bewerbers zu senden. Das Ministerium hat mitgeteilt, daß es diese Empfehlung umsetzt.

3.14.4 Prüfung eines Schadensersatzanspruchs bei einem Verkehrsunfall mit einem Dienstkraftfahrzeug

Für die Schadensabwicklung von Verkehrsunfällen, an denen Dienstfahrzeuge des Landes beteiligt sind, ist das Finanzministerium zuständig. Nach einem solchen Verkehrsunfall erhielt ein Landesbediensteter zu diesem Zweck einen Erhebungsbogen, in dem er den Unfallhergang schildern sollte. Im Anschreiben wurde er darüber informiert, daß aus den bereits vorhandenen Unterlagen abgeleitet werden könne, daß er den Unfall möglicherweise grob fahrlässig verursacht habe. Um diese Vorwürfe zu prüfen, sei es daher erforderlich, die auf dem Erhebungsbogen gestellten Fragen zu beantworten. Da er gegen die umfangreiche Datenerhebung Bedenken hatte, bat er mich um datenschutzrechtliche Prüfung.

Neben Angaben zum Unfallhergang und zum technischen Zustand des Fahrzeuges sollte der Bedienstete auch seine soziale Situation darlegen, beispielsweise Familienstand, Anzahl der Kinder und Einkommen des Ehepartners. Außerdem sollte er vorhandene außergewöhnliche finanzielle Belastungen angeben. Zur Klärung der Schuldfrage waren diese Daten jedoch nicht erforderlich.

Ich habe empfohlen, das Verfahren zweistufig zu gestalten. Zunächst sollten die Fragen geklärt werden, die mit dem Unfall in unmittelbarem Zusammenhang stehen. Erst wenn aus diesen Daten abzuleiten ist, daß der Beschäftigte seine Sorgfaltspflicht vorsätzlich oder grob fahrlässig verletzt hat und er den entstandenen Schaden teilweise oder vollständig ersetzen muß, können Angaben über die soziale Situation des Beschäftigten in Betracht kommen. Diese Daten dürfen dann erhoben werden, wenn seine wirtschaftliche Lage so angespannt ist, daß die festgesetzte Kostenbeteiligung eine außergewöhnliche Härte darstellen würde oder er mit dem ihm zur Verfügung stehenden Teil seines Gehalts dann nicht mehr in ausreichendem Maße seinen Lebensunterhalt bestreiten könnte.

Das Finanzministerium ist meinen Empfehlungen gefolgt.

3.14.5 Weitergabe dienstlich erlangter Kenntnisse an Dritte

Beamte und Angestellte im öffentlichen Dienst haben über die ihnen bei ihrer Tätigkeit bekanntgewordenen dienstlichen Angelegenheiten zu schweigen. Diese Schweigepflicht ist für die Beamten im Landesbeamtengesetz (§ 64 LBG M-V) sowie für die Angestellten im Bundesangestelltentarifvertrag-Ost (§ 9 BAT-O) geregelt. Daß dem nicht immer die entsprechende Bedeutung beigemessen wird, zeigt folgendes Beispiel:

Ein Petent hatte sein Fahrzeug in einer Halteverbotzone abgestellt. Als er zu seinem Auto zurückkam, rief ihm der Mitarbeiter des Ordnungsamtes, der ihm namentlich bekannt war, zu: „Sie kommen sechs Minuten zu spät." Er ahnte, daß er demnächst einen Bußgeldbescheid wegen nicht ordnungsgemäßen Parkens erhalten wird. Da dieser zu Recht erteilt wurde, war die Angelegenheit für ihn zunächst erledigt. Um so erstaunter war er, als er am Abend des gleichen Tages von einem Nachbarn erfuhr, daß dieser genaustens über sein Vergehen informiert war. In dem Gespräch stellte sich heraus, daß dieser in der Mittagspause vom Mitarbeiter des Ordnungsamtes darüber in Kenntnis gesetzt worden war. Der Petent fragt nun an, ob hier eine Verletzung datenschutzrechtlicher Bestimmungen vorliegt.

Auf meine Anfrage bei der Stadtverwaltung wurde der betreffende Mitarbeiter aufgefordert, zum Sachverhalt Stellung zu nehmen. Er erklärte, da es sich bei dem Petenten um einen gemeinsamen Bekannten handele, hatte er sich mit dessen Nachbarn über die begangene Ordnungswidrigkeit unterhalten. Erst nachdem er vom Amtsleiter über die Einhaltung der Verschwiegenheitspflicht belehrt wurde, sei ihm sein Fehlverhalten klar geworden. Obwohl eine Dienstanweisung, die eine Verpflichtung zur Verschwiegenheit enthält, allen Mitarbeitern zur Kenntnis gegeben wurde, hatte er falsch gehandelt.

Um solchen Vorkommnissen künftig vorzubeugen, wurden alle Amtsleiter aufgefordert, ihre Mitarbeiter nochmals zu belehren. Insbesondere sollte darauf hingewiesen werden, daß dienstliche Angelegenheiten nicht Dritten gegenüber beziehungsweise in Anwesenheit Dritter zu erörtern sind. Des weiteren informierte mich der Bürgermeister, daß er sich bereits beim Petenten für das Verhalten seines Mitarbeiters entschuldigt hat.

Dieses Beispiel zeigt, daß ein Verstoß gegen die Verschwiegenheitspflicht allein schon dadurch vermieden werden kann, wenn die Mitarbeiter in regelmäßigen Abständen, beispielsweise durch den Dienstvorgesetzten, für die Fragen des Datenschutzes sensibilisiert werden.

3.14.6 Erteilung der Aussagegenehmigung durch Dienstvorgesetzte

Nach dem Landesbeamtengesetz (LBG M-V) darf ein Beamter über dienstliche Angelegenheiten, über die er Verschwiegenheit zu bewahren hat, ohne Genehmigung des Dienstvorgesetzten weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben. Soweit sich der fragliche Vorgang bei einem früheren Dienstherren ereignet hat, muß neben der Genehmigung des gegenwärtigen auch der frühere Vorgesetzte zustimmen (§ 64 Abs. 1 und 2 LBG M-V).

Vom Innenministerium war ich um eine Stellungnahme zu der Frage gebeten worden, ob durch die erforderliche Aussagegenehmigung des gegenwärtigen Dienstvorgesetzten in Angelegenheiten, die in einem früheren Dienstverhältnis begründet sind, nicht in unverhältnismäßiger Weise in die Persönlichkeitsrechte der in diesem Fall beteiligten Personen eingegriffen wird. Der gegenwärtige Vorgesetzte müsse hierzu von dem früheren Vorgesetzten Informationen einholen und möglicherweise Akten einsehen, um die Genehmigung begründen und erteilen zu können.

Ich habe dem Innenministerium mitgeteilt, daß eine Aussagegenehmigung nur versagt werden darf, wenn dadurch Nachteile zum Wohle des Bundes oder eines Landes entstehen würden oder eine öffentliche Aufgabe nicht mehr oder nur schwer erfüllt werden könnte (§ 65 Abs. 1 und 2 LBG M-V). Folglich muß auch nur geprüft werden, ob eine der genannten Bedingungen erfüllt ist und deshalb die Aussage nicht genehmigt werden darf. Für diese Prüfung ist eine Akteneinsicht im Regelfall nicht erforderlich. Es dürfte vielmehr ausreichend sein, wenn der Vorgesetzte den Beamten zum Sachverhalt befragt und die gesetzlich vorgeschriebene Zustimmung des früheren Vorgesetzten einholt. Dadurch wird meines Erachtens nicht in unzulässiger Weise in Persönlichkeitsrechte der Beteiligten eingegriffen, denn die Übermittlung oder Nutzung personenbezogener Daten ist regelmäßig nicht erforderlich.

Die landesrechtlichen Vorschriften zu diesem Sachverhalt müssen daher aus datenschutzrechtlichen Gründen nicht geändert werden.

3.14.7 Dürfen Gleichstellungsbeauftragte Personalakten einsehen?

Die Gleichstellungsbeauftragte der Landesregierung hat mir den Entwurf des ersten Änderungsgesetzes zum Gesetz zur Gleichstellung von Frau und Mann im öffentlichen Dienst des Landes Mecklenburg-Vorpommern zur Stellungnahme zugeleitet.

Im Entwurf war ein Einsichtsrecht der Gleichstellungsbeauftragten „in alle Akten, die Maßnahmen betreffen, an denen sie zu beteiligen ist“, vorgesehen. Eine solche Formulierung würde es der Gleichstellungsbeauftragten ermöglichen, auch die Personalakten der Beschäftigten einzusehen. Das verstößt gegen die Grundsätze des Personalaktenrechts.

Der Umgang mit den Personalakten der Landesbeamten ist in den §§ 100 - 107 Landesbeamtengesetz normiert. Entsprechende Regelungen für den Umgang mit Personalakten der Angestellten und Arbeiter im öffentlichen Dienst gibt es nicht. Der Innenminister hat jedoch zu den §§ 100 - 107 LBG M-V die Verwaltungsvorschrift „Richtlinien über die Führung von Personalakten“ erlassen, die im Geltungsbereich der obersten Landesbehörden sinngemäß auch für die Personalaktenführung der Angestellten und Arbeiter anzuwenden ist. Den Gemeinden, Städten, Landkreisen und Ämtern sowie den sonstigen Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts empfiehlt der Innenminister, ebenfalls entsprechend der Verwaltungsvorschrift zu verfahren (siehe auch Punkt 3.17.3). Im Ergebnis ist daher ein einheitlicher Maßstab an den Umgang mit Personalakten der Beamten, Angestellten und Arbeiter im öffentlichen Dienst des Landes anzulegen.

Nach den Vorschriften des LBG M-V und den Regelungen in der Richtlinie darf Einsicht in Personalakten ausschließlich nehmen, wer im Personalbereich mit der Bearbeitung von Personalangelegenheiten der betreffenden Beschäftigten beauftragt ist. Dritten kann grundsätzlich nur mit Einwilligung eines Betroffenen Einsicht gewährt werden. Auch zu Zwecken der Personalvertretung dürfen Personalakten lediglich mit Zustimmung des Beschäftigten und nur von den von ihm bestimmten Personalratsmitgliedern eingesehen werden.

Die Gleichstellungsbeauftragte ist nicht mit der Bearbeitung von Personalangelegenheiten betraut. Sie ist allerdings bei allen personellen, sozialen und organisatorischen Maßnahmen, die weibliche Beschäftigte betreffen, zu beteiligen. Ihre Funktion ist daher in dieser Beziehung mit der des Personalrates vergleichbar, dem ebenfalls ein - wenn auch umfassenderes - Beteiligungsrecht in den erwähnten Bereichen zusteht. Hieraus ergibt sich zwingend, daß auch der Gleichstellungsbeauftragten nur dann Einsicht in die Personalakte eines Beschäftigten gewährt werden darf, wenn dieser ausdrücklich eingewilligt hat. Das Einsichtsrecht der Gleichstellungsbeauftragten geht nicht über das Einsichtsrecht des Personalrates hinaus.

Es ist jedoch zu beachten, daß der Gleichstellungsbeauftragten im Vorfeld einer Einstellung ein umfassendes Einsichtsrecht in Bewerberunterlagen zusteht, da diese noch nicht dem Personalaktenrecht unterliegen.

Ich habe eine entsprechende Änderung des Gesetzentwurfes empfohlen. Bisher liegt noch kein neuer Entwurf zum Gesetz zur Gleichstellung von Frau und Mann im öffentlichen Dienst des Landes Mecklenburg-Vorpommern vor.

3.15 Bildung, Kultur, Wissenschaft und Forschung

3.15.1 Unzulässige Datenweitergabe und späte Einsicht im Kultusministerium

Ein Ehepaar wandte sich an das Kultusministerium und bat um Informationen, wie das Ministerium Werbeveranstaltungen an Schulen beurteilt und ob Rechtsgrundlagen zur Mitteilung von Noten in der Klasse existieren.

Das Ehepaar hatte im Briefkopf seine Adresse angegeben. Bereits bevor sie eine Antwort aus dem Ministerium erhielten, teilte ein Lehrer ihrer Tochter mit, daß er die Noten nicht mehr namentlich vor der Klasse verkünden wolle. Außerdem sollten die Eltern doch künftig zunächst mit dem Lehrpersonal Kontakt aufnehmen, ehe sie sich an das Kultusministerium wenden. Die Eltern waren über diese Äußerung sehr erstaunt, denn sie hatten in ihrer Anfrage bewußt nicht mitgeteilt, daß sie Kinder haben und wo diese zur Schule gehen. Sie wandten sich daraufhin an mich und baten um Prüfung des Vorfalls.

Meine Kontrolle im Kultusministerium ergab, daß sich ein Mitarbeiter aufgrund der Adresse an die örtlich zuständige Schule gewandt und unter Angabe des Namens des Ehepaares angefragt hat, ob deren Kinder dort zur Schule gehen. Bei dieser Recherche wurde der Schule mitgeteilt, daß sich die Petenten beim Kultusministerium „beschwert“ hätten.

Allein zur Beantwortung der Fragen war die Übermittlung des Namens des Ehepaares an die Schule nicht erforderlich. Dies habe ich bei der Kontrolle erläutert, und der zuständige Referatsleiter stimmte meiner Auffassung zu. Ich habe dem Kultusministerium Empfehlungen zum künftigen datenschutzgerechten Umgang mit Anfragen gegeben sowie um eine Stellungnahme gebeten. Der Inhalt dieser Stellungnahme war allerdings überraschend, denn entgegen der Einsicht während der Kontrolle wurde nunmehr von einem anderen Mitarbeiter des Ministeriums argumentiert, daß die Datenübermittlung erforderlich gewesen sein soll und nach dem Schulgesetz (SchulG M-V) auch zulässig sei. Begründet wurde dies damit, daß personenbezogene Daten von Schülern und Erziehungsberechtigten einer Schule, der Schulaufsichtsbehörde und dem Schulträger übermittelt werden dürfen, soweit sie von diesen zur Erfüllung der ihnen durch Rechtsvorschrift übertragenen Aufgabe benötigt werden (§ 70 Abs. 2 Satz 1 SchulG M-V).

Im folgenden Schriftverkehr habe ich dem Kultusministerium mehrfach ausführlich dargelegt, warum die Recherche und Ermittlung der Schule hinter dem Rücken der Eltern sowie die Bekanntgabe ihrer Namen nicht zulässig war. Das Kultusministerium hielt jedoch weiterhin an seiner Rechtsauffassung fest und signalisierte damit, bei ähnlichen Anfragen grundsätzlich genauso zu verfahren. Daraufhin habe ich die Datenübermittlung gegenüber der Kultusministerin förmlich beanstandet und zu einer weiteren Stellungnahme aufgefordert. Da auch danach keine Einsicht zu erkennen war, habe ich mich an die Öffentlichkeit gewandt und den Bürgern empfohlen, bei Anfragen an das Kultusministerium ausdrücklich auf vertraulicher Behandlung ihres Anliegens zu bestehen. Darüber hinaus informierte ich den Kultusausschuß des Landtages über den Vorgang.

Nachdem der Kultusausschuß meine Auffassung unterstützte und sich die Kultusministerin persönlich mit dem Sachverhalt beschäftigte, teilte sie mir mit, daß derartige Bürgeranfragen

künftig vertraulich behandelt werden. In einem Brief an die Eltern hat sie die fehlerhafte Bearbeitung in ihrem Hause bedauert.

Von meiner ersten Empfehlung bis zu dieser Einsicht sind neun Monate für die Lösung eines an sich unkomplizierten datenschutzrechtlichen Sachverhaltes vergangen.

3.15.2 Umgang mit Schülerdaten

Verschiedene Anfragen von Bürgern und Schülern zeigten, daß auch nach dem Inkrafttreten des Schulgesetzes für das Land Mecklenburg-Vorpommern (SchulG M-V) noch Unsicherheiten beim Umgang mit den personenbezogenen Daten der Schüler (Schülerdaten) und Eltern bestehen.

Kleiner Lauschangriff im Klassenzimmer

Ein Journalist teilte mir mit, daß ein Schulleiter mit Wissen einer Fachlehrerin das Unterrichtsgeschehen mit einem „Babyphon“ abgehört und auf Magnetband aufgezeichnet hat. Die Aufzeichnung sollte als Beweis für die Disziplinlosigkeit der Klasse dienen und auf einer Elternversammlung abgespielt werden.

Um den Vorgang datenschutzrechtlich beurteilen zu können, habe ich den Direktor der Schule befragt. Als Motiv für das „Belauschen“ gab er an, daß die Musiklehrerin bereits mehrfach über die Disziplinschwierigkeiten in der Klasse berichtet und ihn um Hilfe gebeten hatte. Da der Direktor ebenfalls in der Klasse Unterricht erteilt, aber diese Disziplinlosigkeit bisher nicht festgestellt hatte, nahm er an, daß seine Hospitation in der Musikstunde wahrscheinlich erfolglos bleiben würde. Außerdem seien in der Vergangenheit die Aussagen der Lehrer auf Elternversammlungen über die schlechte Disziplin der Schüler in bestimmten Unterrichtsstunden bezweifelt worden, so daß er über diesen Weg den Eltern einen „Beweis“ liefern wollte.

Ich habe ihn auf die Unzulässigkeit der heimlichen Datenerhebung und -speicherung hingewiesen. Er sollte besser sofort eingreifen, wenn die Schüler in einer Unterrichtsstunde derart lärmen, daß dadurch der Unterricht in benachbarten Klassenzimmern beeinträchtigt ist. Dazu be-

darf es jedoch keines „Lauschangriffes“. Dies hat der Direktor eingesehen und versichert, meine Empfehlung zu beachten.

Bekanntgabe schulischer Leistungen vor der Klasse

Häufig erhalte ich Anfragen von Eltern und Lehrern, ob die Note eines Schülers vor der Klasse bekanntgegeben werden darf. Die Eltern möchten einerseits darüber informiert werden, wie sich die Leistung ihres Kindes zu derjenigen der Klasse verhält. Andererseits sehen sie teilweise selbst ein, daß das Recht auf informationelle Selbstbestimmung diesem Informationsanspruch gewisse Grenzen setzt.

Ich habe empfohlen, bei schriftlichen Leistungskontrollen einen Notenspiegel oder den Notendurchschnitt bekanntzugeben.

In einem anderen Fall hat eine Lehrerin die Schüler einer 12. Klasse durch Handzeichen darüber abstimmen lassen, ob sie mit der Bekanntgabe der Noten ihrer schriftlichen Arbeit vor der Klasse einverstanden sind. Die Noten derjenigen Schüler, die damit nicht einverstanden waren, wurden nicht genannt. Trotz dieser „Einwilligung“ halte ich das Verfahren für nicht zulässig, weil die Bekanntgabe der Noten weder zur Erfüllung eines Informationsanspruchs noch zu einer anderen Aufgabe erforderlich ist. Die Einwilligung zum Umgang mit personenbezogenen Daten kommt nur dann in Frage, wenn die Daten zur gesetzlichen Aufgabenerfüllung einer Stelle erforderlich sind und keine Rechtsvorschrift existiert, die diesen Umgang ausdrücklich erlaubt. Im übrigen erfüllt eine Abstimmung auch nicht die formalen Voraussetzungen an eine Einwilligung im datenschutzrechtlichen Sinne.

Anders zu beurteilen ist die Bekanntgabe der Note allerdings bei mündlichen Leistungskontrollen vor der Klasse. Ein Schuldirektor berichtete mir, daß ein Schüler sich gegen die Bekanntgabe seiner mündlichen Note mit dem Hinweis auf den Datenschutz ausgesprochen hatte und fragte, welche Auffassung ich hierzu vertrete. Wird eine solche Leistung vor der Klasse erbracht, so ist die Bekanntgabe dieser Note sicher aus pädagogischen Gründen erforderlich und damit zulässig. Die anderen Schüler haben in diesem Fall ein berechtigtes Interesse an dem Bewertungsergebnis und daran, wie es begründet wird. Sie müssen erfahren können, was der

Lehrer positiv und was er negativ bewertet hat und wie das Ergebnis zustande kam, um ihren eigenen Wissensstand und ihre mündliche Leistung bewerten zu können.

Ausforschung der Schüler oder Vermittlung von Unterrichtsstoff?

Es erreichten mich auch mehrere Anfragen sowohl von Lehrkräften als auch von Eltern, wie mit personenbezogenen Daten zur Erreichung der Unterrichtsziele umgegangen werden darf. Auch hierzu einige Beispiele:

Im Mathematikunterricht wurde das Stoffgebiet Stochastik behandelt. Zum Zweck einer besseren Anschaulichkeit hatte der Fachlehrer auf der Grundlage einer Rahmenrichtlinie des Kultusministeriums zum Mathematikunterricht einen Erhebungsbogen erarbeitet. Die Erfahrungswelt der Schüler sollte hierbei einbezogen werden. So wurde unter anderem nach der Höhe des Taschengeldes im Monat und nach der Zahlweise (täglich/wöchentlich/monatlich/unregelmäßig) gefragt. Der Vater eines Schülers hat sich über diese „Ausforschung“ bei mir zu Recht beschwert. Deshalb habe ich geraten, Beispiele künftig sensibler auszuwählen. Dem Kultusministerium habe ich empfohlen, die Rahmenrichtlinien für den Unterricht an den Schulen des Landes auf datenschutzrechtlich bedenkliche Inhalte durchzusehen und entsprechend zu ändern. Das Ministerium hat mitgeteilt, daß das Landesinstitut für Schule und Ausbildung (L.I.S.A.) damit beauftragt wurde.

In einem anderen Fall sollten Schüler im Deutschunterricht eine Selbstdarstellung schreiben und dabei insbesondere die Personen nennen, die ihnen auf ihrem bisherigen Lebensweg geholfen haben, und beschreiben, auf welche Art und Weise sie dies taten. Eine Mutter befürchtete, daß die Lehrerin Interna der Familie ausforschen wollte, und wandte sich deshalb an mich. Ein solches Thema ist durchaus geeignet, die Schüler auf ihr künftiges Leben vorzubereiten und aus datenschutzrechtlichen Gründen nicht prinzipiell abzulehnen. Allerdings muß auch dabei die Privatsphäre respektiert werden. Deshalb habe ich der Lehrerin empfohlen, die Schüler und gegebenenfalls die Eltern bei solchen Themenstellungen auf den Datenschutz hinzuweisen. Des weiteren sollte Schülern, die ihren Lebensweg nicht offenbaren wollen, eine Alternative angeboten werden. Beispielsweise könnte das Thema auch auf der Grundlage einer veröffentlichten Biographie einer Person der Zeitgeschichte behandelt werden.

3.15.3 Datenübermittlung von der Schule in den Papierkorb des Jugendamtes?

Anläßlich einer Kontrolle im Jugendamt eines Landkreises erfuhr ich, daß die Schulen auf der Grundlage des § 60 Abs. 6 Satz 1 Schulgesetz Mecklenburg-Vorpommern (SchulG M-V) die Jugendämter regelmäßig unterrichten, wenn bestimmte Ordnungsmaßnahmen gegen Schüler in Betracht kommen oder bereits eingeleitet worden sind. Derartige Maßnahmen sind zum Beispiel der Ausschluß vom Unterricht oder die Verweisung von der Schule. Im Rahmen der Kontrolle teilte mir der Amtsleiter mit, daß diese personenbezogenen Daten zu einem großen Teil nicht benötigt und daher vernichtet werden. Bei einem weiteren Kontrollbesuch in einem anderen Jugendamt wurde mir bestätigt, daß die Informationen über schulische Ordnungsmaßnahmen in vielen Fällen nicht verwertet werden können.

Die Jugendämter nehmen regelmäßig Aufgaben der Kinder- und Jugendhilfe nach dem Achten Buch des Sozialgesetzbuches (SGB VIII) wahr. Im Rahmen dieser Aufgaben sollen unter anderem Eltern bei der Erziehung beraten und unterstützt sowie Kinder und Jugendliche vor Gefahren für ihr Wohl geschützt werden. Weil die Erziehung Recht und Pflicht der Eltern ist, über deren Betätigung der Staat lediglich wacht, hat das Jugendamt zunächst nur die Möglichkeit, präventive Angebote allgemeiner Art, wie zum Beispiel Beratungen, bereitzustellen, die Mütter, Väter oder sonstige Personensorgeberechtigte ebenso wie Kinder und Jugendliche bei Bedarf nutzen können. Ist das Wohl des Kindes oder des Jugendlichen jedoch gefährdet, ist das Jugendamt berechtigt, von Amts wegen tätig zu werden und gezielte Maßnahmen zum Schutz des Kindes oder des Jugendlichen - auch gegen den Willen der Eltern - zu treffen.

Wenn ein Schüler bereits vom Jugendamt betreut wird, ist die Information über etwaige Ordnungsmaßnahmen für die Aufgabenerfüllung des Amtes sinnvoll und im datenschutzrechtlichen Sinne erforderlich. Anders ist dies aber zu bewerten, wenn ein Schüler dem Jugendamt vor der Unterrichtung über die geplante oder bereits verhängte „Schulstrafe“ noch nicht bekannt war. In diesen Fällen ist es dem Amt nicht möglich, lediglich aufgrund dieser Information personenbezogen tätig zu werden. Eine schulische Ordnungsmaßnahme berechtigt das Jugendamt in Ermangelung einer konkreten Gefährdung nicht, von Amts wegen gezielte Maßnahmen zum Schutz des Wohls des betreffenden Schülers einzuleiten. Es benötigt daher auch seine personenbezogenen Daten nicht.

Ich halte die Regelung des § 60 Abs. 6 Satz 1 SchulG M-V für praxisfremd und verfassungsrechtlich zweifelhaft. Letzteres insbesondere deshalb, weil Jugendämter bei der geschilderten Verfahrensweise Datensammlungen anlegen können, die zu ihrer Aufgabenerfüllung nicht erforderlich und damit unzulässig sind. Daher habe ich dem Kultusministerium empfohlen, die Verfassungsmäßigkeit der Vorschrift prüfen zu lassen und bei einer Novellierung des Schulgesetzes auf die Streichung dieses Satzes hinzuwirken. Das Kultusministerium hält jedoch weiterhin an der Auffassung fest, daß die gesetzlich vorgesehene regelmäßige Unterrichtung der Jugendämter zu deren Aufgabenerfüllung in jedem Fall erforderlich ist.

Bei einer Novellierung des Schulgesetzes werde ich noch einmal Stellung nehmen und die Streichung des § 60 Abs. 6 Satz 1 SchulG M-V empfehlen.

3.15.4 Antrag auf Kostenzuschuß zur Schülerbeförderung

Ein Bürger übersandte mir einen zwanzigseitigen Antragsformularsatz für einen Kostenzuschuß zur Schülerbeförderung durch den Landkreis. Weil ihm die Menge der abgefragten Daten datenschutzrechtlich bedenklich schien, bat er mich, die Fragebögen zu prüfen.

Nach Mitteilung des Schulverwaltungsamtes des Landkreises sollte der Fahrtkostenzuschuß laut Satzung auf Antrag „in Anlehnung an das Bundesausbildungsförderungsgesetz (BAföG)“ gewährt werden. Entsprechend dieser Vorgabe hatte der Antragsteller umfangreiche Angaben zu seinem Einkommen und dem seiner Eltern oder Unterhaltsverpflichteten zu machen, die in die Berechnung des Zuschusses einfließen sollten.

Obwohl einige der erfragten Daten für die Gewährung eines Fahrtkostenzuschusses nicht erforderlich waren, deckte die Satzung durch die Anlehnung an das BAföG-Verfahren grundsätzlich die Datenerhebung des Schulverwaltungsamtes. Aus datenschutzrechtlicher Sicht ist jedoch ein Verwaltungsverfahren, das eine Erhebung einer Vielzahl von personenbezogenen Daten erfordert, dann bedenklich, wenn es - wie in diesem Fall - außer Verhältnis zu dem verfolgten Zweck steht. Ich habe daher die Vereinfachung des Antragsverfahrens, insbesondere der Fragebögen, empfohlen. Der Landkreis hat mir mitgeteilt, daß er meiner Empfehlung folgt.

3.15.5 Datenerhebung an den Musikschulen des Landes

Ein kommunaler Datenschutzbeauftragter informierte mich, daß das Kultusministerium unseres Landes Personaldaten der an den Musikschulen tätigen Lehrer erhebt. Die Schulleiter wurden aufgefordert, neben Namen und Vornamen auch Qualifikation, Einstufung, Unterrichtsfächer sowie die Anzahl der Wochenstunden anzugeben. Eine Rechtsgrundlage hierfür war seiner Meinung nach nicht vorhanden, so daß er mich um Beratung bat.

Auf meine Anfrage zur Rechtsgrundlage teilte mir das Kultusministerium mit, daß die Daten aufgrund der „Richtlinie über die Gewährung von Zuwendungen zur Förderung der Musikschulen in Mecklenburg-Vorpommern“ in Verbindung mit der Landeshaushaltsordnung erhoben werden. Die Angabe des Namens sei erforderlich, um zu prüfen, ob hauptamtlich vollbeschäftigte Lehrer auch als nebenberuflich Beschäftigte geführt werden und die Schulen somit möglicherweise unberechtigte Zuwendungen erhalten. Dies sei in der Vergangenheit bereits in vereinzelten Fällen vorgekommen.

Die Richtlinie regelt, daß das Land den Musikschulen Zuwendungen zu den Personalkosten der haupt- und nebenberuflich tätigen Lehrer gewähren kann, wenn bestimmte Voraussetzungen erfüllt sind. Beispielsweise müssen die Musikschulen bestimmte Fachbereiche (Musikalische Früherziehung oder Musikalische Grundausbildung) eingerichtet haben, und die überwiegende Zahl der Lehrkräfte muß über einen Abschluß als Diplommusikerzieher beziehungsweise eine gleichwertige Ausbildung verfügen. Des weiteren ist geregelt, daß dem Antrag auf Zuwendungen eine namentliche Aufstellung der beschäftigten Musiklehrer beizufügen ist.

Weder die vom Kultusministerium angeführten Normen der Landeshaushaltsordnung noch die Richtlinie rechtfertigten eine Einschränkung des informationellen Selbstbestimmungsrechts der Musiklehrer. Ohne Einwilligung der Betroffenen ist eine Datenerhebung nur zulässig, wenn ein Gesetz es erlaubt. Dieses Gesetz muß bestimmen, welche Daten erforderlich sind und zu welchem Zweck sie erhoben werden. Diese Rechtslage habe ich dem Kultusministerium mitgeteilt und empfohlen, die Richtlinie entsprechend zu überarbeiten und künftig im Rahmen des Zuwendungsverfahrens auf die Namen der beschäftigten Lehrer zu verzichten.

Das Kultusministerium hat meine Empfehlung umgesetzt.

3.16 Wirtschaft und Gewerbe

3.16.1 Imagekampagne Mecklenburg-Vorpommern

Im Vorfeld der derzeit durchgeführten bundesweiten Anzeigenkampagne für unser Land hatte mich die von der Staatskanzlei beauftragte Werbeagentur gebeten, das geplante Konzept datenschutzrechtlich zu prüfen. In jedem Anzeigenmotiv wurde eine Telefonnummer angegeben, um interessierten Lesern die Kontaktaufnahme mit der Landesregierung zu ermöglichen. Diese Anrufe sollten in einer externen zentralen Annahmestelle, einem sogenannten Call-Center, entgegengenommen, personenbezogene Angaben der Anrufer abgefragt und in einer Datenbank nach verschiedenen Interessentengruppen differenziert gespeichert werden. Das Call-Center sollte diese Daten täglich an die Agentur übermitteln, die diese je nach Interessentengruppe an entsprechende Ansprechpartner in Verbänden und Verwaltung weiterleiten wollte. Dieses Vorgehen sollte in erster Linie eine sachgerechte Beantwortung der unterschiedlichen Fragen ermöglichen. Es war auch geplant, die Daten statistisch aufzubereiten, damit die Landesregierung die Wirksamkeit und Reichweite der Kampagne einschätzen kann.

Der oben skizzierte Umgang mit personenbezogenen Daten bei Agentur und Call-Center ist Datenverarbeitung im Auftrag im Sinne des § 4 DSG MV. Die Staatskanzlei ist im vorliegenden Fall der Auftraggeber, und sie bleibt somit für die Einhaltung datenschutzrechtlicher Vorschriften bei den Auftragnehmern verantwortlich. Zum Verfahren habe ich folgende Empfehlungen gegeben:

- Die Anrufer sollten darauf hingewiesen werden, daß das Call-Center eine private Stelle ist, die im Auftrag der Landesregierung Informations- und Vermittlungsdienste anbietet und zu diesem Zweck auch personenbezogene Daten speichert und übermittelt.

- Den Anrufern sollte - alternativ zur Bekanntgabe eigener Daten - auch die Möglichkeit eingeräumt werden, von sich aus mit den Ansprechpartnern in Kontakt zu treten, indem ihnen Institution, Name und Telefonnummer auf Wunsch genannt werden.

– Die Staatskanzlei erteilt den Auftrag schriftlich. Dabei ist unter anderem der Datenumfang sowie der Zweck und die Art des Umganges festzulegen, und es sind technische und organisatorische Maßnahmen zum Schutz der Daten zu bestimmen. Darüber hinaus ist die Löschung der Daten nach Durchführung der Kampagne vorzusehen.

– Die Staatskanzlei hat die Agentur zu verpflichten, sich der Kontrolle des Landesbeauftragten für den Datenschutz zu unterwerfen, und die Einhaltung datenschutzrechtlicher Vorschriften bei dem Call-Center zu überwachen.

Diese Empfehlungen wurden vollständig umgesetzt.

3.16.2 Personalbogen der Ingenieurkammer

Ein Petent bat um Prüfung eines Erhebungsbogens, den ihm die Ingenieurkammer Mecklenburg-Vorpommern anläßlich der Aktualisierung des Mitgliederverzeichnisses übersandt hatte. Er hatte datenschutzrechtliche Bedenken, weil er eine Vielzahl persönlicher Daten preisgeben sollte und weil der Fragebogen weder einen Hinweis über die Verwendung der Daten noch darüber enthielt, ob und welche Angaben freiwillig waren. Neben dem Geburtsdatum und -ort des Kammermitgliedes sollte auch mitgeteilt werden, bei welcher Versicherungsgesellschaft die Berufshaftpflichtversicherung abgeschlossen worden ist. Überdies sollte der Befragte detaillierte Angaben zu Pflichtmitgliedschaften in weiteren Kammern und zu Mitgliedschaften in Ingenieurverbänden machen und mitteilen, ob er als betrieblicher Beauftragter für Sicherheit, Umweltschutz oder für ein anderes Gebiet bestellt ist.

Die Prüfung des Fragebogens ergab, daß lediglich ein Teil der geforderten personenbezogenen Daten für die Erfüllung der Kammeraufgaben und -pflichten nach dem Ingenieurgesetz Mecklenburg-Vorpommern (IngG M-V) und der Kammersatzung erforderlich war. Nicht erforderlich waren die Angaben zu dem Geburtsdatum und -ort, zur Versicherungsgesellschaft, zu weiteren Mitgliedschaften in Kammern und Verbänden sowie zur Tätigkeit als betrieblicher Beauftragter. Diese Daten konnten deshalb lediglich auf freiwilliger Basis erhoben werden.

Ich habe der Ingenieurkammer daher folgende Empfehlungen gegeben:

- Der Erhebungsbogen soll in Pflichtangaben nach dem IngG M-V und der Kammersatzung und in freiwillige Angaben untergliedert werden. Dabei ist zu kennzeichnen, welche Daten pflichtgemäß anzugeben sind und welche Daten auf freiwilliger Basis angegeben werden können. Die Kammermitglieder sind darüber zu informieren, daß der Erhebungsbogen überarbeitet und umstrukturiert worden ist.

- Den Kammermitgliedern soll ein Widerspruchsrecht bei den bereits erhobenen Daten, deren Angabe freiwillig ist, eingeräumt werden. Sie sind auf die Möglichkeit der Datenlöschung und auf deren Folgen hinzuweisen.

- Die Betroffenen sind umfassend darüber aufzuklären, zu welchem Zweck die Daten verarbeitet und genutzt werden.

- Es soll eine Dienstanweisung zum Umgang mit den Daten ausgearbeitet werden, in der Aufbewahrungs- und Löschungsfristen festzulegen und die Zugriffsberechtigung und Datensicherung zu regeln sind. Überdies sind technische und organisatorische Maßnahmen zum Schutz der Daten gemäß § 17 DSG MV zu treffen und die bisher noch nicht vorliegende Dateibeschreibung und ein Geräteverzeichnis nach Maßgabe des § 16 DSG MV anzulegen und zu führen.

Meine Empfehlungen sind vollständig umgesetzt worden.

3.16.3 Sparkassenunterlagen im Papiercontainer

So oder ähnlich lautende Meldungen hatte ich in den letzten Jahren bereits mehrfach den Medien entnommen. In diesem Fall wurde darüber berichtet, daß Bürger Überziehungs- und Dispositionslisten aus den Jahren 1990 und 1991 hinter Altstoffbehältern gefunden hatten. Auf diesen Listen waren die Namen der Kunden und Beträge vermerkt. Auf meine Anfrage bei der zuständigen Kreissparkasse schilderte mir der Vorstand den Sachverhalt wie folgt:

Die Sparkasse ist bereits 1992 in ein anderes Gebäude gezogen. Es sei damals jedoch versäumt worden, sämtliche Unterlagen aus dem alten Gebäude zu entfernen. Beim Abriß des ehemaligen Sparkassengebäudes wurden die Unterlagen gefunden und ohne Rückfrage bei der Sparkasse im Container entsorgt. Sofort, nachdem die Sparkasse von dem Vorfall Kenntnis hatte, erhielt die Innenrevision den Auftrag, den Sachverhalt aufzuklären. Mitarbeiter suchten die ehemalige Geschäftsstelle und deren nähere Umgebung sowie mögliche Entsorgungscontainer nach weiteren Unterlagen ab. Um künftig solche Vorkommnisse auszuschließen, wurden die Führungskräfte und die Mitarbeiter belehrt.

Der Vorstand teilte des weiteren mit, daß jeder Mitarbeiter bereits bei der Einstellung auf die Einhaltung der datenschutzrechtlichen Bestimmungen verpflichtet wird. Er erhält den Leitfaden „Datenschutz am Arbeitsplatz“ mit dem Hinweis, daß dieser Anweisungscharakter hat. Die Vernichtung der Sparkassenunterlagen erfolgt seit 1995 durch eine Entsorgungsfirma.

Die bereits eingeleiteten Maßnahmen waren meines Erachtens geeignet, um sicherzustellen, daß sich derartige Vorfälle künftig nicht wiederholen. Der Leitfaden „Datenschutz am Arbeitsplatz“ stellte allerdings nur auf die Regelungen des Bundesdatenschutzgesetzes ab, so daß ich dazu noch folgende Hinweise gegeben habe:

Soweit öffentlich-rechtliche Unternehmen, wie die Sparkassen, in den Wettbewerb mit privaten Unternehmen treten, sind auf diese grundsätzlich die Vorschriften des Bundesdatenschutzgesetzes anzuwenden. Gleichwohl gelten für sie die in § 2 Absatz 4 DSG MV explizit genannten Normen des Landesdatenschutzgesetzes. So unterliegen sie meiner Kontrolle und nicht - wie in dem Leitfaden ausgeführt - der Kontrolle der Aufsichtsbehörde (hier: dem Innenministerium). Bei einer Überarbeitung des Leitfadens sollten daher die für die Sparkassen geltenden Rechtsvorschriften eingearbeitet werden. Bis dahin habe ich empfohlen, dies in Form eines Beiblattes vorzunehmen. Darüber hinaus war auch ein Abschnitt „Maßnahmen der Datensicherung“ enthalten. Da dieser jedoch lediglich eine Aufzählung unterschiedlicher Maßnahmen enthielt, habe ich empfohlen, die zum Schutz personenbezogener Daten erforderlichen technischen und organisatorischen Maßnahmen gesondert in einem Datenschutz- und Datensicherheitskonzept festzulegen. Diese sollten auf die in der Sparkasse vorhandenen Bedingungen abgestellt werden.

Diese Hinweise werden nunmehr berücksichtigt.

3.16.4 Vorlage von Mitgliederlisten bei staatlicher Projektförderung

Der Vorstand eines eingetragenen Vereins beantragte für ein Projekt Mittel aus dem Europäischen Fonds für regionale Entwicklung. Mit der Eingangsbestätigung erhielt er auch eine Aufstellung der noch einzureichenden Unterlagen. Ein halbes Jahr später forderte die Bewilligungsbehörde zusätzlich eine namentliche Liste aller Vereinsmitglieder. Diese Forderung hat der Verein mit dem Hinweis auf den Datenschutz abgelehnt. Er bot jedoch an, die Mitgliederliste für Kontrollzwecke im Büro des Vereins einzusehen. Dieser Vorschlag schien für beide Seiten akzeptabel zu sein. Um so erstaunter war der Vereinsvorstand, daß im Zuwendungsbescheid als Auflage doch wieder die Vorlage einer Mitgliederliste verlangt wurde. Ich wurde gebeten, den Sachverhalt zu prüfen.

Die Bewilligungsbehörde hat mir als Rechtsgrundlage § 44 in Verbindung mit § 23 der Landeshaushaltsordnung (LHO) genannt. Darüber hinaus habe der Europäische Rechnungshof die Vorlage der Mitgliederliste bei der Förderung von Vereinen empfohlen. Nur so könnten mögliche Unregelmäßigkeiten, wie die Bevorteilung von Vereinsmitgliedern durch sogenannte Scheingeschäfte, weitgehend ausgeschlossen werden. Dieser Empfehlung des Europäischen Rechnungshofes werde gefolgt. Sie sei auch allen Vereinen bekannt.

Die Vorschriften der LHO erfüllen jedoch nicht die Anforderungen, die an Rechtsgrundlagen zu stellen sind, welche in die Persönlichkeitsrechte der Betroffenen eingreifen. Gleiches gilt für die Empfehlungen des Europäischen Rechnungshofes.

Es war also zu prüfen, ob eine Nutzung der Mitgliederliste nach den Vorschriften des Landesdatenschutzgesetzes (DSG MV) zulässig ist. Dort ist geregelt, daß personenbezogene Daten, die für andere Zwecke erhoben oder erstmalig gespeichert worden sind, zur Aufsicht, Kontrolle oder Rechnungsprüfung nur dann genutzt werden dürfen, wenn die konkrete Aufgabe ohne sie nicht oder nicht rechtmäßig erfüllt werden kann.

Ich habe folgende Verfahrensweise empfohlen:

Die Bewilligungsbehörde sollte zunächst nur die eingereichten Projektunterlagen prüfen. Gibt es Hinweise darauf, daß die Fördergelder möglicherweise nicht zweckentsprechend verwendet werden, ist im zweiten Schritt zu prüfen, ob eine Mitgliederliste überhaupt geeignet ist, diesen Mißbrauch festzustellen. Wird dieses bejaht, ist es datenschutzrechtlich nicht zu beanstanden, wenn die Bewilligungsbehörde die Vorlage der Liste fordert. In die Unterlagen ist nur ein Vermerk aufzunehmen, daß die Liste vorgelegen hat und zu welchem Ergebnis die Prüfung führte. Die Mitgliederliste wird urschriftlich an den Verein zurückgeschickt. Sie muß für weitere Prüfungen und Kontrollen zur Verfügung stehen. Mit diesem Verfahren wird erreicht, daß die Daten nicht in unverhältnismäßiger Weise in den Unterlagen gespeichert werden.

Die Bewilligungsbehörde hat mitgeteilt, daß sie künftig entsprechend diesen Empfehlungen verfahren wird.

3.17 Forschungsprojekte im Land

3.17.1 Umfrage bei älteren Mietern

Eine kommunale Wohnungsbau- und Verwaltungsgesellschaft wollte zweitausend ihrer Mieter im Alter ab fünfzig Jahre zu Problemen des selbstbestimmten Wohnens befragen und bat mich, das geplante Verfahren zu prüfen. Die Umfrage sollte auf freiwilliger Basis erfolgen, und es war der Einsatz von Interviewern vorgesehen. Die Ergebnisse sollten der Gesellschaft ermöglichen, die Bedürfnisse älterer Mieter bei weiteren Bauvorhaben stärker zu berücksichtigen.

Auf dem Fragebogen befand sich eine Kennziffer, aus der sich Stadtteil und Straße des jeweiligen Interviews ersehen ließen. Die Mieter sollten unter anderem detaillierte Fragen nach ihrem Familienstand, nach der Rentenart sowie nach der Höhe des monatlichen Haushaltsnettoeinkommens beantworten und angeben, ob sie ergänzend Sozialhilfe beziehen. Überdies sollten die Befragten Auskunft über ihre Krankheiten geben, sofern diese zu Beeinträchtigungen in der Wohnung oder im unmittelbaren Wohnumfeld führen.

Die Befragung in der geplanten Form hielt ich wegen der fehlenden Anonymität für datenschutzrechtlich bedenklich. Die Angaben hinsichtlich des Familienstandes, des Renten- und Sozialhilfebezuges sowie des Haushaltsnettoeinkommens im Zusammenhang mit Stadtteil und Straße schienen überdies für den Befragungszweck auch nicht erforderlich zu sein. Gleiches galt für die Frage nach Erkrankungen. Zudem war durch den vorgesehenen Einsatz von Interviewern die Freiwilligkeit zumindest in der Hinsicht eingeschränkt, daß die Mieter nicht die Wahl hatten, den Fragebogen auch allein auszufüllen.

Auf meine Empfehlung hin hat die Gesellschaft die betroffenen Mieter schriftlich um ihre Einwilligung in eine Befragung durch Interviewer gebeten. Die Kennziffer auf den Fragebögen wurde dergestalt geändert, daß keine Rückschlüsse auf die interviewte Person mehr möglich waren. Bei der Frage nach dem Familienstand wurden die Kategorien „verwitwet“ und „geschieden“ zu „alleinlebend“ zusammengefaßt. Die Auskunft über bestimmte Erkrankungen, so teilte mir die Gesellschaft mit, sei für die gesamte Studie von außerordentlicher Wichtigkeit, weil sich daraus erhebliche Konsequenzen für die Gestaltung der Wohnung und des Wohnumfeldes ergäben. Sie versicherte jedoch, daß bei der Auswertung nur das Vorliegen der Krankheit an sich von Bedeutung sei, so daß kein Identifizierungsrisiko bestünde. Die Angaben zum Renten- bzw. Sozialhilfebezug sowie zum Haushaltsnettoeinkommen sollten der Einordnung der Mieter in Sozialkategorien dienen. Die Mieter wurden noch einmal ausdrücklich auf die Freiwilligkeitder gesamten Befragung hingewiesen.

3.17.2 Wie familienfreundlich ist unsere Stadt? - Tücken einer Bürgerbefragung

Der Bürgermeister einer Stadt plante eine Bürgerbefragung und bat um Prüfung des dazu erarbeiteten Fragebogens. Ziel der Befragung war, einen Überblick über die Wohn- und Lebenssituation der Einwohner zu erhalten, um deren Interessen bei der künftigen Stadtentwicklung berücksichtigen zu können. Die Fragebögen sollten nach dem Zufallsprinzip per Postwurfsendung verteilt werden. Die Teilnahme sollte freiwillig sein.

Im Entwurf des Fragebogens wurde die Bürgerbefragung als „anonym“ bezeichnet. Diese Bezeichnung traf jedoch nicht zu. Es wurde unter anderem nach Alter und Anzahl der Familienmitglieder und danach gefragt, ob diese im gleichen Haushalt leben. Da zum Beispiel eine

Familie mit vier Kindern statistisch gesehen selten ist, könnte durch einen Abgleich dieser Angaben mit Daten aus dem Melderegister der Personenbezug ohne weiteres wiederhergestellt werden. Zur Beantwortung anderer Fragen waren Freitextangaben der Bürger nötig. Hier wäre die Identifizierung der Befragten durch Handschriftenvergleich möglich.

Ich habe empfohlen, der Postwurfsendung ein detailliertes Informationsblatt beizufügen und auf diese Weise die Bürger deutlich darüber aufzuklären, daß die Befragung freiwillig ist und daß die Ergebnisse in nicht-personenbezogener Form dargestellt werden. Über die Verarbeitung und Nutzung der Daten sollte umfassend informiert werden. Hinsichtlich des Umganges mit den Fragebögen habe ich überdies darauf hingewiesen, daß technische und organisatorische Maßnahmen nach § 17 Abs. 3 DSG MV zu treffen sind und dafür zu sorgen ist, daß die Bögen nach der Auswertung unverzüglich datenschutzgerecht vernichtet werden.

Der Bürgermeister teilte mit, daß er meine Empfehlungen umsetzen wird.

3.17.3 Geschichtsträchtiges Sinfonieorchester

Ein Bürger beabsichtigte, Personalunterlagen ehemaliger Mitglieder eines staatlichen Sinfonieorchesters einzusehen. Er benötigte diese Daten, um die Geschichte des Orchesters auf wissenschaftlicher Basis aufzuarbeiten. Die Ergebnisse seiner Forschung wollte er nicht personenbezogen veröffentlichen.

Sollen personenbezogene Daten ohne Einwilligung des Betroffenen zu Forschungszwecken genutzt werden, so muß die zuständige oberste Aufsichtsbehörde dies nach dem Landesdatenschutzgesetz Mecklenburg-Vorpommern genehmigen. Diese prüft, ob das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen erheblich überwiegt und ob der Zweck der Forschung nicht auf andere Weise erreicht werden kann. Personalakten und Personalaktendaten der Landesbeamten sind durch das Landesbeamtengesetz (LBG M-V) besonders geschützt (§§ 100 - 107 LBG M-V). Die vom Innenminister zu diesen Regelungen erlassene Verwaltungsvorschrift „Richtlinien über die Führung von Personalakten“ ist sinngemäß auch auf die Personalaktenführung der Arbeitnehmer im Geltungsbereich der obersten Landesbehörden anzuwenden.

Den Gemeinden, Städten, Landkreisen und Ämtern sowie den juristischen Personen des öffentlichen Rechts hat der Innenminister empfohlen, ebenfalls entsprechend der Verwaltungsvorschrift zu verfahren (siehe Punkt 3.14.7). Die Richtlinien sind daher auch für den Umgang mit den Personalakten der Orchestermitglieder maßgeblich. Danach haben Dritte ohne Einwilligung des Betroffenen grundsätzlich kein Auskunftsrecht. Ausnahmsweise erhält ein Dritter jedoch dann Auskunft aus der Akte, wenn die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen des Dritten dies zwingend erfordern. Diese Voraussetzungen lagen in diesem Fall nicht vor.

Ich habe dem Bürger daher empfohlen, die Einwilligung der Orchestermitglieder oder ihrer Erben einzuholen. Daten von Orchestermitgliedern, deren Todesdatum mehr als 30 Jahre zurückliegt, können auch ohne Einwilligung der Erben genutzt werden.

3.17.4 „Wie erleben Patienten die Elektrokrampftherapie“

Zwei Ärzte einer psychiatrischen Klinik wollten der Frage nachgehen, wie die Elektrokrampftherapie von den Patienten erlebt wurde. Zu diesem Zweck hatten sie sich mit einem Schreiben und einem beigefügten Fragebogen an ehemalige Patienten ihrer Klinik gewandt und um die Beantwortung von Fragen gebeten. In dem Anschreiben wurde nicht ausdrücklich darauf hingewiesen, daß die Teilnahme an der Befragung freiwillig ist. Den Betroffenen wurde aber zugesichert, daß die Auswertung anonym erfolgt. Am Ende des Fragebogens sollten allerdings Name, Vorname und Geburtsdatum angegeben werden, um - wie im Schreiben erläutert - die Antworten im Zusammenhang mit der Krankengeschichte auswerten zu können. Außerdem sollten die Teilnehmer ihre Telefonnummer angeben, um eventuelle Rückfragen zu ermöglichen.

Für die Beurteilung des Vorhabens war entscheidend, auf welcher Rechtsgrundlage die ehemaligen Patienten ausgewählt und persönlich angeschrieben worden sind. Das Gesetz über Hilfen und Schutzmaßnahmen für psychisch Kranke (PsychKG) enthält keine Regelungen zur Nutzung von Patientendaten für Forschungszwecke, es verweist jedoch auf die entsprechenden Normen im Landeskrankenhausgesetz (LKHG M-V) sowie auf das Landesdatenschutzgesetz.

Nach dem LKHG M-V dürfen Daten eines Patienten zu Forschungszwecken verarbeitet und genutzt werden, wenn er eingewilligt hat (§ 20 Abs. 1 LKHG M-V). Ohne Einwilligung ist dies unter anderem zulässig, wenn zum Beispiel seine schutzwürdigen Belange wegen der Art der Datennutzung nicht beeinträchtigt werden oder wenn die für das Krankenhaus zuständige oberste Aufsichtsbehörde feststellt, daß das öffentliche Interesse an dem Vorhaben die schutzwürdigen Belange des Patienten erheblich überwiegt (§ 20 Abs. 2 LKHG M-V). Darüber hinaus darf ein Arzt, soweit er die gesetzlich normierten Bedingungen beachtet, unter anderem für eigene Forschungszwecke Dateien mit Patientendaten anlegen. Allerdings muß er die Daten anonymisieren, sobald es der Forschungs- bzw. Verarbeitungszweck erlaubt (§ 20 Abs. 6 LKHG M-V).

Auf meine Frage, wie die Adressen der mit dieser Therapie behandelten Patienten gewonnen wurden, teilte mir der Chefarzt mit, daß der behandelnde Arzt sie aus den Krankenunterlagen entnommen hat. Er sei dabei davon ausgegangen, daß wegen der Art der Datennutzung keine schutzwürdigen Interessen der Patienten beeinträchtig wurden.

Der Verein „Angehörige und Freunde psychisch Kranker e. V.“, der sich in dieser Angelegenheit auch an mich gewandt hatte, sah dies jedoch anders: Viele der angeschriebenen Patienten seien aufgrund ihres Zustandes gar nicht in der Lage, die Tragweite und Bedeutung ihrer Antworten einzuschätzen. Somit könnten durch dieses Verfahren durchaus schutzwürdige Interessen der Betroffenen beeinträchtigt werden. Diese Argumentation erschien mir vor allem deshalb nachvollziehbar, da auch Patienten befragt wurden, ohne daß nähere Angaben über ihren gegenwärtigen Gesundheitszustand vorlagen.

Neben dieser Nutzung der Adressen von ehemaligen Patienten habe ich an dem Verfahren insbesondere folgendes kritisiert:

- Den Betroffenen wurde nicht eindeutig erklärt, daß die Teilnahme an der Befragung freiwillig ist.
- Es handelt sich allein schon wegen der Angabe des Namens um keine anonyme Befragung. Deshalb hätte lediglich darauf hingewiesen werden können, daß die Angaben vertraulich behandelt werden.

- Für die beabsichtigte Zuordnung der Antworten eines Teilnehmers zu seiner Krankengeschichte hätte eine normgerechte Einwilligung vorliegen müssen.

Die Klinik hat mir schließlich mitgeteilt, daß sie von der Fragebogenmethode Abstand nimmt und statt dessen künftig persönliche Interviews durchführt. Sofern diese Interviews im Zusammenhang mit der medizinischen Behandlung erfolgen und die Betroffenen auf den Zweck der Fragestellung und die freiwillige Beantwortung deutlich und umfassend hingewiesen werden, ist dagegen aus datenschutzrechtlicher Sicht nichts einzuwenden.

3.17.5 „Lebenssituation von behinderten Frauen“

Das Bundesministerium für Familie, Senioren, Frauen und Jugend hatte ein bundesweites Forschungsvorhaben zur Lebenssituation von behinderten Frauen ausgeschrieben. Die Durchführung war einer Forschungseinrichtung der Evangelischen Fachhochschule für Sozialwesen in Freiburg übertragen worden und sollte in Form einer schriftlich-postalischen Befragung von etwa 5.000 Frauen im Alter zwischen 16 und 60 Jahren erfolgen. Zu diesem Zweck hatte sich das Forschungsinstitut an alle Landesversorgungsämter mit der Bitte gewandt, ihm Adressenstichproben von behinderten Frauen zur Verfügung zu stellen. Das Bundesministerium für Familie, Senioren, Frauen und Jugend teilte den Versorgungsämtern zusätzlich mit, daß Einwilligungen in die Weitergabe der Adressen der Betroffenen aus finanziellen und personellen Gründen nicht eingeholt werden könnten und die Versorgungsämter daher bei den obersten Landesbehörden eine Genehmigung zur Übermittlung erwirken sollten, wie es § 75 Abs. 2 Sozialgesetzbuch Zehntes Buch (SGB X) vorschreibe. Einige Landesversorgungsämter hielten dies für datenschutzrechtlich fragwürdig und wandten sich daraufhin an die Landesbeauftragten für den Datenschutz. Auf meine Anfrage hin wurde mir das Konzept des Forschungsvorhabens vom Landesversorgungsamt Mecklenburg-Vorpommern zugesandt.

Gegen die geplante Übermittlung von Adressen an die Forschungseinrichtung hatte ich erhebliche Bedenken. Zum einen bestanden Zweifel daran, daß es tatsächlich unzumutbar sein sollte, die Einwilligungen der betroffenen Frauen vorab einzuholen. Zum anderen lag auf der Hand, daß der Forschungszweck auch ohne Offenbarung der Daten an die Forschungseinrichtung erreicht werden konnte. Hier bot sich das „Adressmittlungsverfahren“ an. In diesem Fall stellt

die Forschungseinrichtung dem jeweiligen Versorgungsamt den Fragebogen, das Anschreiben sowie frankierte Umschläge zur Verfügung, und das Versorgungsamt übernimmt dann die Adressenauswahl, das Adressieren sowie das Versenden der Briefe. Auf diese Weise gehen zunächst nur die Versorgungsämter mit den Namen und Adressen um, bei denen diese ohnehin gespeichert sind. Die angeschriebenen Frauen können entscheiden, ob sie an der Befragung teilnehmen wollen und in diesem Fall den ausgefüllten Fragebogen selbst direkt an die Forschungseinrichtung zurücksenden.

Auf meine Empfehlung hin wurde die Befragung letzlich im Adressmittlungsverfahren durchgeführt. Auch in einigen anderen Bundesländern ist auf Anregung der Landesbeauftragten für den Datenschutz auf diese Weise verfahren worden.

3.17.6 „Kinderwunsch- und Wachstumsstudie“

Eine Universitätsklinik in Mecklenburg-Vorpommern plant in Zusammenarbeit mit zwei weiteren Forschungseinrichtungen eine bundesweite Studie über die Entwicklung der Familie und der sozialen und medizinischen Situation von Müttern. Zu diesem Zweck ist eine Umfrage bei Frauen auf den Entbindungsstationen verschiedener Krankenhäuser vorgesehen. Die erfragten Daten sollen in der Universitätsklinik ausgewertet und statistisch aufbereitet werden und die Ergebnisse als Grundlage für sozial- und familienpolitische Entscheidungen sowie für Verbesserungen der medizinischen Versorgung von Schwangeren und Müttern dienen. Den dazu konzipierten umfangreichen Fragebogen sowie ein Informationsblatt für die Patientinnen, in dem die anonyme Auswertung zugesichert wird, hat mir die Universitätsklinik im Entwurf vorab zur Prüfung zugesandt.

Die Patientinnen werden um ausführliche Auskünfte zu ihrer persönlichen Lebenssituation und zu ihrer medizinischen Vorgeschichte, zum Beispiel zu bereits erlittenen Fehlgeburten, gebeten. Die Namen und Adressen der befragten Frauen werden jedoch nicht erhoben. Zum Teil sind auch Freitextangaben zur Beantwortung der Fragen nötig. In dem Entwurf des Informationsblattes wurde zwar darauf hingewiesen, daß die Befragung auf freiwilliger Basis stattfindet, jedoch nicht, welche der angegebenen Stellen das Forschungsprojekt durchführt und die Auswertung der Daten vornimmt.

Auch in diesem Fall galt es zunächst zu prüfen, ob die Auswertung der Angaben tatsächlich „völlig anonym“ erfolgen kann, wie es die Klinik den Patientinnen versichert.

„Anonymisieren“ bedeutet das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbaren Person zugeordnet werden können (§ 3 Abs. 7 Nr. 5 DSG MV). Anonyme Daten unterliegen in Ermangelung des Personenbezugs nicht den datenschutzrechtlichen Regelungen. Ist jedoch zumindest theoretisch der Rückschluß auf eine bestimmte Person noch möglich, handelt es sich nicht um anonyme, sondern um personenbeziehbare Daten. Dabei ist es unerheblich, auf welche Weise der Personenbezug wieder hergestellt werden kann. Der Umgang mit diesen Daten ist nur nach Maßgabe der gültigen Datenschutzbestimmungen zulässig (siehe Punkt 2.1).

Im vorliegenden Fall ergab die datenschutzrechtliche Prüfung, daß - obwohl die Universitätsklinik allein anhand der Angaben der Frauen keinen Personenbezug herstellen kann - es sich bei den erbetenen Angaben nicht um anonyme Daten handelt. Rückschlüsse auf die befragten Patientinnen waren mit dem Zusatzwissen des jeweiligen Krankenhauses, wie den medizinischen Daten aus der Patientenakte oder einem Handschriftenvergleich, auch bei der Universitätsklinik noch möglich.

Ich habe dem Projektleiter der Studie daher die folgenden Empfehlungen gegeben:

- Die Patientinnen sollten im Informationsblatt ausführlich über Zweck und Verfahren der Befragung aufgeklärt werden. Insbesondere war die datenverarbeitende und -auswertende Stelle, hier die Universitätsklinik, mit Anschrift und Telefonnummer anzugeben, und es war darauf hinzuweisen, daß die Erhebungsbögen ausschließlich dieser Stelle zur Verfügung gestellt und auch nur von dieser zu wissenschaftlichen Zwecken ausgewertet werden.

- Die Universitätsklinik sollte sich darüber hinaus verpflichten, die Erhebungsbögen nach der Erfassung der Daten in einer Datei datenschutzgerecht zu vernichten. Weiter sollte sie sich verpflichten, die Datensätze nicht an Dritte zu übermitteln und diese umgehend nach der Auswertung zu löschen. Auch hierüber waren die Patientinnen zu informieren.

Meinen Empfehlungen wurde vollständig gefolgt.

Da geplant ist, die Befragung auch in Krankenhäusern anderer Bundesländer durchzuführen, habe ich meine Kollegen über das Projekt informiert.

3.18 Technische Maßnahmen

3.18.1 Was Mobiltelefonnutzer wissen sollten

Der Bundesrat hat im Rahmen der Beratungen zum Entwurf eines Begleitgesetzes zum Telekommunikationsgesetz (vgl. Bundesrats-Drucksache 369/97 vom 4. Juli 1997) erweiterte und völlig neuartige Eingriffsbefugnisse im Bereich der Telekommunikation gefordert (siehe auch Punkt 3.10.3). Die Nachrichtendienste und Strafverfolgungsbehörden sollten befugt werden, Abhörgeräte einzusetzen, mit denen sie die netzinternen Rufnummern von Mobiltelefonen ermitteln sowie Gespräche mithören und aufzeichnen können.

Um das Vorhaben datenschutzrechtlich bewerten zu können, habe ich mich über Aufbau, Wirkungsweise und Funktionen dieser als IMSI-Catcher (International Mobile Subscriber Identity - netzinterne Teilnehmerkennung) bezeichneten Abhörgeräte informiert. Es war zu prüfen, welche Gefahren insbesondere für die Wahrung des grundgesetzlich geschützten Fernmeldegeheimnisses vom Betrieb solcher Abhörgeräte ausgehen.

Aus technischer Sicht wird der Einsatz eines IMSI-Catchers überhaupt erst dadurch möglich, weil der für digitale Mobilfunknetze maßgebliche GSM-Standard (Global System for Mobile Communication) eine Sicherheitslücke aufweist.

Bei den hier betrachteten Mobilfunknetzen ist das funktechnisch abzudeckende Gebiet in Funkzellen unterteilt. Jede dieser Zellen wird von einer stationären Funkstation, der Basisstation, verwaltet. Soll mit einem Mobilltelefon ein Gespräch geführt werden, muß es sich gegenüber dem Netz authentifizieren. Eine Authentifikation des Netzes gegenüber dem einzelnen Gerät wurde jedoch bei der Definition des GSM-Standards nicht vorgesehen. Das ist die Sicherheitslücke. Denn dadurch kann sich der Nutzer eines Mobiltelefons prinzipiell nicht sicher

sein, daß seine Kommunikation tatsächlich ausschließlich über eine legitime Basisstation des von ihm gewählten Netzbetreibers abgewickelt wird.

Diese Unzulänglichkeit macht es dem Mobiltelefon unmöglich, zwischen dem IMSI-Catcher und einer Basisstation zu unterscheiden. Der IMSI-Catcher baut eine „illegale“ Funkzelle auf, in der er mit einer etwas stärkeren Leistung als die Basisstationen arbeitet. Deshalb melden sich alle Geräte im Bereich dieser Funkzelle bei ihm und nicht bei der eigentlichen Basisstation an, ohne daß der Nutzer selbst es bemerkt.

Der IMSI-Catcher kann dann in zwei verschiedenen Betriebsarten eingesetzt werden:

Im sogenannten Fangmodus ist er in der Lage, von allen in seiner Reichweite befindlichen Mobiltelefonen neben der IMSI auch die IMEI (International Mobile Station Equipment Identity - Endgerätekennung) abzurufen. Mit diesen Daten sind dann weitere Ermittlungen zu allen Personen möglich, die ihr Gerät im Einzugsbereich des IMSI-Catchers benutzen. Technisch bedingt können während des Fangens mit keinem dieser Telefone Gespräche geführt werden. Selbst Notrufe zur Polizei, zur Feuerwehr oder zum ärztlichen Notdienst sind von keinem der beim IMSI-Catcher eingebuchten Mobiltelefone möglich.

In der zweiten Betriebsart, dem Abhörmodus, können alle Gespräche eines ausgewählten Mobiltelefons unverschlüsselt abgehört und aufgezeichnet werden. Das mag zunächst verwunderlich erscheinen, da die Netzbetreiber und Gerätehersteller lange Zeit gerade mit dem Argument der Abhörsicherheit durch Verschlüsselung für diese neue Kommunikationstechnik geworben haben. In diesem Zusammenhang wurde jedoch meist nicht erwähnt, daß der Netzbetreiber durch einen GSM-Befehl die Verschlüsselung ausschalten kann. Eine Anzeige für den Nutzer, ob verschlüsselt oder unverschlüsselt übertragen wird, ist nicht vorgesehen. Der IMSI-Catcher, der entsprechend der GSM-Konvention arbeitet, kann diesen Befehl nutzen. Wenn also Gespräche abgehört werden sollen, wird beim Verbindungsaufbau die Verschlüsselung ausgeschaltet, so daß die Gesprächsinhalte zwar nach wie vor in digitaler Form, jetzt aber unverschlüsselt und mit entsprechender Software abhörbar, vorliegen und aufgezeichnet werden können. Solange der IMSI-Catcher im Abhörmodus arbeitet, kann mit keinem Gerät im Bereich der illegalen Funkzelle kommuniziert werden. Lediglich abgehende Gespräche des abgehörten Mobiltelefons sind möglich, weil diese vom IMSI-Catcher weitergeleitet werden.

In meiner Stellungnahme zum Entwurf des TKG-Begleitgesetzes habe ich den Einsatz des IMSI-Catchers insbesondere deshalb abgelehnt, weil bei der Feststellung der Rufnummer und beim Abhören eines Betroffenen mit einer bisher noch nicht dagewesenen Intensität das Recht auf unbeobachtete Kommunikation unbeteiligter Dritter beeinträchtigt wird. Wegen Bedenken der Bundesregierung, der Datenschützer und der Netzbetreiber ist in das TKG-Begleitgesetz keine Vorschrift aufgenommen worden, welche die Verwendung eines IMSI-Catchers erlaubt.

Obwohl also der IMSI-Catcher von Nachrichtendiensten und Strafverfolgungsbehörden zunächst nicht eingesetzt werden darf, bleiben die beschriebenen Risiken prinzipiell bestehen. Einerseits ist nicht auszuschließen, daß dieses Gerät beispielsweise für den Export weiter produziert wird. Andererseits dauert es erfahrungsgemäß nicht lange, bis Bauanleitungen für einzelne Komponenten oder für das gesamte Gerät veröffentlicht werden. Vor diesem Hintergrund wäre es leichtfertig anzunehmen, daß es nicht zum Mißbrauch dieser Technik kommt.

Deshalb sind vor allem Netzbetreiber, Entwickler und Hersteller der Mobilfunktechnik aufgefordert, im Rahmen des geltenden Rechts durch geeignete Maßnahmen dafür zu sorgen, daß ihre Kunden vertraulich miteinander kommunizieren können. Darüber hinaus sollten Netzbetreiber und Gerätehersteller ihre Kunden offen und umfassend auch über Schwachstellen und Risiken für die vertrauliche Kommunikation in Mobilfunknetzen aufklären. Einerseits scheint mir eine solche Aufklärung angesichts des Informationsstandes der Bevölkerung längst überfällig, und andererseits gibt es keinerlei Grund zur Panik, denn die Risiken sind nicht größer als beispielsweise beim drahtgebundenen Telefonieren.

Ein Mobiltelefon kann aber auch auf eine ganz andere Art und Weise, nämlich als Abhörgerät, verwendet werden. Voraussetzung ist oft nur die geschickte Auswahl von Leistungsmerkmalen und der Einsatz handelsüblicher Zusatzgeräte. Auch hierüber sollten die Nutzer informiert sein, damit sie sich selbst durch eigene Maßnahmen vor einer Verletzung ihrer Persönlichkeitssphäre schützen können.

Im einfachsten Fall wird beispielsweise ein eingeschaltetes Gerät, mit dem man zuvor eine Gesprächsverbindung aufgebaut hat, im abzuhörenden Raum liegengelassen. Alle im Raum geführten Gespräche werden, sofern das Mikrofon des Mobiltelefons sie erfaßt, zu einem Zielgerät übertragen. Natürlich hat ein solches „Abhörgerät“ wegen der begrenzten Akkukapazität nur eine kurze Betriebsdauer, und der Abhörvorgang kann durch einen Blick auf das Display erkannt werden.

Sind bei einem „vergessenen“ Gerät die Leistungsmerkmale „Automatische Anrufannahme“ und „Lautlosbetrieb“ aktiviert, kann von außen sogar zu einem beliebigen Zeitpunkt abgehört werden. Erst der Anruf versetzt das Mobiltelefon dann in den Gesprächszustand. Allerdings ist das Leistungsmerkmal „Automatische Anrufannahme“ meist nur in Kombination mit einer Freisprecheinrichtung nutzbar. Darüber hinaus schließen sich bei vielen Geräten die Leistungsmerkmale „Automatische Anrufannahme“ und „Lautlosbetrieb“ gegenseitig aus. Es gibt jedoch für viele Gerätetypen Freisprecheinrichtungen als sogenannte Sprechgarnitur (Mikrofon und Ohrhörer), die in diesem Zusammenhang verwendet werden können. Durch eine geschickte Auswahl von Ruftonoptionen kann dann auch auf das Merkmal „Lautlosbetrieb“ verzichtet werden. Somit ist ein Mobiltelefon allein durch Nutzung von Standardmerkmalen und frei verfügbarer Technik schon als recht leistungsfähiges Abhörgerät zu betreiben.

Denkbar ist weiterhin, daß durch Hardwaremanipulationen die Existenz einer Freisprecheinrichtung simuliert wird (beispielsweise entsprechende interne Beschaltung der Anschlußbuchse). Wenn durch einen weiteren Eingriff in das Gerät zusätzlich das Display und der Ruftongenerator deaktiviert und dann Leistungsmerkmale wie oben beschrieben eingerichtet werden, ist am Gerät nicht mehr erkennbar, ob und wann mit ihm abgehört wird.

Wer über entsprechende Spezialkenntnisse und die dafür erforderlichen Hard- und Softwarekomponenten verfügt, kann sogar die im Mobiltelefon gespeicherte Systemsoftware so verändern, daß ohne Aktivierung von Leistungsmerkmalen das Abhören zu einem beliebigen Zeitpunkt durch Anruf des Gerätes möglich ist.

Es wird deutlich, daß nur ein ausgeschaltetes Mobiltelefon einen sicheren Schutz vor Mißbrauch garantiert. Natürlich ist das nicht in jedem Fall zu empfehlen, denn gerade die ständige Erreichbarkeit bewirkt ja eine neue Kommunikationsqualität. Jeder Nutzer sollte sich der beschriebenen Gefahren jedoch bewußt sein, um für sich selbst zwischen der vermeintlichen Er-

forderlichkeit der Anwendung dieser neuen Technik und den damit verbundenen Risiken abwägen zu können. Netzbetreiber und Gerätehersteller sollten dafür gewonnen werden, Mobilfunkgeräte so nutzerfreundlich zu entwickeln und den Netzbetrieb so auszugestalten, daß Mißbrauchsmöglichkeiten von vornherein weitestgehend ausgeschlossen sind.

3.18.2 Elektronische Post

Im Zweiten Tätigkeitsbericht hatte ich unter Punkt 2.18.2 bereits über die Bestrebungen öffentlicher Stellen des Landes berichtet, elektronische Mitteilungssysteme für die Kommunikation untereinander und für den schnellen Dokumentenaustausch einzusetzen. Um die entsprechenden organisatorischen Voraussetzungen hierfür zunächst in den obersten Landesbehörden zu schaffen, hat der Ausschuß für Organisationsfragen unter Federführung des Innenministeriums Rahmenbedingungen zum Einsatz eines elektronischen Postsystems MHS/X.400 formuliert und bereits in der Entwurfsphase um Beratung gebeten.

Der Entwurf, in dem vor allem die Rahmenbedingungen für die Einrichtung und den Betrieb einer zentralen X.400-Kopfstelle festgelegt werden sollen, enthielt schon detaillierte Hinweise zur datenschutzgerechten Nutzung. Die Empfehlungen der Datenschutzbeauftragten des Bundes und der Länder zu elektronischen Mitteilungssystemen (Entschließung der 49. Konferenz, siehe Zweiter Tätigkeitsbericht, 15. Anlage) waren teilweise berücksichtigt worden. Daher waren nur noch wenige Änderungen erforderlich.

Beispielsweise habe ich empfohlen, bei der Planung der X.400-Kopfstelle die Konzepte für die Weiterentwicklung des Landesdatennetzes zu berücksichtigen, um eine integrationsfähige und zukunftsorientierte landeseinheitliche Lösung zu finden. Darüber hinaus sollten bereits vorliegende Realisierungsvorschläge für ein ressortübergreifendes Intranet unter der Voraussetzung einbezogen werden, daß bisher vollständig fehlende IT-Sicherheitsmaßnahmen dort aufgenommen werden.

Die Administration der Kopfstelle soll durch Mitarbeiter des Innenministeriums erfolgen. Zu deren Aufgaben gehört es unter anderem, nicht elektronisch zustellbare Post auszudrucken und

weiterzuleiten. Hier sind organisatorische Regelungen erforderlich, die eine unberechtigte Kenntnisnahme vertraulicher Dokumente verhindern.

Weiterhin ist zu klären, ob Mitteilungen als elektronische Post versandt werden dürfen, die beispielsweise an den Personalrat oder das Personalreferat adressiert oder für einen Empfänger als „persönlich“ gekennzeichnet sind. Im konventionellen Postverkehr erhalten solche Empfänger diese Post ungeöffnet. Beim elektronischen Versand kann eine solche „ungeöffnete Zustellung“ nicht immer sichergestellt werden (z. B. bei Eingang in der lokalen Poststelle oder bei Störungen, die den Ausdruck und konventionelle Weiterleitung erfordern).

Elektronische Mitteilungssysteme ermöglichen es, an eine Nachricht beispielsweise Textdokumente „anzuhängen“. Im Entwurf wird vorgeschlagen, als Standardformat Word für Windows 2.0 zu verwenden. Das hat jedoch den Nachteil, daß neben dem Text eine Vielzahl weiterer Informationen, die nicht für den Empfänger vorgesehen sind (z. B. Text früherer Versionen, Informationen zum Autor, statistische Informationen), in der Datei gespeichert und damit unbewußt übermittelt werden. Darüber hinaus trägt die Weitergabe solcher Textdateien zur schnellen Ausbreitung von Makroviren bei (siehe auch Punkt 3.18.4). Vor diesem Hintergrund habe ich empfohlen, ein anderes Format, beispielsweise RTF (Rich Text Format), als Standard zu definieren.

Maßnahmen zur Gewährleistung der Authentizität von Benutzern, Nachrichten und Systemmeldungen, zur Verhinderung von unbefugten, unerkannten Veränderungen bei der Speicherung und Weiterleitung von Daten und als Hilfsmittel zur Beweissicherung für die stattgefundene Kommunikation waren zunächst im Entwurf nicht explizit gefordert worden. Auf meine Empfehlung hin wurde jedoch die Forderung aufgenommen, bei der Nutzung des elektronischen Postsystems Verfahren der digitalen Signatur einzusetzen. Weiterhin wird ausdrücklich darauf hingewiesen, daß zum Schutz personenbezogener Daten zusätzliche geeignete Sicherheitsmaßnahmen, wie beispielsweise Verschlüsselungerforderlich sind.

Im Rahmen des alljährlich stattfindenden IT-Forums Mecklenburg-Vorpommern in der Fachhochschule für öffentliche Verwaltung und Rechtspflege in Güstrow wurde unter dem Motto „Schlanke Verwaltung nur mit Informationstechnik“ ebenfalls über elektronische Postsysteme und mögliche Rationalisierungseffekte diskutiert. Mehrfach wurden diese neuen Kommunikati-

onsmöglichkeiten mit dem konventionellen Informationsaustausch per Telefon verglichen. Die Erforderlichkeit von zusätzlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten wurde deshalb in Frage gestellt. Schließlich ließe sich ja auch nicht verhindern, so die Argumentation, daß auch am Telefon unzulässigerweise vertrauliche Informationen ausgetauscht werden. Dabei wurde jedoch nicht bedacht, daß die Kommunikation auf elektronischem Wege gegenüber dem Telefongespräch schon allein deshalb eine neue Qualität darstellt, weil problemlos in kürzester Zeit große Datenmengen sehr bequem und mit geringer Fehlerrate übermittelt werden können.

Einige Anwender aus dem kommunalen Bereich warben für mehr „Risikobereitschaft“ und stellten elektronische Postsysteme vor, die ohne hinreichende organisatorische und technische Vorgaben entwickelt und in Betrieb genommen worden sind. Dabei wurde bewußt in Kauf genommen, daß infolge fehlender Sicherheitsmaßnahmen „... auch mal ein Dokument verloren geht oder den falschen Adressaten erreicht und nicht überprüfbar ist, ob es bei der Übertragung verändert wurde...“.

Auch wenn man von vornherein davon ausgehen muß, daß grundsätzlich eine hundertprozentige Sicherheit nicht erreicht werden kann, so halte ich eine derart plan- und konzeptionslose Einführung neuer Technologien für nicht vereinbar mit den Grundsätzen ordnungsgemäßer Datenverarbeitung. Darüber hinaus kann der datenschutzgerechte Umgang mit personenbezogenen Daten nicht gewährleistet werden, wenn es an erforderlichen Sicherheitsmaßnahmen mangelt.

Es bleibt abzuwarten, ob meine Empfehlungen im Datenschutz- und IT-Sicherheitskonzept, das vor der Realisierung der X.400-Kopfstelle vorliegen muß, berücksichtigt werden. Eine ressortübergreifende Arbeitsgruppe wird sich im Zusammenhang mit Fragen der Netzwerk- und Intranetkonzeption des Landes auch mit den erforderlichen Sicherheitsmaßnahmen des elektronischen Postsystems befassen.

3.18.3 Datenschutz bei Telefax

Der Datenschutzbeauftragte eines Krankenhauses hatte mir mitgeteilt, daß die Landesversicherungsanstalt (LVA) medizinische Befunde ausdrücklich als Fax anfordert. Seine Nachfrage bei der LVA ergab, daß sie auch gegenüber allen anderen Krankenhäusern des Landes auf dieser Form der Datenübermittlung besteht. Der Petent befürchtete zurecht eine zufällige Offenbarung von Patientendaten und hat mich deshalb gebeten, dieses Verfahren zu prüfen.

Aus gegebenem Anlaß hatte ich in der Vergangenheit schon mehrfach Hinweise zur Übermittlung personenbezogener Daten per Telefax gegeben (siehe beispielsweise Zweiter Tätigkeitsbericht, Punkt 2.12.10). Meine Anfrage bei der LVA ergab, daß diese Hinweise nicht ausreichend berücksichtigt worden waren, so daß die Vertraulichkeit der per Fax übermittelten Patientendaten nicht in angemessener Weise sichergestellt war. Die LVA ist meiner Empfehlung nachgekommen, auf die Anforderung von Patientendaten per Fax zu verzichten, nachdem sie ausführlich über die Risiken bei der Nutzung von Telefaxgeräten informiert wurde. Die Befunde werden nun solange mit der Briefpost übermittelt, bis zusätzliche Sicherungsmaßnahmen die Übermittlung per Fax ermöglichen. So prüft die LVA beispielsweise, ob Verschlüsselungsverfahren eingesetzt werden können.

Die Auswahl geeigneter und angemessener Sicherungsmaßnahmen ist auch in diesem Bereich vor allem vom Stand der Technik abhängig. Moderne Telefaxlösungen, die in Bürokommunikationssysteme integriert sind, erfordern deshalb andere Maßnahmen als konventionelle Telefaxgeräte. Bei integrierten Verfahren ist insbesondere darauf zu achten, daß

- das verwendete Rechnersystem sorgfältig konfiguriert und gesichert ist und Unbefugte keinen Zugang oder Zugriff zu den benutzten Rechnern und Netzwerken haben,

- die Angabe der Empfänger korrekt ist; durch die Nutzung der von der Faxsoftware bereitgestellten Hilfsmittel wie Faxanschlußlisten (Empfänger und Verteiler sind dort mit aussagekräftigen Bezeichnungen versehen) wird dieses erleichtert,

- die in der Faxsoftware gespeicherten technischen Parameter, Anschlußlisten und Protokolle regelmäßig und besonders sorgfältig überprüft werden,

- ausreichende Konfigurationsmöglichkeiten vorhanden sind, um die dringend notwendige Anpassung an die datenschutzrechlichen Erfordernisse des Nutzers zu gewährleisten.

Da bei integrierten Faxlösungen bereits unkomplizierte und kostengünstige kryptographische Verfahren zur Verfügung stehen, sollte geprüft werden, ob diese eingesetzt werden können. Beide Seiten müßten darauf achten, daß die Produkte kompatibl sind.

Aber auch bei konventionellen Faxgeräten bleibt die technische Entwicklung nicht stehen. Von besonderer Bedeutung ist aus datenschutzrechtlicher Sicht die Möglichkeit der Fernwartung, bei der Hersteller unter bestimmten Bedingungen auf die im Faxgerät gespeicherten Daten zugreifen können. Der interne Seitenspeicher kann beispielsweise gelesen oder Rufnummern- und Parameterspeicher beschrieben werden. Deshalb ist insbesondere darauf zu achten,

- daß die am Telefaxgerät eingestellten technischen Parameter und Speicherinhalte regelmäßig überprüft werden und

- daß die Fernwartungsfunktion grundsätzlich durch den Nutzer deaktiviert und nur für notwendige Wartungsarbeiten freigegeben wird und nach Abschluß der Wartungsarbeiten die eingestellten Parameter und Speicherinhalte kontrolliert werden.

Diese neuen technischen Entwicklungen haben die Datenschutzbeauftragten des Bundes und der Länder veranlaßt, in einer gemeinsamen Presseerklärung auf die Gefahren beim Umgang mit Telefaxgeräten und Faxsoftware hinzuweisen (siehe 19. Anlage).

3.18.4 Makroviren

Standardsoftware wie Textverarbeitung und Tabellenkalkulation, aber auch komplette Vorgangsbearbeitungssysteme werden bereits an vielen Arbeitsplätzen öffentlicher Stellen unseres Landes genutzt. Zum Funktionsumfang vieler Standardsoftwareprodukte gehört inzwischen eine eigene Programmiersprache (Makrosprache). Die damit erstellten Makroprogramme (Makros) automatisieren beispielsweise typische Bedienungsschritte oder knüpfen Verbindungen zu anderen Programmen.

Mit solchen Programmiersprachen lassen sich jedoch auch Makros implementieren, die die Integrität von Datenbeständen, von Anwendungsprogrammen oder von Betriebssystemen verletzen. Als Folge können dann sogar die Verfügbarkeit und die Vertraulichkeit des gesamten Systems gefährdet sein. Bei solchen Makros handelt es sich in vielen Fällen um eine neue Art von Computerviren, also Programmteilen, die sich an andere Trägerprogramme binden können. Solche mit Hilfe der Makrosprachen geschriebenen Computerviren (Makroviren) sind inzwischen recht weit verbreitet.

Zur schnellen Ausbreitung dieser Viren trägt vor allem der Austausch von Dokumenten, die Makros enthalten können, bei. Daneben begünstigen folgende Eigenschaften von Makrosprachen und Standardsoftware die Implementation von Viren und anderen schädlichen Programmen:

- Die meisten Operationen, die ein Benutzer in der Standardsoftware auslöst, stehen auch in der Makrosprache zur Verfügung. Dazu gehören auch Verwaltungs- und Konfigurationsfunktionen sowie Zugriffsmöglichkeiten auf Programme und andere Dateien.

- Makros kann man so schreiben, daß sie beim Öffnen von Dateien oder anderen Ereignissen automatisch gestartet werden. Diese Automatik ist mitunter schwer zu sperren. Schon die Frage, ob eine Datei überhaupt Makros enthält, ist nicht einfach zu beantworten. Beispielsweise wird die genaue Behandlung einer Datei nicht unbedingt durch die Endung des Dateinamens bestimmt.

- Das Betriebssystem kann nicht unterscheiden, ob die Standardsoftware gerade von einem Benutzer oder von einem Makro gesteuert wird. So können Benutzer und Makros zum Beispiel gleichermaßen Textteile oder Dateien löschen oder kopieren. Wenn das Betriebssystem solche Operationen prüft oder protokolliert, werden diese in beiden Fällen dem Benutzer zugerechnet.

- In der Standardsoftware ist oft kein Zugriffsschutzmechanismus enthalten, mit dem die Wirkungen von Makroprogrammen auf einen bestimmten Bereich begrenzt werden könnten.

- Makroprogramme sind nicht an ein bestimmtes Betriebssystem, sondern an eine Anwendung oder eine Familie von Anwendungen mit derselben Makrosprache gebunden. Daher ist eine automatische Verbreitung oder manuelle Weitergabe von schädlichen Makroprogrammen auch dann möglich, wenn Benutzer verschiedener Betriebssysteme Dokumente austauschen.

Daher empfehle ich, folgende Gesichtspunkte bei Planung und Einsatz von Standardsoftware zu beachten:

- Sowohl zum Dokumentenaustausch, zum Beispiel per Datenträger oder elektronischer Post, als auch zur Archivierung sollten Dateiformate benutzt werden, die keine Makros enthalten können. Damit wird eine Weitergabe von Makroviren ausgeschlossen.

- Programme, die am Arbeitsplatz zur Verfügung stehen sollen, müssen formal freigegeben und ordnungsgemäß installiert werden. Damit wird die Verbreitung von Computerviren wirkungsvoll eingeschränkt. Angesichts der beschriebenen Gefahren, die von ungeprüften Makroprogrammen ausgehen können, sollten Freigabe- und Installationsverfahren auf Makroprogramme ausgedehnt werden.

- Mit Virenscannern sollte regelmäßig auch nach Makroviren gesucht werden. Dies ist besonders bei eingehenden Dokumenten unabhängig vom Übertragungsverfahren (zum Beispiel Datenträgeraustausch oder E-Mail) notwendig. Ein Prüfverfahren, welches Dateien mit Makros gleich welcher Art erkennt und auf Zulässigkeit kontrolliert, ist jedoch wirkungsvoller. Damit werden nicht nur bekannte Makroviren, sondern auch nicht freigegebene Makroprogramme aller Art erfaßt.

- Wenn automatisch startende Makros nicht notwendig sind, sollte diese Automatik nach Möglichkeit abgeschaltet werden.

3.18.5 Sicherheitsfunktionen bei Standardsoftware

Zahlreiche Standardsoftwareprodukte (siehe auch Punkt 3.18.4) bieten einfache Paßwort- und Verschlüsselungsfunktionen und erwecken auf den ersten Blick den Eindruck, daß mit diesen

Funktionen bereits ein wirksamer Schutz gegen unberechtigte Kenntnisnahme schutzbedürftiger Daten erreicht werden kann.

Viele dieser Sicherheitsfunktionen sind jedoch mit geringem Aufwand zu umgehen. Die dazu geeignete Software ist für jedermann leicht zugänglich. Beispielsweise finden selbst ungeübte Internetnutzer mit Hilfe einer Suchmaschine relativ schnell sogenannte Crack-Programme, die geeignet sind, den Paßwortschutz von Datenbanken, Tabellenkalkulationen oder Textverarbeitungsprogrammen zu umgehen. Ursprünglich waren diese Hilfsprogramme dafür vorgesehen, den Zugriff auf paßwortgeschützte Datenbestände auch bei einem vergessenen Paßwort zu ermöglichen. Diese Crack-Programme können natürlich auch mißbräuchlich genutzt werden. Sie sind jedenfalls nur anwendbar, weil für Sicherheitsfunktionen der meisten Standardsoftwareprodukte keine sicheren kryptographischen Algorithmen verwendet werden beziehungsweise keine ordnungsgemäße Schlüsselverwaltungerfolgt (siehe auch Punkt 2.3).

Auch in öffentlichen Stellen des Landes existieren teilweise falsche Vorstellungen über die Qualität dieser Schutzmechanismen. In einem Fall wurde ich darüber informiert, daß bestimmte Mitarbeiter einer Behörde auf vertrauliche Daten nur im Beisein eines Vorgesetzten zugreifen durften. Dazu sollten Paßwortfunktionen einer Standarddatenbankanwendung so genutzt werden, daß erst die Eingabe eines geteilten Paßwortes nach dem „Vier-Augen-Prinzip“ den Zugriff ermöglichte. Doch damit wird die eigentliche Schwachstelle – der leicht zu brechende Paßwortschutz – nicht beseitigt.

Ich habe empfohlen, auf die Verwendung dieser Paßwortoptionen zu verzichten, damit nicht der Eindruck von Sicherheit geweckt wird, tatsächlich jedoch nur ein geringer Schutz gegen unbefugten Zugriff realisiert ist. Vielmehr sollte geprüft werden, ob nicht sichere kryptographische Verfahren eingesetzt werden können (siehe auch Zweiter Tätigkeitsbericht, Punkt 2.16.4).

3.18.6 Wenn die Festplatte defekt ist

Häufig werde ich gefragt, ob privaten Dienstleistern defekte Festplatten zur Reparatur überlassen werden dürfen, wenn sensible personenbezogene Daten darauf gespeichert sind. In diesen

Fällen bestehen berechtigte Bedenken, ob die Vertraulichkeit dieser Daten gewährleistet werden kann.

Die datenschutzgerechte Reparatur wäre möglich, wenn vor Übergabe der Festplatte alle darauf befindlichen personenbezogenen Daten gelöscht werden könnten. Voraussetzung hierfür ist allerdings, daß die Daten ordnungsgemäß gesichert worden sind. Mit entsprechenden Löschbefehlen oder durch Überschreiben können defekte Platten jedoch nicht mehr gelöscht werden. Auch die Löschung mit handelsüblichen Geräten, die ein Magnetfeld zur physischen Löschung der Platte erzeugen, ist nicht ausreichend, da der eigentliche Datenträger gegen den Einfluß von Magnetfeldern üblicherweise durch die konstruktive Gestaltung der Gehäuse weitgehend geschützt ist. Selbst wenn der eigentliche Datenträger vom Magnetfeld erreicht wird, wäre eine vollständige Löschung kaum möglich. Der verbleibende Restmagnetismus reicht oftmals aus, um mit empfindlichen Spezialköpfen die Information auszulesen. Mit modernen Verfahren kann der Inhalt von so „gelöschten“ Platten rekonstruiert werden.

Da für eine Reparatur also unvermeidlich personenbezogene Daten mit übergeben werden müßten, würde eine Datenverarbeitung im Auftrag im Sinne von § 4 DSG MV stattfinden. Der Auftraggeber bliebe in diesem Falle datenverarbeitende Stelle und wäre auch weiterhin für die Daten verantwortlich. Er müßte sicherstellen, daß eine mißbräuchliche Nutzung der Daten ausgeschlossen ist. Das ist mit vertretbarem Aufwand jedoch kaum möglich, da üblicherweise die defekte Festplatte lediglich gegen eine andere getauscht wird. Der Verbleib der Originalfestplatte ist nicht mehr nachvollziehbar und somit der Kontrolle des Auftraggebers entzogen. Kommt eine Reparatur aus den oben genannten Gründen nicht in Frage, muß die defekte Platte entweder im Besitz des Nutzers bleiben und gegen unberechtigte Zugriffe geschützt aufbewahrt werden, oder die Daten sind durch Vernichten der Festplatte physikalisch zu löschen.

Dem Wartungsunternehmen darf die defekte Platte nur dann überlassen werden, wenn sensible personenbezogene Daten verschlüsselt gespeichert sind (siehe auch Punkt 2.3). Nur unter dieser Voraussetzung kann der Auftraggeber sicherstellen, daß eine mißbräuchliche Nutzung dieser Daten ausgeschlossen ist, da ohne Kenntnis des Schlüssels nicht auf die Daten zugegriffen werden kann.

3.18.7 Datenschutz durch Havarievorsorge

Die Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) ist für zahlreiche öffentliche Stellen des Landes ein wichtiger Dienstleister. Zu ihren Auftraggebern gehören viele Landesbehörden, unter anderem das Statistische Landesamt, die Polizei und das Landesvermessungsamt, aber auch zahlreiche Kommunen.

Einige öffentliche Auftraggeber müssen sehr hohe Anforderungen an die Verfügbarkeit der von ihnen beauftragten Dienstleistungen und der auftragsgemäß verarbeiteten Daten stellen. Auch aus datenschutzrechtlicher Sicht ist die Verfügbarkeit bestimmter Datenbestände grundlegendes Schutzziel. Die DVZ M-V GmbH bietet deshalb als Absicherung gegen Schäden durch Katastrophenfälle wie Brand, Sturm, Flugzeugabstürze oder terroristische Anschläge eine Reihe von Vorsorgemaßnahmen an. Selbst im Fall schwerwiegender Schäden wird die Wiederaufnahme des Betriebes innerhalb von 48 Stunden nach solchen Ereignissen garantiert.

Voraussetzung hierfür ist zunächst eine geeignete Strategie zur regelmäßigen Sicherung der Datenbestände (Backup). Die Datenträger mit den Sicherungskopien werden in einem speziellen Sicherheitsarchiv gelagert. Außerdem werden für die hochschutzbedürftigen Anwendungen Katastrophenhandbücher erarbeitet. Diese Handbücher enthalten genaue Anweisungen, nach denen die zuständigen Fachleute handeln, um den Rechenbetrieb wieder aufzunehmen. Darüber hinaus steht der DVZ M-V GmbH ein mobiles Vorsorgerechenzentrum zur Verfügung. Dieses besteht aus mehreren Lastzügen, auf denen die Technik eines kompletten Rechenzentrums installiert ist. Die DVZ M-V GmbH hält für den Notfall lediglich einen Stellplatz mit geeigneter Infrastruktur (Anschlüsse für die Energieversorgung und Datenleitungen) bereit.

Regelmäßig werden verschiedene Katastrophenfälle geprobt. In diesem Berichtszeitraum habe ich an einer Übung teilgenommen, bei der das Automatisierte Liegenschaftsbuch (ALB) des Landesvermessungsamtes im Notfallbetrieb getestet wurde. Die Übung verlief planmäßig. An den dezentralen Arbeitsplätzen wurde nicht einmal bemerkt, daß die Umschaltung der Verarbeitung auf das mobile Vorsorgerechenzentrum erfolgt war.

Diese Art der Katastrophenvorsorge ist selbstverständlich nicht für alle datenverarbeitenden Stellen notwendig und angemessen. Havariepläne sollten jedoch überall dort vorliegen, wo eine

Verwaltung weitgehend auf das Funktionieren einer IT-Infrastruktur angewiesen ist. Oft lassen sich schon mit relativ geringem Aufwand die Auswirkungen solcher Havariefälle auf ein Minimum begrenzen. So sollten Backups immer so gelagert werden, daß beim Verlust der Originaldatenträger (zum Beispiel Festplatten in Servern) nicht auch die Sicherungskopien vernichtet werden. Außerdem sollten Systembetreuer den geordneten Wiederanlauf des Datenverarbeitungssystems planen und möglichst auch trainieren. Auf diese Weise kann die Ausfallzeit auch bei weniger schwerwiegenden Störungen minimiert werden, zum Beispiel nach eine Festplattenausfall (siehe auch Punkt 3.18.6) oder nach dem Auftreten von Computerviren, welche Daten verändern (siehe auch Punkt 3.18.4).

3.18.8 Alte Verzeichnisse auf neuen Datenträgern

In zunehmendem Maße werden CD-ROM angeboten, die Sammlungen von personenbezogenen Daten enthalten. Beispielsweise sind die seit Jahrzehnten bekannten Telefonbücher inzwischen auf CD-ROM gespeichert und im Handel erhältlich. Zumeist sind diese elektronischen Verzeichnisse umfangreicher und aussagekräftiger als die einzelnen bisher in Buchform erschienenen Datensammlungen. Es sind nicht nur Telefon- oder Adreßdaten der Bewohner eines bestimmten Ortes oder einer Region gespeichert, sondern Daten von Personen des gesamten Bundesgebietes. Hinzu kommt, daß nicht nur anhand des Namens weitere Angaben in Erfahrung gebracht werden können, sondern weitere Recherche- und Verknüpfungsmöglichkeiten zur Verfügung stehen. So kann bei einigen CD-ROM zu einer bekannten Telefonnummer durch die sogenannte Inverssuche der Anschlußinhaber problemlos gefunden werden. Selbst wenn nur Bruchstücke eines Namens, einer Telefonnummer oder einer Anschrift bekannt sind, führen Such- und Verknüpfungsmöglichkeiten zu dem aus datenschutzrechtlicher Sicht bisweilen zweifelhaften „Erfolg“.

In den Datenschutzgesetzen von Bund und Ländern wird zu Recht nach der Speicherform personenbezogener Daten unterschieden. Der Gesetzgeber hat erkannt, daß in Abhängigkeit von der jeweiligen Speicherform ein unterschiedliches Gefährdungspotential für den Mißbrauch dieser Daten ausgeht. Für die automatisierte Verarbeitung personenbezogener Daten fordert er deshalb besondere technische und organisatorische Maßnahmen. Die Datenschutzbeauftragten des Bundes und der Länder sehen die Entwicklung mit Sorge. Die genannten Vorkehrungen

verhindern nicht, daß mit Hilfe der verschiedenen, am Markt erhältlichen elektronischen Verzeichnisse Persönlichkeitsprofile erstellt werden können, die beispielsweise für Direktmarketingunternehmen von Interesse sind. Das bisher in vielen Bereichen geltende Widerspruchsrecht, beispielsweise gegen die Meldedatenübermittlung an Adreßbuchverlage, genügt nach bisherigen Erfahrungen nicht mehr, um die Privatsphäre Betroffener in angemessener Weise zu schützen. Auch im Telekommunikationsbereich sollte in Zukunft berücksichtigt werden, daß nicht jeder Kunde, der die Veröffentlichung seiner Daten im konventionellen Telefonbuch zuläßt, möchte, daß sie auch auf einem elekronischen Datenträger erscheinen.

Im Telekommunikationsbereich existieren bereits gesetzliche Regelungen, die zur datenschutzfreundlichen Ausgestaltung öffentlicher Kundenverzeichnisse beitragen sollen. Die Telekommunikationsdienstunternehmen-Datenschutzverordnung (siehe auch Punkt 3.10.4) erlaubt es den TK-Diensteanbietern, diese Verzeichnisse in gedruckter und elektronischer Form herauszugeben. Die Kunden haben jedoch die Möglichkeit, die Art des Eintrags in gedruckte Verzeichnisse weitgehend frei zu bestimmen, einen Eintrag vollständig abzulehnen und der Aufnahme in elektronische Verzeichnisse zu widersprechen. Das Telekommunikationsgesetz (siehe auch Punkt 3.10.2) geht noch einen Schritt weiter. Kunden können hiernach in gedruckte oder elektronische Verzeichnisse nur dann aufgenommen werden, wenn sie dies ausdrücklich beantragt haben. Da die Regelungen des später in Kraft getretenen TKG denen der TDSV vorgehen, sind Übergangsregelungen notwendig. Für einen Kunden, der beim Inkrafttreten des TKG bereits in ein Kundenverzeichnis eingetragen war, unterbleibt die Eintragung erst dann, wenn er widerspricht.

Aber selbst eine solche auf den ersten Blick datenschutzfreundlich erscheinende Lösung ist nicht unproblematisch. Fehlt der Hinweis im gedruckten Verzeichnis, daß ein Kunde gegen die Aufnahme seiner Daten in elektronische Verzeichnisse widersprochen hat, bedeutet das wegen der mangelnden Aktualität gedruckter Verzeichnisse nicht automatisch, daß er einverstanden ist. CD-ROM-Herausgeber müssen also damit rechnen, daß auch nicht besonders gekennzeichnete Kunden widersprochen haben. Darüber hinaus ist die Kennzeichnung selbst auch wieder ein personenbezogenes Datum. Der Kunde müßte deshalb ausdrücklich die Aufnahme dieser zusätzlichen Angabe im Sinne des TKG beantragen.

Die Deutsche Telekom kommt der Pflicht zur Information ihrer Kunden zu diesen schwer durchschaubaren Einwilligungs- und Widerspruchsmöglichkeiten durch Informationsschriften und durch Einrichtung einer Hotline nach. Wie andere TK-Unternehmen ihre Kunden über ihre Rechte informieren werden, bleibt abzuwarten.

Die Veröffentlichung von Adreßbüchern auf elektronischen Medien ohne angemessene Beteiligung der Betroffenen würde ebenfalls einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen. Auch deshalb ist im Landesmeldegesetz Mecklenburg-Vorpommern festgelegt, daß Meldedaten an Adreßbuchverlage nur zum Zweck der Herausgabe von Adreßbüchern in gedruckter Form übermittelt werden dürfen. Sowohl diese Beschränkung als auch die Vorschrift, daß die Daten ausschließlich in alphabetischer Reihenfolge veröffentlicht werden dürfen, sind vom Gesetzgeber vorgesehene - wenn auch recht schwache - Schutzmechanismen für diese Daten vor Mißbrauch. Denn die besondere Problematik elektronischer Verzeichnisse bleibt weiterhin bestehen, da nicht verhindert werden kann, daß Dritte Daten aus Adreßbüchern zur Herstellung solcher Verzeichnisse verwenden.

Unser Innenministerium hat bereits im Frühjahr 1996 in einem Rundschreiben darauf hingewiesen, daß sich Meldebehörden vor der Datenübermittlung an Adreßbuchverlage von der ausschließlichen Nutzung dieser Daten für die Herausgabe gedruckter Verzeichnisse vergewissern müssen. Es wurde empfohlen, die Einwohner im Rahmen der amtlichen Bekanntmachung zur Widerspruchsmöglichkeit darauf aufmerksam zu machen, daß bei einer Veröffentlichung im gedruckten Adreßbuch nicht ausgeschlossen werden kann, daß Dritte diese Daten trotzdem nutzen, um elektronische Verzeichnisse herzustellen und zu vertreiben.

Bereits im Ersten Tätigkeitsbericht, Punkt 2.3.5, hatte ich empfohlen, die im Landesmeldegesetz formulierte Widerspruchsregelung in eine Zustimmungsregelung umzuwandeln. Im Saarland gilt seit August 1997 diese datenschutzfreundliche Variante der Datenübermittlungsvorschrift an Adreßbuchverlage. Dort dürfen nunmehr nur noch dann Vor- und Familiennamen, Doktorgrad und Anschriften an Adreßbuchverlage übermittelt werden, wenn der Betroffene dieser Datenübermittlung ausdrücklich zugestimmt hat. Er kann dabei bestimmen, ob die Eintragung in gedruckten, elektronischen oder beiden Verzeichnissen erfolgt.

3.18.9 Datenschutzgerechter Einsatz von Chipkartensystemen

Die Chipkartenindustrie präsentiert ein ständig zunehmendes Angebot an technischen Lösungen, beispielsweise im Bereich der elektronischen Zahlungssysteme, der Personenidentifikation oder im Gesundheitswesen. Darüber hinaus wird die Herstellung und Nutzung multifunktioneller Chipkarten untersucht.

In vielen Fällen dienen Chipkarten als Speicher sensibler personenbezogener Daten. Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb seit langem effektive Regelungen des Datenschutzes für Chipkartensysteme (siehe Zweiter Tätigkeitsbericht, 1. und 24. Anlage). Die Bundesregierung hat die Empfehlung der Datenschutzbeauftragten, Sonderregelungen zu Chipkarten in den Entwurf zur Novellierung des Bundesdatenschutzgesetzes (BDSG) aufzunehmen, bisher nicht aufgegriffen (siehe auch Punkt 2.4 und 13. Anlage). Lediglich für den Teilbereich der Krankenversichertenkarte hat der Gesetzgeber die Einführung von Chipkartensystemen geregelt (§ 291 SGB V).

Neben der Schaffung rechtlicher Rahmenbedingungen sind für den Einsatz von Chipkartensystemen geeignete technische und organisatorische Maßnahmen von grundlegender Bedeutung, um zu verhindern, daß Informationen unbefugt preisgegeben, verändert oder vorenthalten werden. Diese Gefahren sind sowohl dann zu berücksichtigen, wenn die Daten auf der Chipkarte selbst gespeichert sind, als auch dann, wenn sie in einer externen Datenbank gespeichert werden, die sich durch die Chipkarte erschließen läßt. Es ist also eine komplexe Sicherungstechnologie erforderlich.

Eine Arbeitsgruppe des AK Technik (siehe auch Punkt 3.20.1) hat dazu die Orientierungshilfe "Anforderungen zur informationstechnischen Sicherheit bei Chipkarten" erstellt, in der auch Empfehlungen zum datenschutzgerechten Einsatz von Chipkartensystemen gegeben werden. Die folgenden Hinweise orientieren sich an dieser Ausarbeitung.

Datensicherungsmaßnahmen müssen in ihrer Gesamtheit einen hinreichenden Schutz der Daten vor Mißbrauch gewährleisten. Die Vertraulichkeit, Integrität, Verfügbarkeit und Authentität der auf der Chipkarte gespeicherten Daten muß weitgehend sichergestellt werden können.

Vor der Entscheidung über den sicherheitsrelevanten Einsatz von Chipkarten-Anwendungen sollte deshalb 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 es sind Lösungsvorschläge für eine Sicherungstechnologie zu erarbeiten. Dabei ist zwischen den technischen Systemen (künftig vorwiegend auf Basis der Prozessorchipkartentechnologie) und den Anwendungen, die sich dieser Systeme bedienen, zu unterscheiden. Neben der eigentlichen Chipkarte und deren Herstellung, Initialisierung und Versand muß in die Betrachtungen auch das Kartenterminal (Chipkartenbasiertes Dienstleistungssystem - CDLS) einbezogen werden.

Ein Sicherungskonzept für Chipkarten sollte entsprechend des Schutzbedarfs folgende Mindestanforderungen erfüllen:

1) Grundschutzmaßnahmen

- Ausstattung des Kartenkörpers mit fälschungssicheren Authentisierungsmerkmalen, wie Unterschrift, Foto oder Hologramm
- 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 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 Anwen-

dungen, 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 beziehungsweise 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 (siehe auch Punkt 2.1).

4) Der Chipkarteninhaber beziehungsweise 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.

Der vollständige Text der Orientierungshilfe ist in meiner Dienststelle kostenlos erhältlich.

3.18.10 Datenschutz im Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik

In zahlreichen öffentlichen Stellen wird Informationstechnik (IT) eingesetzt, um die Effizienz der Verwaltung zu erhöhen. Dieser Effekt kann jedoch nur dann eintreten, wenn die Informations- und Kommunikationssysteme störungsfrei und sicher funktionieren. Um diesen Gesichtspunkt während der Planung, der Realisierung und des Betriebs der Systeme angemessen zu berücksichtigen, sind insbesondere die Empfehlungen aus dem Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) als Orientierungspunkte gut geeignet. Der Schutzbedarf für personenbezogene Daten war dabei bisher jedoch noch nicht ausreichend berücksichtigt worden (siehe auch Zweiter Tätigkeitsbericht, Punkt 2.16.5).

Das BSI hatte den Bundesbeauftragten für den Datenschutz (BfD) um Unterstützung für eine entsprechende Ergänzung des Grundschutzhandbuches gebeten. Unter dem Dach des Arbeitskreises "Technische und organisatorische Datenschutzfragen" wurde daraufhin eine Arbeitsgruppe gebildet, die unter Federführung des BfD Erläuterungen zu technischen und organisatorischen Aspekten des Datenschutzes im Grundschutzhandbuch ausarbeiten sollte. Dazu mußten einerseits die Bewertungskriterien für die Schutzbedürftigkeit von IT-Verfahren erweitert werden, da die Bewertung von Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung bisher sehr pauschal gehalten waren. Andererseits waren aus datenschutzrechtlicher Sicht Maßnahmen erforderlich, die im Grundschutzhandbuch bisher nur als Option genannt wurden, zum Beispiel die Transportverschlüsselung personenbezogener Daten. Letztlich sind zur Umsetzung datenschutzrechtlicher Vorschriften geeignete organisatorische Maßnahmen notwendig. Beispielsweise ist darauf zu achten, daß ein Interessenkonflikt des behördlichen beziehungsweise betrieblichen Datenschutzbeauftragten mit anderen Aufgaben vermieden werden muß.

Die Ergänzung im Grundschutzhandbuch soll dazu beitragen, die Auswahl und Umsetzung datenschutzrechtlich bedingter technischer und organisatorischer Maßnahmen zu erleichtern und die Anwendung des Grundschutzhandbuches auch in diesem Zusammenhang zu ermöglichen. Auch für personenbezogene Daten kann somit ein Grundschutz sichergestellt werden. Um das Kapitel uneingeschränkt sowohl für den öffentlichen als auch für den nichtöffentlichen

Bereich anwenden zu können, wird voraussichtlich auf rechtliche Erörterungen weitgehend verzichtet.

Zum Abschnitt „Datenschutz“ im IT-Grundschutzhandbuch liegt ein Entwurf vor. Bis Ende 1997 konnte er von künftigen Anwendern aus der Wirtschaft und den Behörden beim Bundesbeauftragten für den Datenschutz angefordert werden, um Änderungsvorschläge zu unterbreiten und Ergänzungshinweise zu geben. Rechtzeitig eingegangene Hinweise sollen dann bei der endgültigen Formulierung berücksichtigt werden. Es ist zu erwarten, daß die endgültige Fassung in der 1998 erscheinenden Auflage des IT-Grundschutzhandbuches des BSI enthalten sein wird.

3.19 Organisation

3.19.1 Umgang mit sensiblen Daten beim Pförtner der Staatsanwaltschaft

Eine Petentin suchte eine Staatsanwaltschaft auf, um dem für ihre Angelegenheit zuständigen Mitarbeiter einen Brief persönlich zu übergeben. Das Aktenzeichen des Vorgangs, mit Hilfe dessen sie bereits telefonisch Auskunft erhalten hatte, war auf dem Umschlag vermerkt. Als sie sich beim Pförtner anmeldete, nahm dieser den Brief entgegen und erläuterte den Sachverhalt telefonisch einem Mitarbeiter. In dem Warteraum, der als „Anmeldung“ gekennzeichnet ist, saß ein zweiter Bürger, der alle Erläuterungen einschließlich personenbezogener Daten mithören konnte. Ein dritter Bürger kam hinzu. Auch dessen Angelegenheit wurde vor allen Anwesenden telefonisch „abgehandelt“. Nachdem die Petentin ihr Mißfallen über diese Vorgehensweise geäußert hatte, ließ sie ihren Brief dort, und der Pförtner versah diesen mit einem Eingangsstempel.

Die Petentin wandte sich an mich und bat um datenschutzrechtliche Prüfung des Vorgangs. Im Ergebnis habe ich der Staatsanwaltschaft empfohlen, technische und organisatorische Maßnahmen zu realisieren, um künftig auszuschließen, daß sensible personenbezogene Daten im Pförtnerbereich von jedermann mitgehört werden können.

- Die Pförtner wurden angewiesen, daß sie mit sensiblen Daten in Zukunft sorgfältiger umzugehen haben.

- Sie haben darauf zu achten, daß die Verbindungstüren zur Pforte und zum Warteraum während der Telefonate geschlossen sind.
- Außerdem sind grundsätzlich nur die Daten zu erfragen, die unbedingt notwendig sind, um dem Bürger mit seinem Anliegen weiterzuhelfen.

Abschließend habe ich der Staatsanwaltschaft empfohlen, diese Maßnahmen in schriftlicher Form, beispielsweise in einer Dienstanweisung, festzuhalten. Eine Antwort steht noch aus.

3.19.2 Auftragsdatenverarbeitung und Verträge

Häufig vergeben kleine Kommunen Datenverarbeitungs-Aufträge an Dienstleistungsunternehmen, weil sie selbst nicht über die finanziellen und personellen Mittel zum Aufbau und zur Unterhaltung einer eigenen Datenverarbeitungs-Infrastruktur verfügen. Es handelt sich hierbei um den Umgang mit personenbezogenen Daten im Auftrag, der gemäß § 4 DSG MV in einem schriftlichen Vertrag zu regeln ist.

Neben anderen Aspekten ist bei der Vertragsgestaltung vor allem darauf zu achten, daß die Auftragsvergabe nicht zur völligen Abhängigkeit des Auftraggebers führt. Deshalb muß beim Auftraggeber immer soviel eigene Fachkompetenz vorgehalten werden, daß Verträge sachgerecht gestaltet sowie Leistung und Qualität der vertraglich geregelten Dienstleistungen abgenommen und kontrolliert werden können. So muß der Auftraggeber beispielsweise wenigstens die Eignung eines potentiellen Auftragnehmers feststellen können. Dazu muß er in der Lage sein, bei diesem die erforderlichen technischen und organisatorischen Maßnahmen zu überprüfen.

In einem konkreten Fall hatte ich bei einer Kontrolle festgestellt, daß bereits die Ausarbeitung der Verträge dem zukünftigen Dienstleister überlassen worden war, da die betroffenen Kommunen selbst dazu nicht in der Lage waren. Immerhin hatte mich dann jedoch die Privatfirma um Beratung gebeten, weil auch sie noch keine Erfahrung in der Formulierung solcher Verträge hatte.

Da Datenverarbeitung im Auftrag die verschiedensten Bereiche betreffen kann, ist es kaum möglich, in einem Mustervertrag alle erforderlichen Aspekte zu berücksichtigen. Verträge müssen immer auf den einzelnen Fall zugeschnitten werden. Nachfolgend sind datenschutzrechtliche Anforderungen genannt, die in jedem Vertrag zum Umgang mit personenbezogenen Daten im Auftrag enthalten sein sollten:

- detaillierte Angaben zu Gegenstand und Umfang der Datenverarbeitung,
- die erforderlichen technischen und organisatorischen Maßnahmen nach dem Stand der Technik (§ 17 DSG MV),
- Regelungen zur Auskunft, Berichtigung, Löschung und Sperrung von personenbezogenen Daten,
- Ausschluß von Unterauftragsverhältnissenoder Zustimmungsvorbehalte des Auftraggebers,
- Weisungsrecht des Auftraggebers,
- alleiniges Verfügungsrecht des Auftraggebers über die Daten,
- umfassende Kontrollrechte des Auftraggebers,
- Freigabe des Verfahrens durch den Auftraggeber,
- Kündigungsrechte, insbesondere bei Verletzung von Datenschutzvorschriften durch den Auftragnehmer,
- Hinweispflicht des Auftragnehmers auf Datenschutzverletzungen,
- Unterwerfung unter die Kontrolle des Landesbeauftragten für den Datenschutz bei Auftragnehmern aus dem nicht-öffentlichen Bereich,
- Verpflichtung der Mitarbeiter auf das Datengeheimnis nach § 5 DSG MV.

Darüber hinaus sind Meldepflichten zu beachten, die die Auftraggeber und Auftragnehmer einzuhalten haben. Der Auftraggeber muß den Landesbeauftragten für den Datenschutz über die Beauftragung informieren. Der Auftragnehmer muß seiner Meldepflicht nach § 32 BDSG gegenüber der zuständigen Aufsichtsbehörde nachkommen.

3.19.3 Neue Organisationsformen in der Verwaltung

Verwaltungen sollten ständig bemüht sein, ihre Dienstleistungen zu verbessern und den Bürger dabei als Kunden zu betrachten. Die Einrichtung von sogenannten Bürger- oder Stadtteilbüros

oder Außenstellen von Landratsämtern, in denen beispielsweise Wohnberechtigungsscheine, Sozialhilfe oder andere kommunale Leistungen beantragt werden können, ist dabei sicher ein Schritt in diese Richtung. Aufgaben, für die bisher verschiedene Fachämter zuständig sind, sollen künftig in der Nähe der Wohnung angeboten werden, um den Bürgern Wege und lange Wartezeiten zu ersparen sowie die Orientierung im Ämterdschungel gegenstandslos zu machen.

Eine Stadt unseres Landes plant beispielsweise, soziale Leistungen in Stadtteilbüros anzubieten. In einem ersten Schritt wurden zu diesem Zweck die Verwaltungsbereiche des Sozialamtes, des Jugendamtes und des Amtes für Wohnungswesen in einem Amt für Jugend, Soziales und Wohnen zusammengefaßt. Die fachliche Arbeit erfolgt gegenwärtig noch getrennt, das heißt, Leistungen jedes der drei Ämter werden ohne gemeinsame Verarbeitung oder Nutzung der Sozialdaten erbracht. In der weiteren Folge sollen Stadtteilbüros eingerichtet werden, deren Arbeitsweise durch einen „ganzheitlichen Ansatz“ gekennzeichnet sein soll. Mit diesem Ansatz könnte dann auch die umfassende Beratung der Bürger sowie die Erhebung, Verarbeitung und Nutzung ihrer Daten durch den Ansprechpartner in einem solchen Büro verbunden sein.

Neben den Vorteilen, die sich für die Bürger daraus ergeben können, enthalten solche Verfahren aber auch datenschutzrechtliche Risiken. Es besteht die Gefahr des „gläsernen Bürgers“. Insbesondere ist die notwendige funktionelle und personelle Trennung bei der Wahrnehmung verschiedener Aufgaben nicht ohne weiteres gewährleistet.

Selbst wenn den Bürgern die Wahl zwischen der funktionell und personell getrennten Bearbeitung von Leistungsansprüchen nach herkömmlicher Art und zwischen der Bearbeitung in Stadtteilbüros angeboten wird, wären hierfür gesetzliche Änderungen erforderlich.

Weniger bedenklich wäre dagegen eine umfassende Beratung der Bürger, da diese prinzipiell auch durchgeführt werden kann, ohne daß in großem Umfang personenbezogene Daten angegeben werden müssen, oder auch lediglich die Ausgabe von Anträgen auf Sozialleistungen beziehungsweise eine allgemeine Beratung zum Ausfüllen der Anträge.

Ich habe die Stadt auf die datenschutzrechtliche Bedeutung dieser geplanten strukturellen Änderungen hingewiesen. Ein konkreter Termin für die Neuorganisation auch der fachlichen Arbeit im Amt für Jugend, Soziales und Wohnen konnte bisher nicht genannt werden. Es wurde zugesichert, daß die erforderlichen Maßnahmen sorgfältig geprüft werden.

4 Arbeitskreis „Technische und organisatorische Datenschutzfragen“

Im Februar 1993 hat mir die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den Vorsitz des Arbeitskreises "Technische und organisatorische Datenschutzfragen" (AK Technik) übertragen (siehe Erster Tätigkeitsbericht, Punkt 2.21.1). Der Arbeitskreis berät die Konferenz vorwiegend in technischen Fragen und unterstützt die Beratungstätigkeit der Datenschutzbeauftragten durch die Anfertigung von Gutachten, Empfehlungen und Orientierungshilfen.

Im Berichtszeitraum habe ich vier Sitzungen in Bonn, Schwerin und Wismar vorbereitet und durchgeführt. Schwerpunkte der Zusammenarbeit im Bereich Technik waren unter anderem die Themen Chipkarte, Kryptographie, Grundschutz, Telefax und datenschutzfreundliche Technologien.

Die Vielfalt der zu bearbeitenden Themen hat zu einer Form der Zusammenarbeit geführt, die für einen Arbeitskreis der Datenschutzbeauftragten bisher untypisch war. Es wurden mehrere Arbeitsgruppen aus Mitgliedern des AK Technik gebildet, die auch durch Nutzung neuer Kommunikationsmedien wie E-Mail und Mailboxen oft schon in kurzer Zeit konkrete Ergebnisse vorlegen konnten, über deren weitere Verwendung der Arbeitskreis dann im Einzelfall entschieden hat.

Diese Arbeitsweise hat zu einer zusätzlichen Belastung der bundesweit beteiligten Kollegen geführt, die sie mit viel persönlichem Engagement auf sich genommen haben. Die Ergebnisse zeigen jedoch, daß das Spezialwissen der einzelnen Kollegen so am besten nutzbar gemacht und vorhandene Fachkompetenz entsprechend der zeitlichen und personellen Ressourcen optimal eingesetzt werden kann. In diesen Arbeitsgruppen sind in zunehmendem Maße externe Spezialisten aus Wissenschaft, Industrie und Verwaltung vertreten, die beispielsweise neueste Erkenntnisse der Forschung einbringen und die technische Realisierbarkeit oder als zukünftige Anwender die Umsetzbarkeit von Empfehlungen der Datenschutzbeauftragten bewerten können.

Hervorzuheben sind die Kontakte zur Europäischen Kommission. Insbesondere mit der Generaldirektion XV hat sich eine konstruktive Zusammenarbeit entwickelt. So findet unter anderem ein ständiger Informationsaustausch zu international relevanten datenschutzrechtlichen Themen statt. Darüber hinaus wurde eine Mitarbeiterin der Generaldirektion XV direkt in die oben beschriebene Arbeitsgruppentätigkeit einbezogen. Die unter Punkt 2.1 beschriebenen Papiere des AK Technik wurden mit Mitteln der Europäischen Kommission in Englisch und Französisch übersetzt und unter folgenden Adressen im Internet veröffentlicht:

- http://europa.eu.int/comm/dg15
- http://www2.echo.lu/legal/en/dataprot/dataprot.html

Die Ausarbeitungen des AK Technik sind in meiner Dienststelle kostenlos erhältlich. Im Berichtszeitraum wurden folgende Papiere veröffentlicht:

- Orientierungshilfe „Anforderungen zur informationstechnischen Sicherheit von Chipkarten“ (siehe auch Punkt 3.18.9),
- Entwurf eines Datenschutzkapitels für das IT-Grundschutzhandbuch des BSI (siehe auch Punkt 3.18.10),
- Grenzen und Möglichkeiten der staatlichen Reglementierung des Einsatzes von Verschlüsselungsverfahren (siehe auch Punkt 2.3),
- Datenschutzfreundliche Technologien (siehe auch Punkt 2.1),
- Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu Datenschutz und Telefax (siehe auch Punkt 3.18.3).

5 Zusammenarbeit mit Landes- und Kommunalverwaltungen

Im Zweiten Tätigkeitsbericht hatte ich an der Zusammenarbeit mit dem Interministeriellen Ausschuß für Informations- und Telekommunikationstechnik (IMA IT) Kritik geübt (siehe Zweiter Tätigkeitsbericht, Punkt 2.17.1).

Die Beratungen des Landtages zu meinem Bericht und zur Stellungnahme der Landesregierung (Drucksache 2/1573) führten zu einem Landtagsbeschluß, in dem der Regierung unter anderem die ständige Beteiligung des Landesbeauftragten für den Datenschutz an den Beratungen des IMA-IT empfohlen wurde (Drucksache 2/2327).

Danach wurde es möglich, die obersten Landesbehörden in angemessener Weise effektiv und frühzeitig vor der Einführung neuer automatisierter Verfahren zur Verarbeitung personenbezogener Daten so zu beraten, wie es beispielsweise von Beginn an bei den Planungen zu einer Netzwerkkonzeption der Landesregierung oder zur Einrichtung eines elektronischen Postsystems (siehe auch Punkt 3.18.2) der Fall war.

In den IT-Richtlinien des Landes wird empfohlen, daß Landes- und Kommunalverwaltungen auch auf dem Gebiet der Informationstechnik zusammenarbeiten. Auf Initiative der Koordinierungs- und Beratungsstelle der Landesregierung für IT in der Landesregierung (LKSt) wurde im Frühjahr 1996 der Kooperationsausschuß IT (Koop IT) gegründet, in dem Vertreter von Städten, Landkreisen und Ministerien einen ständigen Erfahrungsaustausch pflegen sollten. Um datenschutzrechtliche Fragen angemessen berücksichtigen zu können, wurde auch ich zu den Sitzungen des Koop IT eingeladen.

Die ersten beiden Zusammenkünfte zeigten, daß der Bedarf am Informationsaustausch auch deshalb groß war, weil der Ausbau der IT-Infrastruktur in der Kommunalverwaltung unterschiedlich weit vorangeschritten ist. Die Bandbreite der Ausstattung reicht von Einzelplatz-PC bis zu umfangreichen lokalen Netzwerken mit Intranetstrukturen und Internetnutzung.

In den ersten beiden Sitzungen zeigte sich vor allem Beratungsbedarf zu den Themen Internet, E-Mail und Telekommunikationsanlagen. Der Geschäftsführer des Landkreistages hat daraufhin allen Landkreisen Datenschutz-Informationsmaterial (unter anderem Orientierungshilfen und Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder) zugesandt.

Leider kam es bisher nur zu diesen beiden Sitzungen des Koop IT. Die LKSt war aus personellen Gründen nicht in der Lage, weitere Zusammenkünfte zu organisieren. Ich bedaure dies sehr, da der Koop IT meines Erachtens eine gute Möglichkeit darstellt, auch im kommunalen Bereich auf effektive Weise beraten zu können. Ich würde es sehr begrüßen, wenn die Zusammenarbeit zwischen Landes- und Kommunalverwaltungen im Rahmen des Koop IT wieder intensiviert würde.

6 Öffentlichkeitsarbeit

Im Berichtszeitraum haben meine Mitarbeiter und ich Vorträge zu unterschiedlichen datenschutzrechtlichen Themen gehalten. Dabei wurden sowohl grundsätzliche Fragen des Datenschutzes als auch juristische Sachverhalte erläutert, um auch spezialgesetzliche Datenschutzregelungen für die Anwender in der Landesverwaltung und im kommunalen Bereich transparenter zu machen. Technische Fragestellungen bildeten einen weiteren Schwerpunkt. Zu folgenden Themen wurden Vorträge gehalten beziehungsweise Beratungen durchgeführt:

- Grundsätze des Datenschutzes
- Nutzung von Archivgut
- Datenschutz in der Schule
- Umgang mit Sozialdaten
- Kinder- und Jugendhilfe
- Datenschutzrechtliche Anforderungen bei Personaldatenverarbeitungsanlagen
- Adoptionsvermittlung
- Arzneimittelforschung
- Krebsregister
- Asylbewerberdaten
- Medizinische Datennetze
- Schulgesundheitspflegeverordnung
- Fragen des Datenschutzes bei der Schuldnerberatung
- Elektronischer Gesundheitsdienst
- Personenbezogene Müllerfassung
- Umgang mit Patientendaten
- ISDN-Telekommunikationsanlagen
- Nutzung des Internet in Behörden
- Neue Gesetze im Telekommunikationsbereich

Auch die steigende Nachfrage nach schriftlichem Informationsmaterial zu verschiedenen Themen zeigt, daß datenschutzrechtliche Fragen sowohl in der Verwaltung als auch bei den Bürgern auf zunehmendes Interesse stoßen. So war beispielsweise die erste Auflage der Broschüre

„Gesetze und Verordnungen zum Datenschutz“ nach kurzer Zeit vergriffen. Die zweite Auflage, die ich zur besseren Aktualisierung in Ringordnerform herausgegeben habe, ist seit September 1997 in meiner Dienstelle kostenlos erhältlich.

Orientierungshilfen zu vorwiegend technischen Themen, die im Rahmen des Arbeitskreises "Technische und organisatorische Datenschutzfragen" erarbeitet wurden (siehe Punkt 3.20.1), sind in vielen öffentlichen Stellen zu wichtigen Hilfsmitteln bei der datenschutzgerechten Ausgestaltung von automatisierten Verfahren zur Verarbeitung personenbezogener Daten geworden. In der Broschüre „Technik und Datenschutz“ habe ich deshalb einige Arbeitsergebnisse des Arbeitskreises veröffentlicht. Vor allem diejenigen Mitarbeiter, die für die Planung und die Administration von Informations- und Kommunikationstechnik verantwortlich sind, erhalten damit einen Überblick über technische und organisatorische Maßnahmen, die für den datenschutzgerechten Betrieb dieser Technik erforderlich sind.

7 Anlagen

1. Anlage: Entschließung der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996

Modernisierung und europäische Harmonisierung des Datenschutzrechts

Die Datenschutzrichtlinie der Europäischen Union vom Oktober 1995 verpflichtet alle Mitgliedstaaten, ihr Datenschutzrecht binnen drei Jahren auf europäischer Ebene zu harmonisieren. Die Richtlinie geht zu Recht von einem hohen Datenschutzniveau aus und stellt fest: "Die Datenverarbeitungssysteme stehen im Dienste des Menschen".

Die Datenschutzbeauftragten begrüßen diesen wichtigen Schritt zu einem auch international wirksamen Datenschutz. Sie appellieren an den Gesetzgeber in Bund und Ländern, die Umsetzung der Richtlinie nicht nur als Beitrag zur europäischen Integration zu verstehen, sondern als Aufforderung und Chance, den Datenschutz fortzuentwickeln. Die Datenschutzbeauftragten sprechen sich für eine umfassende Modernisierung des deutschen Datenschutzrechts aus, damit der einzelne in der sich rapide verändernden Welt der Datenverarbeitung, der Medien und der Telekommunikation über den Umlauf und die Verwendung seiner persönlichen Daten soweit wie möglich selbst bestimmen kann.

Die wichtigsten Ziele sind:

1. Weitgehende Vereinheitlichung der Vorschriften für den öffentlichen und privaten Bereich mit dem Ziel eines hohen, gleichwertigen Schutzes der Betroffenen, beispielsweise bei der Datenerhebung und bei der Zweckbindung bis hin zur Verarbeitung in Akten
2. Erweiterung der Rechte der Betroffenen auf Information durch die datenverarbeitenden Stellen über die Verwendung der Daten, auf Auskunft, auf Widerspruch und im Bereich der Einwilligung

3. Verpflichtung zu Risikoanalyse, Vorabkontrolle, Technikfolgenabschätzung und zur Beteiligung der Datenschutzbeauftragten bei der Vorbereitung von Regelungen mit Auswirkungen auf den Datenschutz

4. Verbesserung der Organisation und Stärkung der Befugnisse der Datenschutzkontrolle unter den Gesichtspunkten der Unabhängigkeit und der Effektivität

5. Einrichtung und effiziente Ausgestaltung des Amtes eines internen Datenschutzbeauftragten in öffentlichen Stellen

6. Weiterentwicklung der Vorschriften zur Datensicherheit, insbesondere im Hinblick auf Miniaturisierung und Vernetzung

Darüber hinaus machen die Datenschutzbeauftragten folgende Vorschläge:

7. Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen und Regelung der Video-Überwachung

8. Stärkere Einbeziehung von Presse und Rundfunk in den Datenschutz; Aufrechterhaltung von Sonderregelungen nur, soweit dies für die Sicherung der Meinungsfreiheit notwendig ist

9. Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren

10. Sicherstellung der informationellen Selbstbestimmung bei Multimedia-Diensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsformen anzubieten, durch den Schutz vor übereilter Einwilligung, z. B. durch ein Widerrufsrecht, und durch strenge Zweckbindung für die bei Verbindung, Aufbau und Nutzung anfallenden Daten

11. Besondere Regelungen für Chipkarten-Anwendungen, um die datenschutzrechtliche Verantwortung aller Beteiligten festzulegen und den einzelnen vor unfreiwilliger Preisgabe seiner Daten zu schützen

12. Schutz bei Persönlichkeitsbewertungen durch den Computer, insbesondere durch Beteiligung des Betroffenen und Nachvollziehbarkeit der Computerentscheidung

13. Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing

14. Verbesserung des Datenschutzes bei grenzüberschreitender Datenverarbeitung; Datenübermittlung ins Ausland nur bei angemessenem Datenschutzniveau

2. Anlage: Entschließung der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996

Transplantationsgesetz

Bei der anstehenden gesetzlichen Regelung, unter welchen Voraussetzungen die Entnahme von Organen zur Transplantation zulässig sein soll, werden untrennbar mit der Ausformung des Rechts auf Selbstbestimmung auch Bedingungen des Rechts auf informationelle Selbstbestimmung festgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont hierzu, daß von den im Gesetzgebungsverfahren diskutierten Modellen die "enge Zustimmungslösung" - also eine ausdrückliche Zustimmung des Organspenders - den geringsten Eingriff in das Recht auf informationelle Selbstbestimmung beinhaltet. Sie zwingt niemanden, eine Ablehnung zu dokumentieren. Sie setzt auch kein Organspenderegister voraus.

Mit einer engen Zustimmungslösung ist auch vereinbar, daß der Organspender seine Entscheidung z. B. einem nahen Angehörigen überträgt.

3. Anlage: Entschließung der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996

Grundsätze für die öffentliche Fahndung im Strafverfahren

Bei den an die Öffentlichkeit gerichteten Fahndungsmaßnahmen nach Personen (Beschuldigten, Verurteilten, Strafgefangenen und Zeugen) wird stets das Recht des Betroffenen auf informationelle Selbstbestimmung eingeschränkt. Es bedarf daher nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil vom 15. Dezember 1983 für alle Maßnahmen der öffentlichen Fahndung nach Personen einer normenklaren und dem Grundsatz der Verhältnismäßigkeit entsprechenden gesetzlichen Regelung, die bisher fehlt.

1. Der Gesetzgeber hat zunächst die Voraussetzungen der öffentlichen Fahndung zu regeln und dabei einen sachgerechten Ausgleich zwischen dem öffentlichen Strafverfolgungsinteresse und dem Recht auf informationelle Selbstbestimmung des Betroffenen zu treffen.

   Die öffentliche Fahndung sollte nur bei Verfahren wegen Verletzung bestimmter vom Gesetzgeber zu bezeichnender Straftatbestände und bei Straftaten, die aufgrund der Art der Begehung oder des verursachten Schadens ein vergleichbares Gewicht haben, zugelassen werden.

   Sie soll nur stattfinden, wenn weniger intensive Fahndungsmaßnahmen keinen hinreichenden Erfolg versprechen.

   Der Grundsatz der Erforderlichkeit mit der gebotenen Beschränkung des Verbreitungsgebiets ist auch bei der Auswahl des Mediums zu berücksichtigen.

2. Bei der öffentlichen Fahndung nach unbekannten Tatverdächtigen, Beschuldigten, Angeschuldigten, Angeklagten einerseits und Zeugen andererseits erscheint es geboten, die Entscheidung, ob und in welcher Weise gefahndet werden darf, grundsätzlich dem Richter vorzubehalten; dies gilt nicht bei der öffentlichen Fahndung zum Zwecke der Straf- oder Maßregelvollstreckung gegenüber Erwachsenen.

Bei Gefahr in Verzug kann eine Eilkompetenz der Staatsanwaltschaft vorgesehen werden; dies gilt nicht bei der öffentlichen Fahndung nach Zeugen. In diesem Falle ist unverzüglich die richterliche Bestätigung der Maßnahme einzuholen.

Die öffentliche Fahndung nach Beschuldigten setzt voraus, daß ein Haftbefehl oder Unterbringungsbefehl vorliegt, bzw. dessen Erlaß nicht ohne Gefährdung des Fahndungserfolges abgewartet werden kann.

3. Eine besonders eingehende Prüfung der Verhältnismäßigkeit hat bei der Fahndung nach Zeugen stattzufinden.

   Eine öffentliche Fahndung nach Zeugen darf nach Art und Umfang nicht außer Verhältnis zur Bedeutung der Zeugenaussage für die Aufklärung der Straftat stehen. Hat ein Zeuge bei früherer Vernehmung bereits von seinem gesetzlichen Zeugnis- oder Auskunftsverweigerungsrecht Gebrauch gemacht, so soll von Maßnahmen der öffentlichen Fahndung abgesehen werden.

4. In Unterbringungssachen darf eine öffentliche Fahndung mit Rücksicht auf den Grundsatz der Verhältnismäßigkeit nur unter angemessener Berücksichtigung des gesetzlichen Zwecks der freiheitsentziehenden Maßregel, insbesondere der Therapieaussichten und des Schutzes der Allgemeinheit angeordnet werden.

5. Die öffentliche Fahndung zur Sicherung der Strafvollstreckung sollte zur Voraussetzung haben, daß

   - eine Verurteilung wegen einer Straftat von erheblicher Bedeutung vorliegt und

   - der Verurteilte, der sich der Strafvollstreckung entzieht, (noch) eine Restfreiheitsstrafe von in der Regel mindestens einem Jahr zu verbüßen hat, oder ein besonderes öffentliches Interesse, etwa tatsächliche Anhaltspunkte für die Begehung weiterer Straftaten von erheblicher Bedeutung, an der alsbaldigen Ergreifung des Verurteilten besteht.

6. Besondere Zurückhaltung ist bei internationaler öffentlicher Fahndung geboten. Dies gilt

sowohl für Ersuchen deutscher Stellen um Fahndung im Ausland als auch für Fahndung auf Ersuchen ausländischer Stellen im Inland.

7. Öffentliche Fahndung unter Beteiligung der Medien sollte in den Katalog anderer entschädigungspflichtiger Strafverfolgungsmaßnahmen des § 2 Abs. 2 StrEG aufgenommen werden.

   Durch Ergänzung des § 7 StrEG sollte in solchen Fällen auch der immaterielle Schaden als entschädigungspflichtig anerkannt werden.

Der Gesetzgeber sollte vorsehen, daß auf Antrag des Betroffenen die Entscheidung über die Entschädigungspflicht öffentlich bekanntzumachen ist.

4. Anlage: Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996

Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen

Mit der Markteinführung des digitalen Fernsehens 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.

5. Anlage: Anlage zum Entwurf einer Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (vorgelegt vom Arbeitskreis Medien)

Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen

Grundsätzlich werden auch Pay-per-View-Programme - wie das traditionelle Abonnenten-Fernsehen - verschlüsselt übertragen. Der Kunde braucht einen Decoder, um die Programme empfangen zu können (die sog. Set-Top-Box). Die Sendesignale werden von dem Decoder nur entschlüsselt, wenn er "freigeschaltet" wurde. Die Freischaltung kann mit verschiedenen technischen Verfahren realisiert werden:

1. Zentrale Freischaltung aus dem Netz

Mit dem Sendesignal gekoppelt werden die Benutzernummern sämtlicher Kunden übertragen, die eine bestimmte Sendung sehen wollen. Der Decoder wird auf diese Weise aus dem Netz nur für die betreffende Sendung "freigeschaltet". Dieses Verfahren setzt voraus, daß die Kunden entweder telefonisch oder über einen Rückkanal beim Sender die Freischaltung für eine Sendung verlangen. Damit wird das vom Kunden gewünschte Programmangebot grundsätzlich zunächst registriert.

Zudem werden mit dem über Kabel oder Satellit verteilten Signal für die Sendung auch die Nutzernummern der Interessenten - unverschlüsselt - übertragen, deren Decoder freigeschaltet werden soll; sie könnten im gesamten Netz mit verhältnismäßig geringem Aufwand mitgelesen und ausgewertet werden. Im Unterschied zur periodischen Freischaltung von Decodern im Abonnenten-Fernsehen ist damit eine sendungsspezifische Registrierung des Nutzungsverhaltens möglich.

Nur durch zusätzliche organisatorische Maßnahmen - etwa die Einschaltung eines neutralen Dritten, der die Freischaltung im Auftrag des Anbieters übernimmt, jedoch keinen direkten Kundenkontakt hat - läßt sich bei diesem Verfahren eine direkt personenbezogene Speicherung des Nutzungsverhaltens vermeiden.

2. Lokale Freischaltung durch den Nutzer

Jede Sendung wird mit einer elektronischen Entgeltinformation (Token) versehen. Die Kunden, die das Programmangebot sehen wollen, teilen dies per Fernbedienung dem Decoder mit. Das Guthaben auf der Chipkarte, die in den Decoder eingeführt ist, wird entsprechend verringert und der Decoder lokal freigeschaltet.

Das Token-System läßt sich mit vorhandener Technik so gestalten, daß beim Anbieter keinerlei personenbezogene Informationen über die Inanspruchnahme einzelner Sendungen entstehen. Eine vollständig anonyme Nutzung kann insbesondere durch den Einsatz von Wertkarten realisiert werden. Selbst bei Einsatz personalisierter wiederaufladbarer Wertkarten besteht die Möglichkeit, daß lediglich der Ladevorgang (z. B. durch Einzahlung eines Guthabens an einem Automaten oder bei Aufladung aus dem Netz), nicht jedoch die einzelne Programmnutzung durch den Anbieter oder einen zwischengeschalteten Dritten registriert wird.

Allerdings besteht die Gefahr, daß auch bei Token-Verfahren auf der Chipkarte Informationen über die einzelnen Programmabrufe gespeichert und - per Rückkanal - an den Anbieter für Zwecke seiner Abrechnung mit Programmlieferanten übermittelt bzw. von diesem abgerufen werden.

Dem datenschutzrechtlichen Gebot, technische Verfahren so zu gestalten, daß möglichst wenige personenbezogene Daten entstehen und auch eine anonyme Nutzung gewährleistet ist, kann durch das Token-Verfahren bei Pay-per-View besser entsprochen werden als durch Verfahren mit individueller zentral gesteuerter Freischaltung. Eine anonyme Nutzung ist jedoch auch bei dem Token-Verfahren nur dann zu gewährleisten, wenn der Abruf der Daten über die einzelnen gesehenen Sendungen durch den Anbieter unterbleibt.

6. Anlage: Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996

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 Uberwachung des Fernmeldever kehrs erhalten eine neue Dimension; weil immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden, können sie mit geringem Aufwand kontrolliert und ausge wertet 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 Bedingun gen der Verwendung der modernen Informationstechnologien aufrechterhalten und gewährlei stet 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.

7. Anlage: Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996

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 Kassenzahnärztlichen 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.

8. Anlage: Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997

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 erkenaungsdienstlichen 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 aufgrund 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.

9. Anlage: Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997

Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen

Die Datenschntzbeauftragten 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 Forschungtätig 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 Datenschotzbeauftragten 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 entwikkelnden modernen Formen der Auslagerung medizinischer Patientendaten sowie für die Weitergabe medizinischer Patientendaten für Zwecke wissenschaftlicher medizinischer Forschung einen dem Arztgeheimnisentsprechenden Schutz der Patientendaten zu schaffen.

10. Anlage: Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997

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."

11. Anlage: Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997

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 techni-

schen 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.

12. Anlage: Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997

Geplante Verpflichtung von Teledienstean bietern, Kundendaten an Sicherheitsbehörden zu übermitteln

Der Entwurf der Bundesregierung für ein Teledienstedatenschutzgesetz (Artikel 2 -§ 5 Abs. 3- des Informations- und Kommunikationsdienste-Gesetzes vom 20. Dezember 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.

13. Anlage: Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997

Novellierung des Bundesdatenschutzgesetzes und Modernisierung des Datenschutzrechts

Die fristgerechte Harmonisierung des Datenschutzes entsprechend den Vorgaben der europäischen Datenschutzrichtlinie vom 24. Oktober 1995 droht zu scheitern. Die von dieser Richtlinie gesetzte Dreijahresfrist wird heute in einem Jahr ablaufen. Eine gründliche Beratung im Deutschen Bundestag wird durch den baldigen Ablauf der Legislaturperiode in Frage gestellt.

Noch immer gibt es keinen Kabinettsbeschluß; die Bundesregierung hat bisher noch nicht einmal einen abgestimmten Referentenentwurf vorgelegt. Sie gefährdet dadurch die rechtzeitige Umsetzung der Richtlinie und riskiert ein Vertragsverletzungsverfahren vor dem Europäischen Gerichtshof.

Für die Entwicklung des Datenschutzes ist diese Lage höchst nachteilig:

- Verbesserungen des Datenschutzes der Bürger, z. B. durch genauere Information über die Verarbeitung ihrer Daten, verzögern sich;

- dem Datenschutzrecht droht Zersplitterung, weil den Ländern eine Orientierung für die Anpassung der Landesdatenschutzgesetze fehlt.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an die Bundesregierung, für eine fristgerechte Umsetzung der Richtlinie Sorge zu tragen.

Zur Harmonisierung des europäischen Datenschutzrechts empfehlen die Datenschutzbeauftragten der Bundesregierung und dem Gesetzgeber folgende Grundsatzentscheidungen:

- weitgehende Gleichbehandlung des öffentlichen und des privaten Bereichs bei gleichzeitiger Verbesserung der Datenschutzkontrolle, insbesondere durch generell anlaßunabhängige Kontrolle und durch die ausdrückliche Festlegung der völligen Unabhängigkeit der Aufsichtsbehörden und die Erweiterung ihrer Eingriffsbefugnisse;

- Bestellung weisungsfreier Datenschutzbeauftragter auch bei öffentlichen Stellen mit dem Recht, sich jederzeit an den Bundes- oder Landesbeauftragten für den Datenschutz zu wenden;

- Bürgerfreundlichkeit durch einfache und verständliche Formulierung des BDSG, z. B. durch einen einheitlichen Begriff der Verarbeitung personenbezogener Daten entsprechend der Richtlinie;

- Gewährleistung eines einheitlichen, hohen Datenschutzniveaus durch Beibehaltung der Funktion des BDSG und der Landesdatenschutzgesetze als Querschnittsgesetze sowie durch Vermeidung eines Gefälles zwischen den Bereichen, die der EG-Datenschutzrichtlinie unterfallen, und den übrigen Gebieten, deren Datenschutzregelungen nicht verschlechtert werden dürfen

- Sonderregelungen für Presse und Rundfunk nur, soweit zur Sicherung der Meinungsfreiheit notwendig.

Als ebenso vordringlich betrachten die Datenschutzbeauftragten eine Anpassung der noch von der Großrechnertechnologie der siebziger Jahre bestimmten gesetzlichen Regelungen an die heutige Informationstechnologie und an die Verhältnisse der modernen Informationsgesellschaft. Dazu gehören insbesondere folgende Punkte:

- Verbindliche Grundsätze für die datenschutzfreundliche Gestaltung von Informationssystemen und -techniken, so zur Datensparsamkeit, zur Anonymisierung und Pseudonymisierung, zur Verschlüsselung und zur Risikoanalyse;

- mehr Transparenz für die Verbraucher und mehr Eigenständigkeit für die Anbieter durch Einführung eines Datenschutzaudits;

- Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen, Regelung der Videoüberwachung;

- Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren;

- Einführung einer Vorabkontrolle für besonders risikoreiche Datenverarbeitung, namentlich bei Verarbeitung sensitiver Daten;

- Regelungen für Chipkarten-Anwendungen;

- Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing, unter anderem auch mindestens durch die Festlegung von Hinweispflichten hinsichtlich der Möglichkeit des Widerspruchs; vorzuziehen ist in jedem Fall eine Einwilligungsregelung;

- Verstärkung des Schutzes gegenüber der Einholung von Selbstauskünften vor Abschluß vor Miet-, Arbeits- und ähnlich existenzwichtigen Verträgen;

- Datenexport nach Inlandsgrundsätzen nur bei angemessenem Schutzniveau im Empfängerstaat; Festlegung, unter welchen Voraussetzungen ein Mitgliedstaat Daten, die er im Anwendungsbereich der Richtlinie (also nach Inlandsgrundsätzen) erhalten hat, außerhalb ihres Anwendungsbereichs verwenden darf;

- möglichst weitgehende Ersetzung der Anmeldung von Dateien bei der Aufsichtsbehörde durch Bestellung weisungsfreier Datenschutzbeauftragter; Beibehaltung des internen Datenschutzbeauftragten auch bei Sicherheitsbehörden;

- Stärkung der Kontrollrechte des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz durch uneingeschränkte Kontrollbefugnis bei der Verarbeitung personenbezogener Daten in Akten einschließlich solcher über Sicherheitsüberprüfungen.

Die Konferenz weist ferner auf die Rechtspflicht der Länder hin, ihr Datenschutzrecht ebenfalls der EG-Richtlinie fristgerecht anzupassen.

14. Anlage: Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997

Informationelle Selbstbestimmung und Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren

Überlegungen des Gesetzgebers und eine beginnende öffentliche Diskussion, moderne Dokumentationstechnik der Wahrheitsfindung und dem Zeugenschutz in gerichtlichen Verfahren nutzbar zu machen, liegen auch im Interesse des Datenschutzes. Dabei ist allerdings zu beachten, daß Bild-Ton-Aufzeichnungen von Vernehmungen im Strafverfahren einen erheblichen Eingriff in das Persönlichkeitsrecht darstellen. Sie spiegeln die unmittelbare Betroffenheit der Beschuldigten oder Zeugen in Mimik und Gestik umfassend wider. Zweck und Erforderlichkeit dieses Eingriffs bedürfen einer sorgfältigen Begründung durch den Gesetzgeber. Sie bildet den Maßstab, der über Möglichkeiten, Grenzen und Verfahren der Videotechnologie im Strafprozeß entscheidet. Erkennbar und nachvollziehbar sollte sein, daß der Gesetzgeber die Risiken des Einsatzes dieser Technologie, insbesondere die Verfügbarkeit der Aufzeichnungen nach den allgemeinen Vorschriften über die Beweisaufnahme bedacht und bewertet hat. Ferner sollte erkennbar und nachvollziehbar sein, daß Alternativen zur Videotechnologie, namentlich die Verwendung von Tonaufzeichnungen, in die Erwägungen des Gesetzgebers aufgenommen wurden.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sollten die vorliegenden Gesetzesentwürfe des Bundesrates (BT-Drs. 13/4983 vom 19.06.1996) sowie der Fraktionen der CDU/CSU und F.D.P. (BT-Drs. 13/7165 vom 11.03.1997) in einem umfassenderen Bedeutungs- und Funktionszusammenhang diskutiert werden. Zunehmend tritt das Anliegen der Praxis hervor, Bild-Ton-Aufzeichnungen auch mit anderer Zielsetzung zu verwerten:

Bild-Ton-Aufzeichnungen ermöglichen eine vollständige und authentische Dokumentation nicht nur des Inhalts, sondern auch der Entstehung und Begleitumstände einer Aussage. Die Beurteilung ihres Beweiswerts wird dadurch deutlich verbessert. Zugleich dient eine nur einalige Vernehmung, die möglichst zeitnah zum Tatgeschehen durchgeführt und aufzeichnet wird, der Wahrheitsfindung und erhöht die Qualität der gerichtsverwertbaren Daten („Vermeidung kognitiver Dissonanzen“). Ausgehend von diesen Überlegungen, hat der Gesetzgeber unter

Einbeziehung von Erkenntnissen der Vernehmungspsychologie zu prüfen, ob und inwieweit eine wortgetreue Abfassung von Vernehmungsniederschriften ausreicht und eine Aufzeichnung der Aussage nur im Wort auf Tonband für die Zwecke des Strafverfahrens in ihrer Beweisqualität der Videotechnologie sogar überlegen ist.

Für Videoaufzeichnungen des Betroffenen, die zu seinem Schutz gefertigt werden sollen, ist dessen Einwilligung unverzichtbare Voraussetzung für die Zulässigkeit einer Bild-Ton-Aufzeichnung im Strafverfahren. Sofern der Betroffene nicht in der Lage ist, die Bedeutung und Tragweite einer Bild-Ton-Aufzeichnung und ihrer Verwendungsmöglichkeiten hinreichend zu beurteilen, hat der Gesetzgeber festzulegen, wer anstelle des Betroffenen die Einwilligung erteilen darf. Vor Abgabe der Einwilligungserklärung ist der Betroffene umfassend aufzuklären, insbesondere auch über alle zulässigen Arten der weiteren Verwertung und über die Möglichkeit des Widerrufs der Einwilligung für die Zukunft. Die Aufklärung ist zuverlässig zu dokumentieren. Entsprechendes gilt für die Herausgabe von Videoaufzeichnungen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern wirksame Vorkehrungen zum Schutz des Persönlichkeitsrechts bei Bild-Ton-Aufzeichnungen im Strafverfahren. Unabhängig von der Frage welche Ziesetzung mit Bild-Ton-Aufzeichnungen im Strafverfahren verfolgt werden soll, sind hierbei insbesondere folgende Gesichtspunkte von Bedeutung:

1. Es ist sicherzustellen, daß der Eindruck des Aussagegeschehens z.B. durch Zeitlupe, Zeitraffer, Einzelbildabfolge, Standbild und Zoom nicht gezielt verfremdet oder verzerrt wird.

2. Einsatz und Verwertung von Bild-Ton-Aufzeichnungen sind so zu regeln, daß gesetzliche Zeugnisverweigerungsrechte gewahrt bleiben. Insbesondere ist eine weitere Nutzung der Aufnahme, auch zum Zwecke des Vorhalts, ausgeschlossen, wenn sich ein Zeuge auf sein Zeugnisverweigerungsrecht beruft.

3. Vorbehaltlich des o. g. Einwilligungserfordernisses darf eine Übermittlung von Videoaufzeichnungen an Stellen außerhalb der Justiz, wenn überhaupt, nur in Ausnahmefällen erlaubt sein, da nur so ein wirksamer Schutz vor Mißbrauch, etwa durch kommerzielle Verwertung, gewährleistet werden kann. Soweit der Gesetzgeber aus Gründen eines fai-

ren, rechtsstaatlichen Strafverfahrens die Weitergabe von Videokopien an Verfahrensbeteiligte zuläßt, müssen jedenfalls wirksame Vorkehrungen gegen Mißbrauch gewährleistet sein, z.B. sichtbare Signierung und strafbewehrte Regelungen über Zweckbindungen und Löschungsfristen.

4. Eine Verwertung der Aufzeichnungen im Rahmen eines anderen Strafverfahrens ist nur zulässig, soweit sie auch für die Zwecke dieses anderen Verfahrens hätten angefertigt werden dürfen.

5. Soweit eine Verwertung in einem anderen gerichtlichen Verfahren - etwa zur Vermeidung erneuter Anhörung kindlicher Zeugen vor dem Familien- oder Vormundschaftsgericht - zugelassen werden sollte, sind in entsprechenden Ausnahmeregelungen präzise Voraussetzungen hierfür abschließend zu bestimmen und enge Verwendungsregelungen zu treffen.

6. Spätestens mit dem rechtskräftigen Abschluß des Strafverfahrens sind grundsätzlich die Aufzeichnungen unter Aufsicht der Staatsanwaltschaft zu vernichten. Der Betroffene ist davon zu benachrichtigen. Soweit der Gesetzgeber ausnahmsweise zur Wahrung vorrangiger Rechtsgüter eine längere Aufbewahrung der Aufzeichnungen zuläßt, müssen Voraussetzungen, Umfang und Fristen der weiteren Aufbewahrung klar und eng geregelt werden.

15. Anlage: Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997

Erforderlichkeit datenschutzfreundlicher Technologien

Moderne Informations- und Telekommunikationstechnik (IuK-Technik) gewinnt in allen Lebensbereichen zunehmende Bedeutung. Die Nutzer wenden diese Technik z. B. in Computernetzen, Chipkartensystemen oder elektronischen Medien in vielfältiger Weise an und hinterlassen dabei zumeist umfangreiche elektronische Spuren. Dabei fällt in der Regel eine Fülle von Einzeldaten an, die geeignet sind, persönliche Verhaltensprofile zu bilden.

Den Erfordernissen des Datenschutzes wird nicht in ausreichendem Maße Rechnung getragen, wenn sich der Schutz der Privatheit des einzelnen lediglich auf eine Beschränkung des Zugangs zu bereits erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten reduziert. Daher ist es erforderlich, bereits vor der Erhebung und Speicherung die zu speichernde Datenmenge wesentlich zu reduzieren.

Datensparsamkeit bis hin zur Datenvermeidung, z. B. durch Nutzung von Anonymisierung und Pseudonymisierung personenbezogener Daten, spielen in den unterschiedlichen Anwendungsbereichen der IuK-Technik, wie elektronischen Zahlungsverfahren, Gesundheits- oder Verkehrswesen, bisher noch eine untergeordnete Rolle. Eine datenschutzfreundliche Technologie läßt sich aber nur dann wirksam realisieren, wenn das Bemühen um Datensparsamkeit die Entwicklung und den Betrieb von IuK-Systemen ebenso stark beeinflußt wie die Forderung nach Datensicherheit.

Die Datenschutzbeauftragten des Bundes und der Länder wollen in Zusammenarbeit mit Herstellern und Anbietern auf datenschutzgerechte Lösungen hinarbeiten. Die dafür erforderlichen Techniken stehen weitgehend schon zur Verfügung. Moderne kryptographische Verfahren zur Verschlüsselung und Signatur ermöglichen die Anonymisierung oder Pseudonymisierung in vielen Fällen, ohne daß die Verbindlichkeit und Ordnungsmäßigkeit der Datenverarbeitung beeinträchtigt werden. Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff "Privacy enhancing technology (PET)" eine Philosophie der Datensparsamkeit beschreibt und ein ganzes System technischer Maßnahmen umfaßt, sollten genutzt werden.

Vom Gesetzgeber erwarten die Datenschutzbeauftragten des Bundes und der Länder, daß er die Verwendung datenschutzfreundlicher Technologien durch Schaffung rechtlicher Rahmenbedingungen forciert. Sie begrüßen, daß sowohl der Mediendienste-Staatsvertrag der Länder als auch das Teledienstedatenschutzgesetz des Bundes bereits den Grundsatz der Datenvermeidung normieren. Der in den Datenschutzgesetzen des Bundes und der Länder festgeschriebene Grundsatz der Erforderlichkeit läßt sich in Zukunft insbesondere durch Berücksichtigung des Prinzips der Datensparsamkeit und der Verpflichtung zur Bereitstellung anonymer Nutzungsformen verwirklichen. Die Datenschutzbeauftragten des Bundes und der Länder bitten darüber hinaus die Bundesregierung, sich im europäischen Bereich dafür einzusetzen, daß die Förderung datenschutzfreundlicher Technologien entsprechend dem Vorschlag der Kommission in das 5. Rahmenprogramm "Forschung und Entwicklung" aufgenommen wird.

Neben Anbietern von Tele- und Mediendiensten sollten auch die Hersteller und Anbieter von IuK-Technik bei der Ausgestaltung und Auswahl technischer Einrichtungen dafür gewonnen werden, sich am Grundsatz der Datenvermeidung zu orientieren und auf eine konsequente Minimierung gespeicherter personenbezogener Daten achten.

16. Anlage: Erklärung der Datenschutzbeauftragten von Bund und Ländern zur Ausschreibung des Bundesinnenministers für eine Machbarkeitsstudie einer Asylcard

Die Zusammenführung von Daten aus dem Arbeitsbereich verschiedener Stellen auf einer solchen Asylchipkarte stellt wegen der damit verbundenen Rundumerfassung einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht dar, das auch für Asylbewerber gilt. Die Datenschutzbeauftragten halten einen solchen Eingriff nicht für vertretbar, zumal die Überlegungen zur ASYL-Card durch Mängel im Vollzug des bisherigen Verfahrens ausgelöst werden. Die Datenschutzbeauftragten sind der Ansicht, daß diese Defizite behoben werden sollten, anstatt ein neues, datenschutzrechtlich problematisches Verfahren einzuführen.

Die Datenschutzbeauftragten weisen auf die Gefahr hin, daß durch ein Ergebnis einer solchen Machbarkeitsstudie Fakten geschaffen werden, die eine Diskussion in der Öffentlichkeit und die Entscheidung in den Parlamenten von Bund und Ländern vorwegnehmen. Bezeichnend ist in diesem Zusammenhang, daß die Machbarkeitsstudie auch aufzeigen soll, ob und welche Änderungen der Rechtslage, insbesonders der Datenschutzgesetze, für eine Realisierung der Vorschläge erforderlich sind. Die Datenschutzbeauftragten sehen darin eine Tendenz, daß nicht Vorschläge an die Rechtslage, sondern umgekehrt die - letztlich auf den Grundrechten beruhende - Rechtslage den Vorschlägen angepaßt werden soll. Die Datenschutzbeauftragten halten diese Tendenz für gefährlich.

Die Datenschutzbeauftragten weisen aus diesem Anlaß auf die allgemeine Problematik einer Entwicklung zur multifunktionellen Datenspeicherung auf Chipkarten für Überwachungszwekke hin, die durch die Einführung einer solchen Asylcard ausgelöst werden kann. Effektivitätsgesichtspunkte, Mißbrauchsbekämpfung, Überwachung auferlegter Pflichten u. ä. könnten auch für andere Verwaltungsverfahren geltend gemacht werden. Je mehr Bereiche mit Kartenlösungen versehen werden, umso mehr wächst das Bedürfnis, aus praktischen Erwägungen heraus eine Vereinheitlichung oder Zusammenführung der Informationen auf einer Karte anzustreben. Damit wächst die Gefahr der "Rundumerfassung", die mit dem verfassungsrechtlichen Gebot der Verhältnismäßigkeit nicht vereinbar wäre.

Die Einführung der "ASYL-Card" bedürfte im übrigen eines erheblichen technischen und finanziellen Aufwands. Kryptographische Verfahren, Hard- und Software für die mit der ASYL-Card arbeitenden Stellen und Personal- und Arbeitseinsatz für die Herstellung, Verteilung und Verwaltung der Karten würden einen Aufwand erfordern, der zu den von der Arbeitsgruppe erwarteten Vorteilen außer Verhältnis stehen dürfte.

Umso größer ist die Gefahr, daß eine derartige Infrastruktur dann auch für andere Bereiche nutzbar gemacht werden soll. Die Datenschutzbeauftragten halten deshalb eine solche Asylcard für einen gefährlichen Schritt auf dem Weg zu einem rundum erfaßten Bürger.

München, den 17.06.1997

Reinhard Vetter
Derz. Vorsitzender der Konferenz der Datenschutzbeauftragten von Bund und Ländern

17. Anlage: 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 zusammengeführtwird. 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 aufgrund 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, Multimediäinrichtungen 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 Rechts-

ordnung 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 aufgrund 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. Oktober 1995 einen verantwortlichen inländischen Vertreter zu benennen.

18. Anlage: 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. § 78 a 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 technischen Möglichkeiten fordern die Datenschutzbeauftragten des Bundes und der Länder, geeignete, sichere kryptographische Verfahren beim Transport elektronisch gespeicherter personenbezogener Daten unter Berücksichtigung ihrer Schutzwürdigkeit anzuwenden.

19. Anlage: Pressemitteilung des Vorsitzenden der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. Dezember 1996

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 Parameterspeicher).

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.
4. 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.

5. Telefaxgeräte sollten nur auf der Grundlage schriftlicher Dienstanweisungen eingesetzt werden. Die Bedienung darf nur durch eingewiesenes Personal erfolgen.

6. Das Telefaxgerät ist so aufzustellen, daß Unbefugte keine Kenntnis vom Inhalt eingehender oder übertragener Schreiben erhalten können.

7. Alle vom Gerät angebotenen Sicherheitsmaßnahmen (z. B. Anzeige der störungsfreien Übertragung, gesicherte Zwischenspeicherung, Abruf nach Paßwort, Fernwartungsmöglichkeit sperren) sollten genutzt werden.

8. Die vom Gerät auf der Gegenseite vor dem eigentlichen Sendevorgang abgegebene Kennung ist sofort zu überprüfen, damit bei eventuellen Wählfehlern die Übertragung unverzüglich abgebrochen werden kann.

9. 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.

10. Die Dokumentationspflichten müssen eingehalten werden (z. B. Vorblatt oder entsprechend aussagekräftige Aufkleber verwenden, Zahl der Seiten angeben, Protokolle aufbewahren). Sende- und Empfangsprotokolle sind vertraulich abzulegen, da sie dem Fernmeldegeheimnis unterliegen.

11. Vor Verkauf, Weitergabe oder Aussortieren von Telefaxgeräten ist zu beachten, daß alle im Gerät gespeicherten Daten (Textinhalte, Verbindungsdaten, Kurzwahlziele usw.) gelöscht werden.

12. Die am Telefaxgerät eingestellten technischen Parameter und Speicherinhalte sind regelmäßig zu überprüfen, damit beispielsweise Manipulationsversuche frühzeitig erkannt und verhindert werden können.

13. Verfügt das Telefaxgerät über eine Fernwartungsfunktion, sollte sie grundsätzlich durch den Nutzer deaktiviert werden. Nur für notwendige Wartungsarbeiten ist diese Funktionen 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 Einplatzrechner 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 Zugriffes 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.

Schon bei der Beschaffung integrierter Telefaxlösungen sollte darauf geachtet werden, daß ausreichende Konfigurationsmöglichkeiten vorhanden sind, um die dringend notwendige Anpassung an die datenschutzrechlichen Erfordernisse des Nutzers zu gewährleisten.

8 Abkürzungsverzeichnis

AK Technik	Arbeitskreis "Technische und organisatorische Datenschutzfragen"
AO	Abgabenordnung
AuslG	Ausländergesetz
AZR	Ausländerzentralregister
BAföG	Bundesausbildungsförderungsgesetz
BAT	Bundesangestelltentarifvertrag
BAT-O	Bundesangestelltentarifvertrag - Ost
BauGB	Baugesetzbuch
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Datenschutz
BGB	Bürgerliches Gesetzbuch
BMF	Bundesministerium der Finanzen
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BR-Drs.	Bundesrats-Drucksache
BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStU	Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes
BT-Drs.	Bundestags-Drucksache
BVerfGE	Entscheidungen des Bundesvefassungsgerichts Band ..., Seite ...
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz

CDLS	Chipkartenbasiertes Dienstleistungssystem
DSG MV	Landesdatenschutzgesetz von Mecklenburg-Vorpommern
DVZ M-V GmbH	Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
EU	Europäischen Union
FAG	Fernmeldeanlagengesetz
GG	Grundgesetz
GGO I M-V	Gemeinsame Geschäftsordnung der Ministerien des Landes Mecklenburg-Vorpommern
GSM	Global System for Mobile Communication
HKR	Haushalts-, Kassen- und Rechnungswesen
HVerfG	Hamburgisches Verfassungsgericht
IMA IT	Interministeriellen Ausschuß für Informations- und Telekommunikationstechnik
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
IngG M-V	Ingenieurgesetz Mecklenburg-Vorpommern
ISDN	Diensteintegrierendes digitales Telekommunikationsnetz
IT	Informationstechnik
IuK-Dienste	Informations- und Kommunikationsdienste
IuK-Technik	Informations- und Kommunikationstechnik
IuKDG	Informations- und Kommunikationsdienste-Gesetz
KitaG	Gesetz zur Förderung von Kindern in Tageseinrichtung und Tagespflege
Koop IT	Kooperationsausschuß IT
KV	Kassenärztliche Vereinigung
KV MV	Kommunalverfassung für das Land Mecklenburg-Vorpommern
LAPIS	Landesweites Polizei-Informationssystem

LBG M-V	Landesbeamtengesetz Mecklenburg-Vorpommern
LDSG	Landesdatenschutzgesetz
LHO	Landeshaushaltsordnung
LKHG M-V	Landeskrankenhausgesetz Mecklenburg-Vorpommern
LKSt	Koordinierungs- und Beratungsstelle der Landesregierung für IT in der Landesregierung
LVA	Landesversicherungsanstalt
LVerfSchG	Landesverfassungsschutzgesetz
MAC	Media Access Control
MDK	Medizinischer Dienst der Krankenversicherung
MDStV	Mediendienste-Staatsvertrag
NADIS	Nachrichtendienstliches Informationssystem
OFD	Oberfinanzdirektion
OWiG	Ordnungswidrigkeitengesetz
PED MV	Polizeilichen Erkenntnis Datei Mecklenburg-Vorpommern
PERSYS	Personal- und Stellenverwaltungssystem
PET	Privacy enhancing technology
PODS	Personal- und Organisationsdatensystem
PsychKG	Gesetz über Hilfen und Schutzmaßnahmen für psychisch Kranke
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
RStV	Rundfunkstaatsvertrag
RTF	Rich Text Format
SchulG M-V	Schulgesetz Mecklenburg-Vorpommern
SGB V	Sozialgesetzbuch Fünftes Buch
SGB VIII	Sozialgesetzbuch Achtes Buch
SGB X	Sozialgesetzbuch Zehntes Buch

SigG	Gesetz zur digitalen Signatur
SigV	Signaturverordnung
SNMP	Simple Network Management Protocol
SOG MV	Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern
StGB	Srafgesetzbuch
StPO	Strafprozeßordnung
StUG	Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik
StVÄG	Strafverfahrensänderungsgesetz
StVÄG-E	Entwurf des Strafverfahrensänderungsgesetzes
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikationsdienstunternehmen-Datenschutzverordnung
TK	Telekommunikation
TKG	Telekommunikationsgesetz
UDSV	Teledienstunternehmen-Datenschutzverordnung
WWW	World Wide Web

9 Stichwortverzeichnis

A

B

C

D

E

H

I

J

K

L

M

N

S

T

W

X

Z

10 Publikationen

BEIM LANDESBEAUFTRAGTEN FÜR DEN DATENSCHUTZ SIND DERZEIT FOLGENDE PUBLIKATIONEN KOSTENLOS ERHÄLTLICH

Der Landesbeauftragte für den Datenschutz *(Faltblatt mit allgemeinen Informationen)*

Datenschutz geht jeden an *(Faltblatt des Innenministers MV)*

Gesetze und Verordnungen zum Datenschutz *(Loseblattsammlung)*

Technik und Datenschutz *(Arbeitsergebnisse und Tagungsunterlagen des Arbeitskreises Technik in Broschürenform)*

Informationen zum Datenschutz *(Faltblätter mit aktuellen Informationen)*

Faltblatt Nr.

2. Datenschutz und Personalcomputer
4. Patientenakte
5. Datenschutz und Verfassungsschutz
6. Datenschutz und Personen-Identifikation
7. Datenschutz und Telefax
9. Datenmißbrauch
12. Das ISDN-Netz
13. Freiwillige Patienten-Chipkarten
15. Umgang mit Sozialdaten
16. Personenbezogene Daten in der Forschung
17. Technikfolgenabschätzung
18. Sicherheit der Informationstechnik
19. Personalakten und Personalaktendaten
20. Statistische Erhebungen

Tätigkeitsberichte *(in Broschürenform)*

1. Tätigkeitsbericht für den Zeitraum 1992/93
2. Tätigkeitsbericht für den Zeitraum 1994/95
3. Tätigkeitsbericht für den Zeitraum 1996/97

Informationen des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz *(in Broschürenform)*

BfD - INFO 1 - Bundesdatenschutzgesetz
BfD - INFO 2 - Der Bürger und seine Daten

BfD - INFO 3 - Schutz der Sozialdaten
Datenschutz in der Arztpraxis (*Broschüre des Hamburger DSB in Kopie)*

Handreichungen*(in Form von Kopien)*

Hinweise zu den Aufgaben eines internen Datenschutzbeauftragten öffentlicher Stellen
Orientierungshilfe „Forderung an Wartung und Fernwartung von DV-Anlagen“
Hinweise zur Führung von Dateibeschreibung und Geräteverzeichnis
Organisationshilfe zur Vernichtung von Schriftgut
Orientierungshilfe „Datenschutzrechtliche Protokollierung beim Betrieb informations-technischer Systeme (IT-Systeme)“
Orientierungshilfe „Datenschutzrechtliche Aspekte beim Einsatz optischer Datenspeicherung“
Orientierungshilfe „Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“
Orientierungshilfe „Anforderungen zur informationstechnischen Sicherheit bei Chipkarten“