LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 1/3950**
1. Wahlperiode **06.01.94**

UNTERRICHTUNG

durch den Landesbeauftragten für den Datenschutz

Erster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz gemäß § 29 Abs. 1 des Landesdatenschutzgesetzes von Mecklenburg-Vorpommern (DSG MV)

Zugeleitet mit Schreiben des Landesbeauftragten für den Datenschutz vom 05. Januar 1994 gemäß § 29 Abs. 1 des Landesdatenschutzgesetzes

Vorwort

Das Landesdatenschutzgesetz von Mecklenburg-Vorpommern sieht vor, daß der Landesbeauftragte für den Datenschutz für jeweils zwei Kalenderjahre einen Tätigkeitsbericht verfaßt. Der vorliegende 1. Tätigkeitsbericht umfaßt die Zeit vom 09. September 1992, meinem Amtsantritt, bis zum 31. Dezember 1993.

Ich hoffe, daß es mir durch die Auswahl der einzelnen Vorgänge gelungen ist, einen zumindest repräsentativen Einblick in die breit gefächerte Tätigkeit meiner Mitarbeiter und meine eigene Tätigkeit zu geben. Einige Vorgänge habe ich, selbst wenn sie datenschutzrechtlich nicht von besonderer Bedeutung scheinen, allein deshalb in diesen Bericht mit aufgenommen, weil ich sie für geeignet halte, die Grundsätze des Datenschutzes und meine eigene Auffassung am konkreten Beispiel deutlich zu machen.

Bedanken möchte ich mich an dieser Stelle für die fachliche Unterstützung, die mir meine Kollegen aus den anderen Ländern gewährt haben. Insbesondere denke ich dabei an Herrn Dr. Bäumler, den Landesbeauftragten für den Datenschutz in Schleswig-Holstein und den Berliner Datenschutzbeauftragten, Herrn Dr. Garstka. Und ich danke Herrn Ernst Eugen Becker, dem ehemaligen Datenschutzbeauftragten von Schleswig-Holstein, der mir als erster Mut gemacht hat, diese für mich neue und nicht ganz leichte Aufgabe zu übernehmen.

Dr. Werner Kessel
Landesbeauftragter für den Datenschutz
Mecklenburg-Vorpommern

1. Einleitung

In der DDR gab es eine recht eigenwillige Form von Datenschutz. Ein ganzes Ministerium war fleißig damit beschäftigt, möglichst viele personenbezogene Daten über die Bürger zu sammeln, um dann vor ihnen geheim zu halten, was gespeichert wurde. Die ungebremste Datensammelwut des Ministeriums für Staatssicherheit hat bei vielen betroffenen Bürgern großen psychischen, physischen und materiellen Schaden angerichtet. Deshalb halte ich das Recht auf informationelle Selbstbestimmungfür eines der bedeutendsten Bestandteile unserer neu gewonnenen Freiheit.

Das Recht auf informationelle Selbstbestimmung beinhaltet die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Dieses Recht wird aus Art. 2 Abs. 1 (Recht auf freie Entfaltung der Persönlichkeit) i.V.m. Art. 1 Abs. 1 (Unantastbarkeit der Menschenwürde) Grundgesetz (GG) hergeleitet. Das Volkszählungsurteil vom 15.12.1983 (BVerfGE 65, 1) hat das informationelle Selbstbestimmungsrecht in den Rang eines Grundrechtes erhoben. Wesentlicher Faktor für die Ausübung des Rechts auf informationelle Selbstbestimmung ist das Wissen des einzelnen, was bei welchen Stellen in welchem Umfang über ihn gespeichert ist. Erst wenn dieses Wissen vorhanden ist, kann das Recht in der Praxis ausgeübt werden. So hat schon das Bundesverfassungsgericht in seinem Volkszählungsurteil hervorgehoben:

"Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen und zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.
Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des einzelnen beeinträchtigen, sondern auch das Allgemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.
Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insofern die Befugnis des einzelnen, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen" (aus dem Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz, BVerfGE 65, 43).

Es wäre jedoch verfehlt, Datenschutz als ein Recht des einzelnen auf absolute Herrschaft über seine Daten zu interpretieren. Ziel informationeller Selbstbestimmung ist es nicht, Kommunikationslosigkeit herzustellen, sondern die für eine demokratische Gesellschaft unerläßliche Kommunikation zu ermöglichen, indem sie einen Umgang mit personenbezogenen Daten ohne Beteiligung des Betroffenen verhindert und damit dessen Handlungsfähigkeit sichert.
In diesem Spannungsfeld zwischen den Rechten des einzelnen und denen der Allgemeinheit nehmen die Datenschutzgesetze eine Mittlerrolle ein. Sie enthalten die Grundsätze zur Wahrung des informationellen Selbstbestimmungsrechtes. Beschränkungen dieses Rechtes bedürfen einer (verfassungsmäßigen) bereichsspezifischen gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang klar und für den Bürger erkennbar ergeben müssen. Der Grundsatz der Verhältnismäßigkeit ist dabei in jedem Fall zu beachten.

Mit dem Einigungsvertrag gilt seit dem 3. Oktober 1990 auch in allen neuen Bundesländern das Grundgesetz der Bundesrepublik Deutschland und somit auch das festgeschriebene Recht auf informationelle Selbstbestimmung. In Art. 8 i.V.m. Anlage 1, Kap. II, Sachgebiet C, Abs. III, Nr. 3 enthält der Einigungsvertrag bereits konkrete Regelungen zum Datenschutz. So verpflichtete er beispielsweise den Bundesbeauftragten für den Datenschutz (BfD) als Kontrollinstanz für alle neuen Bundesländer bis zur Schaffung einer landeseigenen Datenschutzkontrolle.
Als gesetzliche Grundlage in den neuen Ländern trat zunächst das Bundesdatenschutzgesetz (BDSG) in der Fassung von 1977 in Kraft. Am 20. 12. 1990 wurde es durch das neue Bundesdatenschutzgesetz ersetzt. Seine Gültigkeit beschränkte sich hier jedoch nicht nur auf die öffentlichen Stellen des Bundes und die nicht-öffentlichen Stellen des Landes. Solange in den neuen Ländern noch keine eigenen Datenschutzgesetze existierten, galten die Regeln des Bundesdatenschutzgesetzes auch für die öffentlichen Stellen dieser Länder.
In Mecklenburg-Vorpommern ist das Gesetz zum Schutz des Bürgers beim Umgang mit seinen Daten (Landesdatenschutzgesetz von Mecklenburg-Vorpommern - DSG MV) am 15. August 1992 in Kraft getreten. Es reiht sich in die Systematik der Datenschutzgesetzgebung der anderen Länder und des Bundes ein. Ausgewertet wurden insbesondere die folgenden Landesdatenschutzgesetze (LDSG):

- DSG Hessen
  in der Fassung vom 11.11.1986 (GVBl. S. 309) geändert durch Gesetz vom 21.12.1988 (GVBl. S. 424)
- Berliner DSG (Bln. DSG)
  in der Fassung vom 17.12.1990 (GVBl. 1991, S. 16, 54) zuletzt geändert durch Gesetz vom 26.01.1993 (GVBl. 1993, S. 40)
- DSG Nordrhein-Westfalen
  in der Fassung vom 15.03.1988 (GVBl. S. 160)
- Regierungsentwurf des DSG von Schleswig-Holstein
  in der Fassung vom 30.10.1991 (GVBl. S. 555)

und das BDSG in der Fassung vom 20.12.1990 (BGBl. I S. 2954)

Es bestehen jedoch einige Besonderheiten zu den Datenschutzgesetzen anderer Länder:

- Eine Verpflichtung des Landesbeauftragten für den Datenschutz, ein Dateienregister zu führen und vorzuhalten, wurde nicht in den Gesetzentwurf mit aufgenommen. Dies geschah aus dem Gesichtspunkt, daß der damit verbundene Verwaltungsaufwand in keinem Verhältnis zu dem Zweck steht, den Umgang mit Daten durch die öffentlichen Stellen transparenter zu machen. Unabhängig davon hat jedoch jeder Bürger grundsätzlich das Recht, bei den öffentlichen Stellen des Landes Auskunft zu den über ihn gespeicherten Daten zu erhalten. Wenn die Auskunftserteilung in bestimmten Fällen unterbleibt, z.B. wenn die Auskunft die öffentliche Sicherheit oder Ordnung gefährden könnte oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde, so ist sie - wenn der Betroffene es wünscht - in jedem Fall dem Landesbeauftragten für den Datenschutz (LfD) zu erteilen.

- Die Vorschriften über die Pflicht zur Benachrichtigung Betroffener (§ 19 DSG MV) und deren Recht auf Sperrung von Daten bis zur Klärung von Schadensersatzansprüchen (§ 21 Abs. 2 DSG MV) gehen dafür über den Regelungsgehalt der Datenschutzgesetze anderer Länder und des Bundes hinaus.

Es ist von Vorteil, daß sich das DSG MV bis auf den Abschnitt IV, der die Regelungen zum Landesbeauftragten enthält, und bis auf eine Besonderheit im Begriffssystem stark an andere Landesdatenschutzgesetze und an das neue Bundesdatenschutzgesetz vom 20.12.1990 anlehnt.

Die Besonderheit besteht in der Verwendung des Begriffes "Umgang mit Daten". Dieser Begriff umfaßt die "Erhebung", "Verarbeitung" und "Nutzung" und ist so in § 3 Abs. 4 DSG MV eindeutig definiert.

Das DSG MV ist ein sogenanntes "Auffanggesetz"; seine Vorschriften kommen immer dann zur Anwendung, wenn und soweit der Umgang mit personenbezogenen Daten nicht durch spezielle bereichsspezifische Rechtsvorschriften, die ihrerseits dem verfassungsrechtlichen Gebot der Verhältnismäßigkeit entsprechen müssen, normenklar geregelt ist. Jeder darüber hinaus gehende Umgang mit personenbezogenen Daten ist unzulässig, es sei denn, der Betroffene hat dazu seine Einwilligung gegeben. Die Einwilligung des Betroffenen wiederum setzt dessen Kenntnis über den Zweck des beabsichtigten Umgangs mit den Daten voraus. Beispiele für bereichsspezifische Gesetze mit datenschutzrechtlichen Regelungen sind das Sicherheits- und Ordnungsgesetz (SOG MV), das Landesmeldegesetz (LMG), das Landesverfassungsschutzgesetz (LVerfSchG) und das Landeskrankenhausgesetz (LKHG).

Bei der Verabschiedung bereichsspezifischer datenschutzrechtlicher Vorschriften sind prinzipiell folgende Punkte zu beachten:

- Nur das erforderliche Minimum an Daten darf verlangt werden.
- Die Daten dürfen grundsätzlich nur für den Zweck verwendet werden, für den sie erhoben wurden.
- Der Gesetzgeber muß dafür sorgen, daß auch bei der Organisation und beim Verfahren des Umgangs mit personenbezogenen Daten auf die Rechte des einzelnen Rücksicht genommen wird.

Für die Überwachung dieser Grundprinzipien wurden eigene Kontrollorgane geschaffen: Der Bundesbeauftragte und die Landesbeauftragten für den Datenschutz für den öffentlichen Bereich. Für den privaten Bereich ist das Innenministerium unseres Landes die Aufsichtsbehörde. Zu beachten ist, daß das DSG MV nur für öffentliche Stellen des Landes gilt. Das sind die Ministerien und die ihnen nachgeordneten Behörden, die Behörden des Kommunalbereiches, aber auch die der Aufsicht des Landes unterstehenden öffentlich-rechtlichen Einrichtungen mit eigener Rechtspersönlichkeit wie Universitäten, Hochschulen, Krankenkassen und Kammern. Für den nicht-öffentlichen Bereich, wie z. B. Handel, Banken, Versicherungen und private Betriebe, findet das Bundesdatenschutzgesetz Anwendung.

Seit dem 09.09.1992 gibt es auch in Mecklenburg-Vorpommern einen Landesbeauftragten für den Datenschutz. An diesem Tag habe ich die Aufgabe übernommen, die Einhaltung des Landesdatenschutzgesetzes und anderer bereichsspezifischer Datenschutzregeln in den öffentlichen Stellen unseres Landes zu kontrollieren.

Zu meinem Aufgabenfeld gehören außerdem die:

- Bearbeitung von Eingaben aus der Bevölkerung
- Auskunftserteilung zu Fragen hinsichtlich automatisierter Datenverarbeitungssysteme
- Beobachtung neuer Datenverarbeitungsprojekte
- Ausarbeitung von Empfehlungen für den Datenschutz
- Stellungnahme zu Gesetzen
- Erarbeitung von Gutachten.

In der Ausübung meines Amtes bin ich nur dem Gesetz unterworfen, unterstehe der Dienstaufsicht des Landtagspräsidenten und kann mich jederzeit an den Landtag wenden.

Soweit ich es aus meiner bisherigen praktischen Tätigkeit beurteilen kann, ist das DSG MV eine gut zu handhabende gesetzliche Regelung für den Umgang mit personenbezogenen Daten der Bürger in den öffentlichen Stellen unseres Landes. Gravierende Mängel im Gesetzestext konnte ich bei meiner bisherigen Arbeit nicht feststellen. In einigen konkreten Fällen zeichnete es sich jedoch bereits ab, daß im Rahmen einer Novellierung Veränderungen und Ergänzungen zu empfehlen sein werden. Am Ende dieses Berichtes werde ich näher hierauf eingehen.

2. Sorgen der Bürger, Vorkommnisse, Beratungen, Kontrollen, Stellungnahmen

2.1 Allgemeines zum Umgang mit Petitionen

Im Datenschutz haben die Sorgen des einzelnen Bürgers Priorität. Deshalb stelle ich den Berichten über konkrete Sachverhalte einige allgemeine Bemerkungen über den Umgang mit Petitionen voran. Ungeachtet ihrer Allgemeinheit erscheinen mir aber auch diese Hinweise am ehesten am konkreten Beispiel verständlich. Ich wähle hierfür ein Beispiel, das kurz nach meiner Amtsübernahme den Anlaß lieferte, über den Umgang mit Petitionen nachzudenken.

Nachdem auf einer Mülldeponie bei Hohen Viecheln (siehe Punkt 2.17.2) auch eine Petition gefunden worden war, in der sich eine Bürgerin über einen Beamten beschwerte, erhielt ich sowohl vom Innenminister als auch vom Petitionsausschuß unseres Landtages die Anfrage, wie mit Petitionen umgegangen werden sollte, damit dem Petenten keine Nachteile entstehen. Im vorliegenden Fall hatte der Anwalt des Beamten, über den sich die Petentin beschwerte, Strafantrag wegen Beleidigung gestellt.

Ich habe daraufhin wie folgt geantwortet:

Soweit bei einer Behörde Petitionen eingereicht werden, liegt die Verantwortung für den ordnungsgemäßen Umgang mit personenbezogenen Daten bei der betreffenden Stelle (speichernde Stelle) selbst. Handelt es sich bei der Petition um ein reines Sachproblem, bei dem der Name des Petenten zur Aufklärung des weiteren Sachverhaltes keine Rolle spielt, habe ich empfohlen - im Falle einer Weiterleitung an eine nachgeordnete Behörde - die Petition zu anonymisieren. Soweit eine Behörde Eingaben vom Petitionsausschuß oder anderen Stellen zur Stellungnahme übermittelt bekommt, liegt es im Verantwortungsbereich der übermittelnden Stelle, für die Anonymisierung - soweit sie erforderlich und möglich ist - Sorge zu tragen, vergl. § 12 Abs. 2 DSG MV.
Daher habe ich dem Petitionsausschuß empfohlen, künftig den Petenten in der Eingangsbestätigung die Behandlung der Eingabe näher zu erläutern. Insbesondere sollte der Petent darauf hingewiesen werden, daß der Petitionsausschuß zur Erfüllung seiner Aufgaben berechtigt ist, die Petition auch in nicht anonymisierter Form an die Landesregierung oder an einen Fachausschuß zur Stellungnahme zu überweisen. Der Petent sollte weiterhin darauf hingewiesen werden, daß er sich, falls er mit der o. g. Verfahrensweise nicht einverstanden ist, schriftlich mit dem Petitionsausschuß innerhalb einer bestimmten Frist in Verbindung setzt.

Die zuständigen Stellen haben meine Empfehlungen aufgegriffen und bemühen sich um eine akzeptable Lösung.

2.2 Rechtswesen

2.2.1 Entwurf eines Strafverfahrensänderungsgesetzes (StVÄG 93)

Nachdem in der Vergangenheit bereits mehrere Entwürfe zur Änderung der Strafprozeßordnung (StPO) vorlagen, steht nunmehr der Entwurf eines Strafverfahrensänderungsgesetzes (StVÄG 1993) zur Debatte. Er erschöpft sich, soweit es den Datenschutz betrifft, in teilweise inhaltsleeren Verweisen auf landesrechtliche Vorschriften und bleibt weit hinter den bisher erreichten Regelungen zum Schutz personenbezogener Daten zurück. Angesichts der vom Bundesverfassungsgericht bereits vor zehn Jahren im Volkszählungsurteil aufgestellten Grundsätze zur Verhältnismäßigkeit und Normenklarheit bei Gesetzesformulierungen verwundert es, daß dies nicht in den vorliegenden Gesetzesentwurf mit eingeflossen ist.
Ich gehe an dieser Stelle nur auf einige Punkte näher ein:

- U. a. soll geregelt werden, daß öffentliche Stellen von sich aus an die Staatsanwaltschaft personenbezogene Daten zur Erfüllung der Ermittlungstätigkeit übermitteln können.
  Eine Regelung in dieser pauschalen Formulierung wird dem Grundsatz der Normenklarheit und Erforderlichkeit in keiner Weise gerecht. Wer was wann übermitteln darf, muß bereichsspezifisch festgelegt werden. Soweit keine solchen Regelungen bestehen, gilt hinsichtlich der Befugnis zur Datenübermittlung entweder das Bundesdatenschutzgesetz bzw. für die öffentlichen Stellen des Landes das Landesdatenschutzgesetz.

  Weiterhin sieht der Entwurf ein pauschales Einsichtsrecht seitens der Gerichte, Staatsanwaltschaften sowie der anderen Justiz- und Strafverfolgungsbehörden "zum Zwecke der Rechtspflege" vor.
  Der Terminus "Rechtspflege" ist weitgehend unbestimmt. So kann sich beispielsweise eine Regelung in der StPO nur auf die Strafrechtspflege, nicht aber auf die gesamte Rechtspflege erstrecken. Häufig benötigt eine Behörde nicht alle Informationen, die sich in einer Akte befinden. Die Strafverfolgungsbehörde braucht z.B. nur die Auskünfte, die sich auf die Strafverfolgung beziehen. Wenn also erkennbar nur Einzelinformationen benötigt werden, ist ein pauschales Akteneinsichtsrecht unzulässig.

- Die im Entwurf geplante Auskunftsregelung an "öffentliche Stellen" ist ebenfalls datenschutzrechtlich nicht akzeptabel, denn danach würden besonders sensible Daten aus Strafverfahrensakten genauso behandelt werden wie sonstige bei öffentlichen Stellen vorhandene Daten.

- Des weiteren ist es nicht zulässig, personenbezogene Informationen von Betroffenen schon dann an Privatpersonen weiterzuleiten, wenn diese über einen Anwalt ein berechtigtes Interesse darlegen. Ich begrüße es daher, daß auch der vorliegende Entwurf an dieser Stelle zusätzlich die Einschränkung aufgenommen hat:

  "... wenn überwiegende schutzwürdige Interessen des Betroffenen einer Auskunftserteilung (nicht) entgegenstehen".

- Die geplante Forschungsklausel berücksichtigt die schutzwürdigen Belange der Betroffenen ebenfalls nur unzureichend. Es wird nicht differenziert nach freiwillig oder unfreiwillig gemachten Angaben und anderen, einer besonderen Zweckbindung unterliegenden Daten, etwa solchen, die aus einer Überwachung des Fernmeldeverkehrs resultieren. In diesem Zusammenhang ist zu berücksichtigen, daß die in der StPO geregelte Forschungsklausel nicht hinter dem Standard des § 30 DSG MV (Verarbeitung und Nutzung personenbezogener Daten zu wissenschaftlichen Zwecken) zurückbleibt. Eine in die StPO aufzunehmende Regelung sollte zumindest soweit ausformuliert sein, wie es die Datenschutzgesetze der Länder vorsehen.

  Ich habe hier einige gravierende Mängel herausgegriffen und dem Justizminister unseres Landes meine Bedenken bereits mitgeteilt und ihn gebeten, sie bei den bevorstehenden Beratungen im Strafrechtsausschuß der Justizministerkonferenz mit zu berücksichtigen.

2.2.2 Entwurf eines Registerverfahrenbeschleunigungsgesetzes

Zur Stellungnahme lag mir der Diskussionsentwurf eines Gesetzes zur Vereinfachung und Beschleunigung registerrechtlicher und anderer Verfahren - Registerverfahrenbeschleunigungsgesetz (RegVBG) - Stand: 17. Februar 1993 vor. Seitens des Bundesministeriums für Justiz (BMJ) wird argumentiert, daß für die wirtschaftliche Entwicklung in den neuen Ländern die Wiederherstellung geordneter Eigentumsverhältnisse und ein reibungsloser Ablauf des Grundbuchverfahrens sowie die Führung der übrigen für das Wirtschaftsleben wichtigen Register, namentlich des Handelsregisters und des Genossenschaftsregisters, von entscheidender Bedeutung seien. Das ist sicher grundsätzlich richtig. Jedoch darf dies nicht dazu führen, daß im Zuge der Automatisierung von Registern bereits erreichte Datenschutzstandards wieder in Frage gestellt werden.

In Mecklenburg-Vorpommern läuft ein teilautomatisiertes Verfahren unter der Bezeichnung "ARGUS-Grundbuch". Dieses Verfahren hat eine umfassende Unterstützung der Arbeit des Grundbuchamtes zum Ziel.

Dem Justizminister unseres Landes habe ich meine Stellungnahme zu dem Gesetzesentwurf übersandt und ihn gebeten, meine Empfehlungen bei den kommenden Beratungen des Gesetzes im Bundesrat mit zu berücksichtigen. Im einzelnen sind dabei folgende Grundsätze zu beachten:

- Die Datenschutzbeauftragten des Bundes und der Länder fordern schon seit langem, daß die Einsichtnahme in das Grundbuch protokolliert wird. Sowohl bei den anderen Landesdatenschutzbeauftragten als auch bei mir gehen immer wieder Petitionen von betroffenen Bürgern ein, in denen sie sich darüber beklagen, daß Eigentums- und finanzielle Verhältnisse, die sich aus dem Grundbuch ergeben, Unbefugten zur Kenntnis gelangen und zum Nachteil der Eigentümer verwandt werden.

- Das Grundbuch ist kein öffentliches Register, in das jedermann schrankenlos Einsicht nehmen kann. In der Grundbuchordnung finden sich deshalb entsprechende Vorschriften, die nur bestimmten Personengruppen beim Vorliegen eines berechtigten Interesses die Einsichtnahme gestatten. Diese Vorschriften gehen jedoch ohne wirksame Kontrolle häufig ins Leere, u. a. auch deshalb, weil sich der Betrieb bei den Grundbuchämtern im Laufe der Jahre zu einem Massengeschäft entwickelt hat.

- Das immer wieder von den Justizverwaltungen vorgebrachte Argument, eine lückenlose Protokollierung aller Einsichtnahmen stelle für die Grundbuchämter eine nicht zu bewältigende Arbeitsbelastung dar, ist nicht akzeptabel. Die Umstellung von einem in Papierform geführten Grundbuch auf ein elektronisches Verfahren wird zu erheblichen Arbeitserleichterungen führen. Dies sollte allerdings auch Anreiz dafür sein, dem informationellen Selbstbestimmungsrechtder Grundstückseigentümer besser gerecht zu werden.

- Insbesondere hinsichtlich der Art und Weise der Protokollierung der Einsichtnahme in das Grundbuch und meiner Möglichkeiten zur Kontrolle der Einhaltung des Datenschutzes hatte ich einen konkreten Vorschlag unterbreitet. Aus Beschleunigungsgründen wurde jedoch die Protokollierung der Einsicht in das Grundbuch in den Gesetzesentwurf nicht mehr aufgenommen.
  Es bleibt zu hoffen, daß in dem Entwurf einer nun geplanten Rechtsverordnung zum Grundbucheinsichtsrechtdie Vorschläge der Datenschutzbeauftragten Berücksichtigung finden.

2.2.3 Bekanntgabe persönlicher Daten im Rahmen von Gerichtsverfahren

Das geltende Recht sichert den Schutz persönlicher Daten von Prozeßbeteiligten zwar in der öffentlichen Hauptverhandlung gem. §§ 170, 171 a, 171 b, 172, 174 Gerichtsverfassungsgesetz (GVG) zu, jedoch ist außerhalb derselben kein Schutz dieses Persönlichkeitsrechtes gewährleistet. Mehrere Petitionen mit z.T. sehr schwerwiegenden Beeinträchtigungen für das Persönlichkeitsrecht der betreffenden Prozeßbeteiligten durch Verbreitung von persönlichen Daten in diesem Verfahrensstadium sind bei mir eingegangen.

Im Kreise der Justizminister und der Datenschutzbeauftragten werden z.Z. zwei Lösungsvorschläge diskutiert. Es könnte § 411 Zivilprozeßordnung (ZPO) oder § 174 GVG (Verhandlung über Ausschluß der Öffentlichkeit; Schweigepflicht) um einen Absatz erweitert werden. Aus meiner Sicht wäre eine geeignete Ergänzung des § 174 GVG die umfassendere Lösung, so daß ich lediglichdiese Variante hier kurz skizzieren möchte.
Der Abs. 4 könnte lauten:

"Abs. 3 gilt entsprechend außerhalb einer Verhandlung, wenn das Gericht im Fall einer mündlichen Verhandlung die Öffentlichkeit nach den in Abs. 3 genannten Vorschriften ausschließen würde. Die Geheimhaltungspflicht ist in diesem Fall den am Verfahren beteiligten Personen aufzuerlegen."

Danach könnte das Gericht den anwesenden Personen, darunter sind insbesondere auch die Parteien und ihre Anwälte zu verstehen, eine Geheimhaltungspflicht auferlegen, die strafrechtlich sanktioniert wäre. Fraglich ist, ob darüber hinaus ein Bedürfnis besteht, die Regelung auf solche Fälle auszudehnen, in denen eine öffentliche Verhandlung nicht stattfindet und daher ein Ausschluß der Öffentlichkeit nicht in Betracht kommt. So kann meines Erachtens ein effektiver Schutz des Persönlichkeitsrechtes von Prozeßbeteiligten nur dann erreicht werden, wenn die Schweigepflicht schon in einem Verfahrensstadium auferlegt werden kann, in dem es noch nicht zu einer mündlichen Verhandlung gekommen ist. Es kann beispielsweise für die Wahrung des Persönlichkeitsrechtes eines Prozeßbeteiligten zu spät sein, wenn bei der mündlichen Verhandlung, in der ein über ihn erstelltes ärztliches Gutachten erörtert wird, die Öffentlichkeit ausgeschlossen und das Schweigegebot des § 174 Abs. 3 GVG erlassen wird. Denn schon vorher ist das Gutachten dem jeweiligen Prozeßgegner bzw. dessen Prozeßbevollmächtigten in Wahrnehmung des rechtlichen Gehörs und zur Vorbereitung der Anhörung zugegangen.

Alles in allem halte ich den obigen Gesetzesvorschlag für geeignet, die Verbreitung intimer persönlicher Daten insbesondere aus ärztlichen oder psychologischen Gutachten, die im Zusammenhang mit Gerichtsverfahren erhoben worden sind, zu verhindern. Diese Auffassung habe ich dem Minister für Justiz, Bundes- und Europaangelegenheiten des Landes zur Kenntnis gegeben. Er hat signalisiert, daß er ebenfalls einer Lösung im Rahmen des § 174 GVG den Vorzug gibt.

2.2.4 Aufbau eines bundesweiten Schuldnerverzeichnisses

In letzter Zeit kommen zunehmend nicht-öffentliche Stellen auf die Idee, bundesweite private Schuldnerverzeichnisse zu erstellen.
Problematisch ist dabei u. a., ob bei derart sensiblen Daten Private die Gewähr dafür bieten, daß z. B. Löschungsfristen, wie sie in § 915 Abs. 2 ZPO vorgeschrieben sind, eingehalten werden. Nach meiner Auffassung ist die Führung eines solchen Verzeichnisses weder aufgrund der gegenwärtigen Gesetzesregelung noch aufgrund der Anforderungen des Bundesverfassungsgerichts an den sogenannten Übergangsbonus zulässig. Nach dem Wortlaut der o. g. Vorschriften werden die Daten von Schuldnern für ein bei dem Vollstreckungsgericht geführtes Schuldnerverzeichnis erhoben und gespeichert. Zweck des Verzeichnisses ist es, Auskünfte geben zu können, ob eine bestimmte Person bei diesem Vollstreckungsgericht die eidesstattliche Versicherung abgegeben hat oder ob gegen sie die Haft angeordnet ist. Mit einer bundesweiten Zentralisierung der Schuldnerverzeichnisse wäre eine über den gesetzlich bestimmten Zweck hinausgehende Zweckänderung verbunden. Zweck des zentralisierten Verzeichnisses wäre es, Auskunft darüber zu geben, ob eine bestimmte Person bei irgend einem Vollstreckungsgericht mit den in § 915 Abs. 1 ZPO beschriebenen Angaben verzeichnet ist. Jede Zweckänderung in der Verwendung erhobener oder gespeicherter Daten ist jedoch ein Eingriff in das Recht des Betroffenen auf informationelle Selbstbestimmung. So kann die Eintragung im Schuldnerverzeichnis für den betreffenden Schuldner gewissermaßen dessen "bürgerlichen Tod" bedeuten, weil eine Teilnahme am Wirtschaftsleben stark beeinträchtigt wird. Dies zeigt, wie empfindlich der Regelungsbereich ist.

Bei der Novellierung der Vorschrift muß unbedingt darauf geachtet werden, daß in das Schuldnerverzeichnis nur solche Daten aufgenommen werden, die zum Schutz des redlichen Geschäftsverkehrs notwendig sind, und daß der Umgang mit diesen Daten normenklar geregelt wird. Ebenso ist für eine unverzügliche Löschung der Eintragungen zu sorgen, wenn ihre Speicherung nicht mehr gerechtfertigt ist.

2.2.5 Datenschutzvorschriften auch für Notare

Bei uns in Mecklenburg-Vorpommern gibt es tatsächlich öffentliche Stellen, die der Auffassung sind, Datenschutz gelte nicht für sie. Die Notarkammer Mecklenburg-Vorpommern ist der Ansicht, daß das DSG MV für Notare nicht gilt, obwohl ein Beschluß des Bundesgerichtshofes vom 30.07.1990 (s. NJW 1991, S. 568 ff) die anderslautende Auffassung der Datenschutzbeauftragten bereits bekräftigte.
Gem. § 2 Abs. 1 DSG MV erfaßt das Gesetz alle Behörden und öffentlich-rechtlich organisierten Einrichtungen und Stellen des Landes. Dazu gehören auch die im Lande tätigen Notare. Gem. §§ 1, 3 Bundesnotarordnung (BNotO) sind sie durch Hoheitsakt bestellte Träger eines öffentlichen Amtes. Nach § 2 Abs. 3 Satz 2 DSG MV gelten die Vorschriften dieses Gesetzes ebenso für Gerichte, soweit sie Verwaltungsaufgaben wahrnehmen. Festzuhalten ist demnach, daß mangels entsprechender bereichsspezifischer Regelungen hinsichtlich der Löschungsfristen das Datenschutzgesetz des Landes grundsätzlich auch für Notare gilt. Weiterhin sind Dateibeschreibungen und Geräteverzeichnisse, die dem aktuellen Stand entsprechen müssen, bei den Notaren vorzuhalten. Die Verpflichtung, die Dateien dem Landesbeauftragten für den Datenschutz zu übersenden, besteht - im Gegensatz zu einigen anderen Bundesländern - nur auf dessen ausdrücklicher Anforderung.

Ich habe die Notarkammer darauf hingewiesen, daß eine Löschung von Daten in erster Linie hinsichtlich des Verwahrungs- und Massebuches in Betracht kommen dürfte und die Angabe erforderlich ist, nach wieviel Jahren die Daten gelöscht werden.
Gem. § 11 Abs. 2 Nr. 4 DSG MV sind personenbezogene Daten zu löschen, wenn ihre Speicherung zur Erfüllung der in der Zuständigkeit der mit den Daten umgehenden Stelle liegenden Aufgaben nicht mehr erforderlich ist. Anstelle der Berichtigung oder Löschung tritt gem. § 11 Abs. 3 DSG MV eine Sperrung, wenn einer Löschung nach § 11 Abs. 2 Nr. 4 DSG MV Rechts- oder Verwaltungsvorschriften entgegenstehen oder Grund zu der Annahme besteht, daß durch die Berichtigung oder Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, eine Löschung wegen der besonderen Art nicht oder nur unter verhältnismäßig hohem Aufwand möglich ist oder es der Betroffene nach § 21 DSG MV verlangt.
Ich habe die Notarkammer Mecklenburg-Vorpommern daher aufgefordert, die Vordrucke "Dateibeschreibung" und "Geräteverzeichnis" den Notaren im Lande zur Verfügung zu stellen. Bisher liegt mir keine Mitteilung vor, daß entsprechend meinen Empfehlungen verfahren wird.

2.3 Einwohnerwesen

2.3.1 Novellierung des Melderechtsrahmengesetzes

In Anbetracht der bevorstehenden Wahlen zum Deutschen Bundestag und zum Europaparlament ist nach Ansicht der Landesbeauftragten für den Datenschutz auf Bundesebene eine Änderung der Verfahrensweise hinsichtlich der Übermittlung von Meldedaten an Parteien und Wählergruppen erforderlich.
Nach der derzeitigen Fassung des § 22 Abs. 1 des Melderechtsrahmengesetzes (MRRG) darf die Meldebehörde den Parteien und Wählergruppen im Zusammenhang mit den genannten Wahlen in den sechs der Wahl vorangehenden Monaten Auskunft aus dem Melderegister über Vor- und Familiennamen, akademische Grade und Anschriften von Wahlberechtigten erteilen. Aus datenschutzrechtlicher Sicht muß diese Regelung zumindest um eine Widerspruchslösung erweitert, wenn nicht gar ersatzlos gestrichen werden. Nach einer Ergänzung der Regelung um die Widerspruchslösung dürfte die Meldebehörde künftig im Rahmen von Wahlen zum Deutschen Bundestag oder zum Europäischen Parlament nur noch dann Auskunft aus dem Melderegister über die Daten des Wahlberechtigten erteilen, wenn der Wahlberechtigte dieser Auskunftserteilung nicht widersprochen hat. Anlaß für den Novellierungsvorschlag war die antragsgemäße Herausgabe von Anschriften über Wahlberechtigte seitens einer Meldebehörde an alle zu einer Wahl angetretenen Parteien unabhängig von ihrer politischen Ausrichtung. Dabei erhielt eine Partei durch die Kombination der Kriterien "bestimmte Ortsteile" plus "Altersstruktur" letztlich eine Auswertung aus dem Melderegister, die im Ergebnis einer Rasterfahndung nahe kam. Damit bei den nächsten Wahlen zum Europäischen Parlament nicht nur die rechtlichen, sondern auch die tatsächlichen Voraussetzungen zur technischen Umsetzung von Widersprüchen gewährleistet sind, muß die Erweiterung der Regelung aus § 22 MRRG auch rechtzeitig erfolgen.

Im LMG Mecklenburg-Vorpommerns ist die Widerspruchslösung für Parlaments- und Kommunalwahlen sowie für verfassungsrechtlich oder gesetzlich vorgesehene Abstimmungen bereits in § 35 Abs. 1 umgesetzt. Auf das Widerspruchsrecht hat die Meldebehörde den Betroffenen bei der Anmeldung und gem. § 36 LMG zusätzlich mindestens einmal jährlich durch öffentliche Bekanntmachung hinzuweisen.
Wie bereits erwähnt, ist jedoch aus datenschutzrechtlicher Sicht die ersatzlose Streichung des § 22 Abs. 1 MRRG einer Widerspruchslösung vorzuziehen, denn letztere hat den Nachteil, daß die Weitergabe der Meldedaten nur dann verhindert wird, wenn die Bürger von sich aus aktiv werden. Nach Ansicht der Landesbeauftragten für den Datenschutz bedarf es jedoch eigentlich in allen Fällen der Weitergabe von Meldedaten an Parteien einer selbständigen Begründung für diese Übermittlung. Denn bereits die Meldepflicht an sich stellt einen Eingriff in das informationelle Selbstbestimmungsrecht des einzelnen dar, der nur im überwiegenden Allgemeininteresse gerechtfertigt ist. Die Weitergabe der Meldedaten an Parteien schränkt dieses Grundrecht erneut ein; auch diese Einschränkung ist nur im überwiegenden Interesse der Allgemeinheit zulässig. Daß aber alle Parteien, die Adressen anfordern und verwenden, hierbei zugleich im überwiegenden Allgemeininteresse handeln, erscheint angesichts der Praxis einzelner Parteien durchaus zweifelhaft.

Ich habe mich an unser Innenministerium gewandt, um auf die Dringlichkeit einer Änderung des § 22 Abs. 1 MRRG hinzuweisen. Von dort wurde mir mitgeteilt, daß im Entwurf eines Ersten Gesetzes zur Änderung des Melderechtsrahmengesetzes (Bundestags-Drucksache 12/2376 vom 06.04.1992) bereits eine Änderung des § 22 Abs. 1 MRRG im Sinne einer Widerspruchslösung vorgesehen ist. Aufgrund meines Schreibens wird sich das Innenministerium nunmehr erneut an das Bundesministerium des Inneren (BMI) wenden, um auf die Notwendigkeit einer rechtzeitigen Änderung des MRRG auch unter datenschutzrechtlichen Gesichtspunkten hinzuweisen.

2.3.2 Einwohnermeldedaten für den Rundfunkgebühreneinzug

Darf die Meldebehörde zum Zwecke der Erhebung und des Einzuges von Rundfunkgebühren nach § 2 Abs. 2 des Rundfunkgebührenstaatsvertrages im Falle der Anmeldung, Abmeldung oder des Todes bestimmte Daten volljähriger Einwohner an die Gebühreneinzugszentrale (GEZ) übermitteln? Diese Frage war zu beantworten, als es darum ging, eine zusätzliche Bestimmung einzuführen, um durch einen Datenabgleich "Schwarzseher und Schwarzhörer" besser zu erfassen.

Gegenüber dem Innenminister unseres Landes habe ich hierzu folgende Stellungnahme abgegeben:

§ 4 Abs. 6 Rundfunkgebührenstaatsvertrag regelt abschließend, daß die Landesrundfunkanstalten über Personen, bei denen tatsächlich Anhaltspunkte vorliegen, daß sie ein Rundfunkgerät zum Empfang bereit halten und dies nicht angezeigt haben, auch Auskünfte bei Meldebehörden eingeholt werden dürfen. Voraussetzung ist, daß dies zur Überwachung der Rundfunkgebührenpflicht erforderlich und die Erhebung der Daten beim Betroffenen nicht möglich ist oder einen unverhältnismäßigen Aufwand erfordern würde. Zunächst setzt die Vorschrift voraus, daß tatsächlich Anhaltspunkte bei der betreffenden Person vorliegen, daß sie bei der An- bzw. Abmeldung ihrer Anzeigepflicht nicht nachgekommen ist. Bei einer im Unterausschuß "EDV im Einwohnerwesen" des Arbeitskreises II der Ständigen Konferenz der Innenminister der Länder vorgesehenen pauschalen Datenübermittlung wird jedoch nicht mehr von tatsächlichen Anhaltspunkten bei einzelnen nicht zahlenden Personen ausgegangen; es wird vielmehr der Umkehrschluß gezogen, daß Personen, die sich beispielsweise ummelden, generell ihrer gem. § 3 Rundfunkgebührenstaatsvertrag bestehenden Anzeigepflicht nicht nachkommen. Aus der Formulierung des § 4 Abs. 6 Rundfunkgebührenstaatsvertrag geht meines Erachtens eindeutig hervor, daß eine Einzelfallübermittlung, nicht jedoch eine generelle Datenübermittlung beabsichtigt war. Würde man nun eine regelmäßige Datenübermittlung in einer Rechtsverordnung - also in eine unterhalb des Gesetzes angesiedelten Norm - festschreiben, so würde die Intention des Gesetzgebers ins Gegenteil verkehrt. Bei einer entsprechenden Formulierung - wie im o. g. Musterentwurf vorgesehen - wären folgende Grundsätze verletzt:

1. Verletzung des Grundrechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) einer Vielzahl von Bürgern,

2. Verletzung des Grundsatzes, daß derartige Eingriffe einer (verfassungsmäßigen) gesetzlichen Grundlage bedürfen (siehe Volkszählungsurteil, BVerfGE 65, 46),

3. Verletzung des Grundsatzes der Verhältnismäßigkeit.

Unser Innenminister hat mir inzwischen mitgeteilt, daß er meine datenschutzrechtlichen Bedenken teilt.
Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 46. Sitzung am 26./27. Oktober 1993 in Berlin eine Entschließung zu der vorgenannten Thematik gegen die Stimme Bayerns und bei Stimmenthaltung Sachsens verabschiedet (siehe Anlage 6).

2.3.3 Datenübermittlungen der Meldebehörde an Private

Ein Bürger bat mich um eine datenschutzrechtliche Bewertung einer von ihm beabsichtigten Melderegisterauskunft. Für ein Projekt sei es erforderlich, daß er die Namen und die Anschriften einer ganz bestimmten Personengruppe in einigen Großstädten der Bundesrepublik erhalte. Nach seiner Vorstellung sollten Namen und Anschriften anhand des selektiven Kriteriums "Geburtsdatum" von den Meldebehörden der jeweiligen Städte erfragt werden, z. B. alle Namen sowie Anschriften derjenigen Personen der Stadt "X", die zwischen dem 1. Januar und dem 31. Dezember 1958 geboren wurden. An den Geburtsdaten selbst hätte er keine Interesse. Aus dem Schreiben des Petenten ging nicht genau hervor, um welches Projekt es sich handelt; er teilte aber mit, daß er mit dem Vorhaben jedenfallsauch privatwirtschaftlicheInteressen verfolge.

Einschlägig ist § 34 des LMG MV. Dort hat der Gesetzgeber unterschieden zwischen einer einfachen Melderegisterauskunft, einer erweiterten Melderegisterauskunft und einer Gruppenauskunft. Im Gegensatz zur einfachen und erweiterten Melderegisterauskunft, bei der unter bestimmten Umständen personenbezogene Daten einzelner bestimmter Einwohner übermittelt werden, zeichnet sich die Gruppenauskunft dadurch aus, daß diese Auskunft über eine Vielzahl nicht namentlichbezeichneter Einwohner erteilt wird.
Im vorliegenden Fall handelt es sich bei der von dem Bürger gewünschten Auskunft um eine Gruppenauskunft. Sie darf gemäß § 34 Abs. 3 LMG von der Meldebehörde nur dann erteilt werden, wenn sie im öffentlichen Interesse liegt. Daß hier ein entsprechendes öffentliches Interesse vorliegt, trägt der Petent selbst nicht vor. Davon ausgehend kann die zuständige Meldebehörde auch keine Auskunft erteilen. Dies habe ich dem Petenten mitgeteilt.

Er hatte sich mit der Bitte um die datenschutzrechtliche Bewertung seiner beabsichtigten Melderegisterauskunft aber nicht nur an mich, sondern - da er für das Projekt auch die Daten von Personengruppen in anderen Großstädten benötigt - auch an meine Kollegen in den anderen Bundesländern gewandt. Von diesen hat er im Ergebnis ebenfalls eine ablehnende Antwort erhalten. Da die Länderregelungen zur Gruppenauskunft den Vorgaben des Melderechtsrahmengesetzes des Bundes folgen, finden sich in den Landesmeldegesetzen gleich- bzw. ähnlich lautende Bestimmungen.

2.3.4 ZER-Zentrales Einwohnermelderegister

1971 wurde allen DDR-Bürgern eine Personenkennzahl (PKZ) zugeordnet. In dem später errichteten zentralen Melderegister diente diese Kennzahl als Ordnungsmerkmal zur eindeutigen Personenidentifizierung. Die Datenbestände des ZER enthielten, was den meisten DDR-Bürgern nicht bekannt war, neben den eigentlichen Meldedaten auch eine Vielzahl personenbezogener Daten, derer sich die Justiz, die Polizei u. a. Verwaltungsbehörden bedienen konnten und zu denen das MfS einen direkten Zugriff hatte.

Gemäß Anlage I, Kap. II, Sachgebiet C, Abschnitt III, Nr. 46 des Einigungsvertrages war nach dem 31. Dezember 1992 eine weitere Nutzung der PKZ und des gesamten ZER-Datenbestandes nicht mehr zulässig. Die Meldebehörden der neuen Bundesländer sollten bis dahin ihre örtlichen Melderegister soweit umgestellt und neu aufgebaut haben, daß sie den Datenbestand des ZER nicht mehr benötigen. Bis zum Herbst 1992 war diese Umstellung vollzogen und der Meldedatenbestand des ZER hätte gelöscht werden können. Nun hat aber der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (Gauck-Behörde) noch Bedarf an der PKZ angemeldet. Sie wird dort insbesondere zur Erleichterung der eindeutigen Identifikation bestimmter Personen benötigt. Der BfD und die zuständigen LfD hatten hiergegen keine grundsätzlichen Bedenken. Allerdings waren die LfD der Auffassung, daß eine eindeutige gesetzliche Regelung, beispielsweise durch Änderung des Stasi-Unterlagen-Gesetzes (StUG) vonnöten sei. Sie haben das auf der Sitzung der Arbeitsgruppe "Datenschutz in den neuen Bundesländern" am 04. März 1993 in Kleinmachnow klar zum Ausdruck gebracht.

Im Juni 1993 erhielt ich aus unserem Innenministerium die Nachricht, daß aus Mecklenburg-Vorpommern ein reduzierter Meldedatenbestand dem BMI zur weiteren Nutzung durch die Gauck-Behörde übergeben werden soll, obwohl bisher keine gesetzliche Grundlage hierfür geschaffen wurde. Dieses Vorgehen war mit den Innenministerien der anderen neuen Bundesländer einschließlich Berlin abgesprochen. Der Innenausschuß des Landtages Brandenburg hat darauf hin sofort reagiert und einen Entschließungsantrag vorbereitet und ein Fraktionsmitglied des Bündnis 90/Grüne hat beim Verfassungsgericht eine einstweilige Verfügung gegen diese Datenübermittlung beantragt. Vom Innenministerium des Landes Brandenburg wurde zugesichert, daß eine Übergabe der Daten nicht stattfinden wird, solange rechtliche Bedenken bestehen.

Am 07. Oktober 1993 erhielt ich den Entwurf (CDU/CSU, SPD und F.D.P.) eines Gesetzes zur Änderung des Stasi-Unterlagen-Gesetzes zur Kenntnis. Dieser Entwurf wurde einige Tage später auf der Sitzung des Arbeitskreises "Datenschutz in den neuen Bundesländern" in Schwerin behandelt. Grundsätzlich begrüßten die Teilnehmer, daß die Weiternutzung des Meldedatenbestandes durch den Bundesbeauftragten für die Stasi-Unterlagen nun bereichsspezifisch geregelt werden soll. Es bestanden lediglich insofern Änderungswünsche, als zum einen der Bundesbeauftragte eine von den übrigen Stellen abgeschottete Stelle innerhalb der Behörde einrichten sollte, so daß eine Nutzung der Daten - Meldedatenbestand der gesamten Bevölkerung der ehemaligen DDR - nur erfolgt, wenn dies im Einzelfall zur Aufgabenerfüllung erforderlich ist. Zum anderen sollte der Zweck (Identifizierung von hauptamtlichen Mitarbeitern, unbekannten Mitarbeitern, Offizieren im besonderen Einsatz sowie inoffiziellen Mitarbeitern) im Hinblick auf das informationelle Selbstbestimmungsrecht der Bürger der ehemaligen DDR konkret benannt werden.

Die Datenschutzbeauftragten der neuen Bundesländer und der Berliner Datenschutzbeauftragte haben ihre dahingehend formulierte Stellungnahme dem Innenausschuß des Deutschen Bundestages zugeleitet. Inwiefern die datenschutzrechtlichen Vorstellungen umgesetzt werden, bleibt abzuwarten.

2.3.5 Einwohneradreßbücher

In den größeren Städten Mecklenburg-Vorpommerns werden seit 1991 wieder Einwohneradreßbücher in einer Auflagenhöhe zwischen 450 und 1500 Exemplaren verlegt.
Ich habe hierzu eine Reihe von Anfragen und Petitionen erhalten. Viele Bürger wollten wissen, ob die Veröffentlichung der Einwohnerdaten im Adreßbuch rechtmäßig sei und äußerten Bedenken, daß durch die Veröffentlichung ihrer Daten Dritte auf diese Zugriff haben und sie mißbräuchlich verwenden könnten.
In allen Fällen habe ich darauf hingewiesen, daß gem. § 35 Abs. 3 LMG die Anschriften aller Einwohner, die das 18. Lebensjahr vollendet haben, Vor- und Familiennamen sowie akademische Grade an Adreßbuchverlage weitergegeben werden dürfen. Ausgenommen von dieser Regelung sind lediglich die Anschriften von Justizvollzugsanstalten, Krankenhäusern und Heimen. Die Einwohner haben jedoch gem. § 35 Abs. 3 Satz 2 LMG das Recht, der Weitergabe ihrer Daten zu widersprechen. Die Meldebehörden sind nach § 35 Abs. 3 Satz 3 LMG verpflichtet, bei der Anmeldung sowie frühestens sechs und spätestens zwei Monate vor der Auskunftserteilung an den Adreßbuchverlag durch amtliche Bekanntmachung auf das Widerspruchsrecht hinzuweisen.
Die in § 35 Abs. 3 Satz 4 LMG getroffene Regelung, wonach die Daten der Einwohner nur in alphabetischer Reihenfolge der Familiennamen veröffentlicht werden dürfen, wird häufig als bürgerfreundlich bezeichnet. Dabei wird jedoch übersehen, daß mittels allgemein zugänglicher und preiswerter technischer Geräte, wie z. B. Scannern und der dazugehörigen Software, auch jede anderweitige Sortierung der Adressen und so auch die Erstellung eines Straßenverzeichnisses leicht möglich ist. Darüber hinaus ist zu erwarten, daß Adreßbücher demnächst ebenso auf maschinenlesbaren Datenträgern angeboten werden, wie es bei Telefonbüchern auf Messen bereits der Fall gewesen ist.
Ich halte die vor allem für die Werbebranche interessanten Einwohneradreßbücher für datenschutzrechtlich bedenklich, da aus ihnen eine Reihe von weiteren persönlichen Daten mittels Recherche gewonnen werden können. So lassen sich u.a. auch durch Vergleiche mit vorherigen Ausgaben zusätzliche Informationen ableiten wie z. B.:

- Wer ist Single? Wer ist erst seit kurzer Zeit verheiratet? Oder wer ist gerade 18 Jahre geworden (besondere Zielgruppen für Werbefirmen)?
- In welchen Häusern oder Wohngegenden leben Ausländer?
- Welche Einfamilienhäuser werden von Einzelpersonen bewohnt?
- Wer ist zu- oder weggezogen?

Außerdem läuft das gem. § 35 Abs. 3 Satz 2 LMG bestehende Widerspruchsrecht als Recht des Einwohners weitgehend leer. Zum einen werden die öffentlichen Bekanntmachungen von sehr vielen Einwohnern nicht gelesen, und zum anderen wird gerade derjenige, der von seinem Widerspruchsrecht Gebrauch macht, für andere interessant. Es könnte der Eindruck erweckt werden, daß diejenigen, die sich gegen eine Veröffentlichung im Adreßbuch aussprechen, etwas zu verbergen haben und so möglicherweise für kriminelle Kreise von besonderem Interesse sind.
Meines Erachtens sollten nur die Daten von den Einwohnern an Adreßbuchverlage weitergegeben werden, die der Weitergabe ausdrücklich zustimmen. Bei einer Novellierung des LMG werde ich mich für die Umwandlung der Widerspruchsregelung in eine Einwilligungsregelung einsetzen.

2.4 Polizei

2.4.1 Großer Lauschangriff

Für die Polizei wird es zunehmend schwieriger, Aktivitäten des organisierten Verbrechens rechtzeitig zu erkennen und schwere Straftaten zu verhindern. Immerhin handelt es sich bei den Personen, die hier am Werke sind, um die Elite der kriminellen Szene. Zumeist sind diese Leute sehr gut ausgebildet, verfügen über ausreichende finanzielle Mittel sowie eine moderne Technik und bedienen sich effektiver Organisationsformen. Deshalb wurde im September 1992 das Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungen der Organisierten Kriminalität (OrgKG) verabschiedet. Zwar war in früheren Gesetzesentwürfen zum OrgKG vorgesehen, unter bestimmten Voraussetzungen das Abhören in und aus Wohnungen bei Anwesenheit eines verdeckt ermittelnden Beamten (sog. "Kleiner Lauschangriff") zuzulassen, jedoch wurde diese Regelung wegen des weitreichenden Eingriffes in die Persönlichkeitssphäre nicht in das OrgKG übernommen. Andere Regelungen hingegen, z. B. über den Einsatz von verdeckten Ermittlern, wurden auf eine gesetzliche Grundlage gestellt. Lediglich im präventiven Bereich ist das Abhören von Wohnungen durch die Polizei zur Abwehr einer gegenwärtigen Gefahr für Leib und Leben einer Person als ultima ratio zulässig. Dies ist durch Art. 13 Abs. 3 GG abgedeckt. Nun erwartet die Polizei aber vom Gesetzgeber, daß er auch Bild- und Tonaufzeichnungen mit technischen Mitteln in und aus Wohnungen zum Zwecke der Strafverfolgung erlaubt. Diese Maßnahme ist unter der Bezeichnung "Großer Lauschangriff" allgemein bekannt geworden und wird öffentlich ziemlich kontrovers diskutiert.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dieses Thema in ihrer Sitzung im Oktober 1992 ausführlich behandelt und im Ergebnis gegen die Stimme Bayerns eine Entschließung bekanntgegeben (Anlage 4), in der sie empfiehlt, daß der Lauschangriff auf Privatwohnungen zum Zwecke der Strafverfolgung auch in Zukunft nicht erlaubt werden darf.
Eine andere Frage sei es, ob und unter welchen Voraussetzungen der Gesetzgeber für Räume, die allgemein zugänglich sind oder bestimmten beruflichen oder geschäftlichen Tätigkeiten dienen, wie z.B. Hinterzimmer von Gaststätten, Spielkasinos, Saunaclubs, Bordelle usw., einen Lauschangriff zulassen kann. Hierfür seien jedoch als Mindestvoraussetzungen ein eng begrenzter abschließender Straftatenkatalog, die Verwendung der gewonnenen Erkenntnisse ausschließlich zur Verfolgung dieser Straftaten, ein strikter Richtervorbehalt sowie die Wahrung besonderer Amts- und Berufsgeheimnisse vonnöten.
Diese Entschließung habe ich nach der Konferenz den Fraktionen unseres Landtages zur Kenntnis gegeben.

In seiner 82. Sitzung am 23. Juni 1993 hat unser Landtag einen Antrag der Fraktionen der CDU und der F.D.P. zur Konkretisierung des Wohnungsbegriffes in Art. 13 GG behandelt und zur federführenden Beratung an den Rechtsausschuß und zur Beratung an den Innenausschuß überwiesen. Im August 1993 habe ich eine Stellungnahme zur Einführung des Großen Lauschangriffes an die Fraktionsvorsitzenden und an den Innenminister versandt und darin meine datenschutzrechtlichen Bedenken geäußert sowie auf die verfassungsrechtliche Problematik, die Erforderlichkeit und Verhältnismäßigkeit des Mittels und auf mögliche Alternativen hingewiesen.
Der Innenminister hat seinen Standpunkt zur Konkretisierung des Wohnungsbegriffes ebenfalls mitgeteilt. Er hält die vorgesehene Konkretisierung des Wohnungsbegriffes in Art.13 GG hinsichtlich Geschäfts- und Privaträumen mit dem Ziel, das Abhören in den gemischt genutzten, kriminell bemakelten Räumen zu ermöglichen, für keine ausreichende Lösung. Nach seiner Auffassung wird diese Initiative ins Leere laufen, weil die Bandenbosse ihre Gespräche in Privatwohnungen verlegen. Außerdem würde eine solche Regelung Abgrenzungsprobleme in der praktischen Anwendung aufwerfen. Deshalb bedarf es nach seiner Auffassung zur erfolgreichen Bekämpfung der Organisierten Kriminalität auch einer rechtsstaatlichen Möglichkeit zur verdeckten Informationserhebung in oder aus Privatwohnungen. Es sollte den schon unterbreiteten Vorschlägen gefolgt werden, die bisherige Definition der Wohnung beizubehalten, dafür aber den Art. 13 GG so zu erweitern, daß der verdeckte Einsatz technischer Mittel in Wohnungen zur Datenerhebung bei Verfolgung schwerwiegender Verbrechen zulässig ist.

Aber selbst wenn wir die Möglichkeit eines heimlichen Einsatzes technischer Mittel in privaten Wohnungen gedanklich einmal antizipieren wollen, so ist doch wohl klar, daß diese Maßnahme ebenso ins Leere laufen würde, wenn sich die Verdächtigen in der Wohnung, die von der Polizei sorgfältig und mit hohem Aufwand präpariert worden ist, zunächst nur treffen, um dann gemeinsam eine andere Wohnung aufzusuchen. Soviel Intelligenz bei der Gestaltung ihrer Logistik müssen wir der Elite der Organisierten Kriminalität wohl zugestehen. Und es ist wohl ebenso klar, daß in einem solchen Fall das Schließen der Wohnungstür das vorläufig letzte Geräusch war, das aus der präparierten Wohnung aufgezeichnet werden konnte. Ich sage das, um auf die fragwürdige Effektivität dieses Mittels hinzuweisen, das in hohem Maße eine Verletzung des Datenschutzes impliziert, weil immer auch unschuldige und unbeteiligte Personen von der Überwachung betroffen sein werden und das als einziges der noch in Frage kommenden Mittel eine Verfassungsänderung erforderlich macht.

Bedauerlicherweise wurde bei öffentlich geführten Diskussionen schon vor einiger Zeit die Ebene der sachlichen Argumentation zugunsten strammer Behauptungen und persönlicher Vorwürfe verlassen. Trotzdem muß es immer wieder billig wundernehmen, wie leicht es fällt, denjenigen, der Bedenken gegen den Großen Lauschangriff äußert, des "Täterschutzes", "Verbrecherschutzes" oder gar eines Angriffes auf den Rechtsstaat zu bezichtigen. Glücklicherweise ist die Diskussion in jüngster Zeit wieder sachlicher geworden. Und selbst von seinen Befürwortern wird dieses Mittel zur Bekämpfung der Organisierten Kriminalität nun nur noch als eines unter vielen (und beileibe nicht als das wirksamste) angesehen. Insofern ist es auch von dieser Seite her durchaus noch fragwürdig, ob es überhaupt die unabdingbare Erforderlichkeit besitzt, die für die Aufgabe bzw. wesentliche Einschränkung eines so wichtigen Grundrechts wie Art. 13 GG notwendig ist.

Ich gehe davon aus, daß sich unser Landtag von solchen oder ähnlichen Überlegungen hat leiten lassen, als er in einem am 20. Oktober 1993 mit den Stimmen der CDU, der F.D.P. und der SPD gefaßten Beschluß die Landesregierung aufforderte, sich im Bundesrat zwar für eine Konkretisierung des Wohnungsbegriffes in Art. 13 GG einzusetzen, um den Einsatz technischer Mittel in bestimmten gemeinschaftlich genutzten Räumen, die heute noch unter den Wohnungsbegriff fallen, zu ermöglichen, aber den engsten Bereich privater Lebensgestaltung dabei nicht anzutasten.
Ich halte das für einen guten Kompromiß, zumal er sich in weitgehender Übereinstimmung mit der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. und 2. Oktober 1992 befindet. Und es bleibt zu hoffen, daß dieser Kompromiß am Ende aller Debatten, nämlich dann, wenn der Bundestag hierzu seine Entscheidung trifft, die Lösung des Problems sein wird, und daß es der Polizei vor allem mit den anderen noch zur Verfügung stehenden Mitteln gelingt, das Organisierte Verbrechen wirksam zu bekämpfen.

2.4.2 INPOL-Neukonzeption

Das Informationssystem der Polizei **(**INPOL) organisiert als gemeinsames arbeitsteiliges System des Bundes und der Länder die polizeiliche Datenverarbeitung. Das Bundeskriminalamt (BKA) verarbeitet als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen personenbezogene Daten, die es in der Regel nicht selbst erhoben, sondern von den Polizeibehörden der Länder übermittelt bekommen hat. In diesem gemeinsamen Informationssystem werden z. Z. folgende Anwendungsbereicheerfaßt:

- Personen- und Sachfahndung
- Kriminalaktennachweis
- Haftdatei
- Erkennungsdienst
- Arbeitsdateien für besondere Kriminalitätsbereiche
- Falldateien für besondere Kriminalitätsbereiche
- Spurendokumentation im Ermittlungsverfahren.

Als eine Schwachstelle im alten INPOL-System wird seitens der Polizei angesehen, daß keine offene Recherche in allen Dateien möglich ist. Dadurch kann es zu Redundanzen infolge von Mehrfacherfassungenkommen.

Mit der Neukonzeption sollen Mehrfacherfassungen vermieden werden. Dies hat auch aus datenschutzrechtlicher Sicht den Vorteil, daß Datenbestände redundanzfrei geführt und beispielsweise Informationen zu einer Person durchgängig gelöscht werden können. Das neue Konzept sieht einen anwendungsunabhängigen Datenpool vor. Damit ergibt sich technisch die Möglichkeit, zunächst alle personenbezogenen Daten unterschiedslos, ohne Differenzierung ihrer Rolle in einem polizeilichen Vorgang zu speichern. Die Zuordnung der Daten (ob es sich um Beschuldigte oder Opfer, Zeugen oder Hinweisgeber in einem Ermittlungsverfahren handelt) ergibt sich nur aufgrund eines komplexen Beziehungsgeflechtes (hinterlegte Logik) in der Datenbank.

Solche technischen Vereinfachungen können aber auch zur Beeinträchtigung schutzwürdiger Belange von Betroffenen führen. Die in einem anwendungsunabhängigen Datenpool gespeicherten personenbezogenen Daten werden gemeinsam verwaltet und stehen somit grundsätzlich allen Anwendern "zur freien Verfügung". Damit nicht jeder, der Zugriff zu diesem Datenbestand hat, alle Informationen unabhängig von seinen konkreten polizeilichen Aufgaben zur Kenntnis nehmen kann, ist ein differenziertes Zugriffsverfahren vorgesehen. Datenschutzrechtlich ist zu bewerten, daß vielfältige Recherchemöglichkeiten eröffnet werden, wobei noch Aussagen darüber fehlen, auf welche Art von Daten sie sich beziehen sollen. Würden sie sich auf den gesamten Datenbestand erstrecken, also auch auf solche Informationen, die ausschließlich für besondere polizeiliche Zwecke gespeichert werden, bestünde die Gefahr, daß die bereits bei der Datenerhebung bis zur Beendigung des Umgangs mit Daten zu beachtende Zweckbindung (Finalitätsprinzip) unterlaufen wird. Die strikte Wahrung des Zweckbindungsgrundsatzes kann aber ebensowenig außer Betracht bleiben wie die Frage nach der Verantwortlichkeit für den Datenbestand, über die sich in den vorliegenden Unterlagen noch keine nachvollziehbaren Aussagen finden. Ferner sollen Informationen, die nicht gesicherte Erkenntnisse betreffen und bisher in SPUDOK-Verfahren oder PIOS-Anwendungen registriert wurden, in INPOL-Neu abgelegt werden. Hierdurch wird gegenüber dem bisherigen Verfahren die Möglichkeit einer erheblich verbesserten Selektion dieser Datenbestände eröffnet. Es wird möglich sein, Abgleiche in unterschiedlichen SPUDOK-Verfahren durchzuführen. Eine entsprechende Regelung in der Strafprozeßordnung, die eine solche Datenverarbeitung zuließe, ist nicht ersichtlich. Die Freitextrecherche soll erweitert und Bestandteil der INPOL-Neu-Anwendungen werden. Der direkte Zugriff auf Fremdsysteme mittels einer Abfrage soll geschaffen und der Datenbestand des Kriminalaktennachweises (KAN) soll um Daten aus Straftaten (Fallgrundinformationen) erweitert werden.

Mit diesen nur beispielhaft genannten Elementen von INPOL-Neu ist eine erhebliche Qualitätsveränderung der Datenverarbeitung gegenüber dem bisherigen Verfahren verbunden. Daraus ergibt sich die Forderung nach einem adäquaten datenschutzrechtlichen Standard. Das vorliegende Grobkonzept von INPOL-Neu enthält im übrigen außer den allgemein gehaltenen Aussagen zur Zugriffsberechtigung und -kontrolle keine hinreichend präzisen Angaben darüber, nach welchem Modus Zugriffsberechtigungen festgelegt werden. Aus datenschutzrechtlicher Sicht muß jedoch sichergestellt sein, daß Berechtigte nur auf den Datenbestand zugreifen können, der für ihre Aufgabenerfüllung erforderlich ist. Darüber hinaus sollte unabhängig von der Funktion des Benutzers eine differenzierende Zugriffsregelung geschaffen werden.
An dieser Stelle habe ich nur einige datenschutzrechtliche Probleme dargestellt, die sich bei der INPOL-Neu-Konzeption ergeben werden. Abschließend weise ich noch darauf hin, daß alle genannten datenschutzrechtlichen Anforderungen und Regelungen für das INPOL-System auf eine gesetzliche Grundlage (BKA-Gesetz) gestellt werden müssen.

2.4.3 Rückwirkende Erfassung von Fingerabdruckblättern aus dem Beitrittsgebiet

Das BKA beabsichtigt, ca. 30.000 Fingerabdruckblätter aus nach DDR-Recht bewerteten Straftaten nachträglich maschinell im automatisierten Fingerabdruckidentifizierungssystem (AFIS) zu erfassen. Die Landesbeauftragten für den Datenschutz waren an der Bereinigung des Altdatenbestandes in den neuen Ländern nicht beteiligt, da zu diesem Zeitpunkt die Dienststellen noch nicht existierten.
In Mecklenburg-Vorpommern liegen ca. 5100 Fingerabdruckblätter zur beabsichtigten Erfassung vor. Zu prüfen war hier, ob die Fingerabdruckblätter, die vom Landeskriminalamt Mecklenburg-Vorpommern (LKA MV) an das BKA übersandt wurden, rechtsstaatlichen Kriterien genügen. Im einzelnen geht es um Aussonderungsfristen, mangelnde Entsprechung von DDR-Straftatbeständen und Straftaten nach bundesdeutschem Recht und um die Prüfung, ob bei den vorhandenen Fingerabdruckblättern auch ein sogenannter Aktenrückhalt (Vorliegen einer Kriminalakte)existiert.

Ich hatte das LKA um Stellungnahme und einen Sachstandsbericht über die Bereinigung des Altdatenbestandes gebeten. Man teilte mir daraufhin mit, daß die Bereinigung in drei Stufen erfolgt sei. In der dritten Stufe, die anhand der Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien) des Bundes (Stand: August 1981) ab November 1991 erfolgte, wurden alle Fingerabdruckblätter in Listen erfaßt und den kriminalaktenführenden Stellen zur Prüfung zugesandt. In diese Listen wurde eingetragen, ob zu den aufgeführten Fingerabdruckblättern Kriminalaktenrückhalte bestehen. Darüber hinaus wurden bei vorhandenem Aktenrückhalt Angaben zur letzten Straftat (Straftatbestand, Datum der letzten Straftat) gemacht. Anhand dieser Angaben sei eine Aussonderung erfolgt. Lediglich die Fingerabdruckblätter, für die Aktenrückhalt bestanden habe und bei denen die Aufbewahrungsfristen nach den KpS-Richtlinien nicht abgelaufen waren, seien an das BKA gegeben worden. Das LKA teilte aber auch mit, daß 500 dieser Fingerabdruckblätter vom BKA wegen Mängel wieder ausgesondert und zur nochmaligen Überprüfung an das LKA zurückgesandt worden sind.

Ich habe sowohl in die Fingerabdruckblätter als auch in die Kriminalakten Einsicht genommen. Bei der Einsichtnahme in die Fingerabdruckblätter und in die Listen zur Bereinigung dieser Blätter waren folgende Mängel zu konstatieren:

1. Es fehlen generell Angaben zum Strafmaß.

2. In einigen Fällen, in denen Personen zu Freiheitsstrafen verurteilt worden waren, fehlte jeweils das Datum der Haftentlassung.

3. Die Angaben der Straftaten waren zum Teil unvollständig.

Bei der Festsetzung von Fristen für die Aussonderung aus der Fingerabdruckblättersammlung ergeben sich wegen der fehlenden Angaben zum Strafmaß Probleme bei der Bewertung der Einzelfälle. Es können ohne diese Angaben keine Einschätzungen dahingehend erfolgen, ob möglicherweise der vorliegende Einzelfall eine Verkürzung der Frist nach den KpS-Richtlinien erfordert, z. B. in Fällen von geringerer Bedeutung. Diese Verfahrensweise kann zu einer unzulässigen Aufbewahrung von Fingerabdruckblättern in der Sammlung über die eigentliche Frist hinaus führen. Als Kriterium für eine Aussonderung wird u.a. auch der Entlassungszeitraum aus einer Justizvollzugsanstalt festgesetzt. In den geprüften Fällen war jedoch lediglich der Zeitpunkt der Straftat, nicht jedoch das Haftentlassungsdatum angegeben, so daß auch in diesen Fällen keine ordnungsgemäße Fristbestimmung möglich ist. Weil nicht in allen Fällen sämtliche Straftaten aufgeführt sind, ist es auch nicht immer möglich, Einschätzungen darüber zu treffen, ob es sich um einen Fall geringerer Bedeutung handelt und hierfür möglicherweise verkürzte Aussonderungsfristen in Betracht kommen. Ferner wurde beim Durchsehen der zu den Fingerabdruckblättern gehörenden Kriminalakten festgestellt, daß - im Vergleich zum Strafgesetzbuch der Bundesrepublik Deutschland - in der DDR für gleiche oder vergleichbare Delikte wesentlich höhere (Freiheits-) Strafen verhängt worden waren. Da die Dauer der Aufbewahrung von Fingerabdruckblättern grundsätzlich von der Schwere der Straftat ausgeht und eine Einzelfallprüfung in den Kriminalpolizeiinspektionen nicht stattfindet, existiert eine Anzahl von Fällen, in denen Fingerabdruckblätter zu einem früheren Zeitpunkt in eine gesperrte Sammlung hätten übernommen werden müssen.

Insgesamt bleibt festzustellen, daß zwar Bereinigungen durchgeführt worden sind, diese aber nicht in allen Fällen datenschutzrechtlichen Anforderungen genügen. Ich stand daher vor der Überlegung, das LKA aufzufordern, sämtliche Fingerabdruckblätter vom BKA zurückzunehmen und diese zur Einzelfallprüfung an die Kriminalpolizeiinspektionen weiterzuleiten. Ich habe davon jedoch Abstand genommen, da wegen des Zeitablaufes und diverser anderer organisatorischer Probleme eine Einzelfallüberprüfung zum jetzigen Zeitpunkt kaum mehr durchführbar ist. Positiv zu vermerken ist, daß im Gegensatz zu anderen Bundesländern jedenfalls ein Kriminalaktenrückhalt existiert und insofern die Erfassung in AFIS nicht zu bemängeln ist.

2.4.4 Kriminalakten

Im Zuge der Überprüfung der Fingerabdruckblätter wurden auch hinsichtlich der Führung der Kriminalakten Mängel festgestellt. Letztere enthalten in der Regel Hinweise und Unterlagen aus strafrechtlichen Ermittlungsverfahren gegen den Betroffenen, Lichtbilder, Fingerabdrücke und sonstige erkennungsdienstliche Unterlagen zur Person. Der momentane Bestand an Kriminalakten in der Kriminalpolizeiinspektion Schwerin beläuft sich auf ungefähr 18.000 Akten. Eine stichprobenartige Einsichtnahme in die Akten ergab folgendes Bild:

Die meisten Akten, die noch zu DDR-Zeiten angelegt wurden, enthalten sogenannte Datenprotokolle, in denen sehr ausführlich über Persönlichkeitsmerkmale, äußere Erscheinung und Auffälligkeiten der jeweiligen Person berichtet wird. So finden sich z. B. detaillierte Angaben über das Auftreten in Gruppen, Hobbys, Freizeitverhalten und sexuelle Gewohnheiten.

Rechtsgrundlage für die Verarbeitung und Nutzung personenbezogener Daten sind §§ 36 und 37 SOG MV. Danach können personenbezogene Daten nur verarbeitet und genutzt werden, soweit dies zur Erfüllung der jeweiligen polizeilichen Aufgabe erforderlich ist. Die Erforderlichkeit ist jedoch bei einer Vielzahl der abgefragten Persönlichkeitsmerkmale in keiner Weise gegeben und damit ist der weitere Verbleib solcher Datenprotokolle im Hinblick auf den Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen unzulässig. Anläßlich der Tagung des Arbeitskreises "Datenschutz in den neuen Bundesländern" am 12. Oktober 1993 haben die Datenschutzbeauftragten des Bundes und der neuen Länder einschließlich Berlin diesbezüglich empfohlen, die nicht zulässigen Fragen und die entsprechenden Antworten zu schwärzen.

In einer Akte befand sich ein mehrere Seiten umfassendes Vernehmungsprotokoll, in dem Fragen zur persönlichen und gesellschaftlichen Entwicklung, zu persönlichen Einstellungen, zum Verhältnis zu Staatsfeiertagen in der DDR und ähnliche Fragen gestellt wurden. Hintergrund dieses Falles war die Beleidigung eines hochrangigen Vertreters der NVA (Oberstleutnant) im Rahmen der Einberufung zum Grundwehrdienst. Für diesen Fall waren die Aufbewahrungsfristen nach den KpS-Richtlinienbereits überschritten.
Es existiert zwar eine Dienstanweisung für die Führung von Kriminalakten (KA-Richtlinien), die vom LKA verfügt und ab dem 01.04.1993 in Kraft gesetzt wurde. Diese sehr allgemein gehaltene Regelung gibt jedoch keinen Aufschluß darüber, welche Unterlagen aus den Altakten zu entfernen und zu archivieren sind. Laut Auskunft des LKA MV existieren keine Richtlinien, die das Verfahren zur Bereinigung der Kriminalaktennäher regeln.
Es bleibt festzuhalten, daß eine ordnungsgemäße Bereinigung der Kriminalakten noch nicht erfolgt ist.

2.4.5 SPUDOK-Datei "Rostock"

Vom Landeskriminalamt Mecklenburg-Vorpommern wurde mir die Errichtungsanordnung zur Spurendokumentationssystem (SPUDOK)-Datei "Rostock" zur Stellungnahme übersandt.
SPUDOK-Dateien werden in der Regel temporär und fallbezogen angelegt. Ihr Kennzeichen ist es, daß das Spuren- und Hinweisaufkommen eines Falles einschließlich aller darin enthaltenen Namen vollständig gespeichert und infolge der weitgehend formatfreien Erfassung mit beliebigen Abfragebegriffen ausgewertet werden kann. SPUDOK-Verfahren werden bei fast allen großen Ermittlungsverfahren eingesetzt, so auch bei der Aufklärung der ausländerfeindlichen Ausschreitungen um die Zentrale Aufnahmestelle für Asylbewerber in Mecklenburg-Vorpommern (ZAST) im August 1992 in Rostock-Lichtenhagen.

Ich hatte seinerzeit empfohlen, die Errichtungsanordnung in folgenden Punkten zu ändern bzw. zu konkretisieren:

- Die Straftaten, wegen derer ermittelt wurde, waren nur unzureichend benannt. Es waren zwar Straftaten wie die Fortführung einer für verfassungswidrig erklärten Partei und der Verstoß gegen ein Vereinigungsverbot aufgeführt, bei den Ausschreitungen wurde jedoch (vorwiegend) wegen anderer Delikte wie Brandstiftung, schwere Brandstiftung, versuchter Mord und Körperverletzung ermittelt. Daher habe ich dem LKA geraten, den Terminus "und andere Straftaten mit extremistischer, gewaltgeneigter Zielsetzung" näher auszuformulieren. Rechtsgrundlage ist § 47 SOG MV.

- Datenschutzrechtliche Bedenken bestanden auch hinsichtlich der Speicherung von Daten über Kontakt- und Begleitpersonen von Beschuldigten. Sogenannte "Kontakt- und Begleitpersonen" können meines Erachtens im Zuge von Ermittlungsmaßnahmen nur dann in Betracht kommen, wenn sie z. B. unwissende Nachrichtenmittler zwischen Beschuldigten sind. Auch in diesem Falle wären sie jedoch Zeugen im strafprozessualen Sinne und können daher auch als solche in der Datei benannt werden.

- Weiterhin habe ich hinsichtlich der Frage der Datenübermittlung bzw. des Zugriffes empfohlen, in Form von einer Protokollierung zu gewährleisten, daß überprüft werden kann, wer wann auf welche Daten zugegriffen bzw. sie übermittelt hat.

- Ein weiterer kritischer Punkt ist häufig auch die Einhaltung der Speicherungshöchstdauer/Prüffristen. So halte ich die Löschung solcher Spuren, die sich als irrelevant erwiesen haben, für notwendig. Dies scheint jedoch das seit zwei Jahrzehnten beim BKA installierte SPUDOK-System nicht zu leisten. Wie der Hamburgische Datenschutzbeauftragte bei einer Überprüfung festgestellt hat, kann keine Einzelfallöschung vorgenommen werden. Da die Länder ebenfalls dieses System für ihre Zwecke nutzen, ist die Forderung beim LKA Mecklenburg-Vorpommern allein nicht durchzusetzen. Ich werde mich deshalb beim BfD für die Lösung dieses Problems einsetzen.

2.4.6 Auswahluntersuchung von Bewerbern für die Bereitschaftspolizei

Wer Polizeibeamter werden will, sollte physisch und psychisch gesund sein. Diese Forderung erscheint zunächst durchaus vernünftig. Wenn aber von den Bewerbern schon vor ihrer polizeiärztlichen Auswahluntersuchung eine Bescheinigung der Krankenkasse verlangt wird, in der diese die exakten Versicherungszeiten, sämtliche Arbeitsunfähigkeitszeiten sowie Krankenhaus-, Kur- und Heilstättenaufenthalte mit den entsprechenden Diagnosen einzutragen hat, dann ist das aus datenschutzrechtlicher Sicht höchst bedenklich.

Daß dieses Verfahren in einem anderen Bundesland so praktiziert wurde und ich davon Kenntnis erhielt, veranlaßte mich, die Vorgehensweise bei der Bereitschaftspolizei des Landes Mecklenburg-Vorpommern zu überprüfen.
Das Landespolizeiamt teilte mir auf meine Anfrage hin mit, daß die Auswahluntersuchung für Bewerber der Polizei auf der Grundlage der Polizeidienstvorschrift (PDV) 300 erfolgt. Danach erhält der Bewerber einen Fragebogen, auf dem er die bisherigen Erkrankungen bzw. gesundheitlichen Störungen selbst einzutragen hat. Auf einem weiteren Bogen wird der Hausarzt gebeten, Erkrankungen der letzten fünf Jahre einzutragen (Art und Dauer der Krankheit). Weiterhin hat der Bewerber einen aktuellen Augen- und Zahnarztbefund einzureichen. Aufgrund dieser Daten entscheidet der Polizeiarzt, welche zusätzlichen Untersuchungen im Vorfeld zu erbringen sind oder ob bereits eine Vorbeschädigung vorliegt, die eine Polizeidienstunfähigkeit bedingt. Die Bewerber werden jedoch nicht aufgefordert, schon vor der polizeiärztlichen Auswahluntersuchung eine Bescheinigung ihrer Krankenkasse einzuholen.
Durch das abgestufte Verfahren vermeidet die Landespolizei Mecklenburg-Vorpommern eine überflüssige Datenerhebung und kommt damit dem stets auch beim Fragerecht des Arbeitgebers zu beachtenden Grundsatz der Verhältnismäßigkeit nach. Aus datenschutzrechtlicher Sicht war die Verfahrensweise daher nicht zu beanstanden.

2.4.7 Können Sie mir mal sagen, wo ich wohne?

Selbst in einer Kleinstadt, wo sich die Leute zumeist sehr gut kennen und viel persönliches voneinander wissen, ist von den öffentlichen Stellen der Datenschutz zu beachten. Folgende Eingabe lag mir zur Bearbeitung vor:

Ein Bürger hatte beim zuständigen Ordnungsamt eine Auskunftssperre nach § 34 Abs. 5 LMG erwirkt. Danach ist jede Melderegisterauskunft unzulässig, wenn der Betroffene der Meldebehörde das Vorliegen von Tatsachen glaubhaft gemacht hat, die die Annahme rechtfertigen, daß ihm oder einer anderen Person durch eine solche Auskunft eine Gefahr für Leib, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Rechte erwachsen kann. Trotz der Auskunftssperre waren verschiedene Personen an die neue Adresse des Bürgers gelangt. Dieser hegte nun den Verdacht, daß die örtliche Polizeibehörde, mit der er gelegentlich in Berührung kam und die somit seine Anschrift kannte, diese weitergegeben hatte. Deshalb stellte er die Polizei auf die Probe, rief unter falschem Namen an und erkundigte sich nach seiner eigenen Adresse. Die Polizei gab ihm bereitwillig Auskunft.

Ich habe den Fall folgendermaßen bewertet:

Gem. § 39 SOG MV darf die Polizei personenbezogene Daten nur zu dem Zweck übermitteln, zu dem sie gespeichert worden sind, soweit gesetzlich nichts anderes bestimmt ist. Abweichend hiervon ist eine Datenübermittlung unter den in § 39 Abs. 1 Nr. 1 - 3 SOG MV genannten Voraussetzungen, u.a. zu Zwecken der Gefahrenabwehr, zulässig. Eine Rechtsgrundlage für die im vorliegenden Fall erfolgte Auskunftserteilung war nicht vorhanden. Ich habe daher den Dienststellenleiter der Polizeiinspektion gebeten, auch die anderen Polizeibeamten seiner Dienststelle darüber zu informieren, daß personenbezogene Daten nur in den von § 39 SOG MV vorgesehenen Fällen weitergegeben werden dürfen und daß es Aufgabe der Meldebehörden ist, Anschriften von Bürgern im Rahmen von Melderegisterauskünften bekanntzugeben. In diesem Zusammenhang ist auch nicht entscheidend, ob ein Polizeibeamter die Anschrift einer Person aus eigenem Wissen kennt.

Der Dienststellenleiter der Polizeiinspektion hat seine Mitarbeiter im Hinblick auf die oben geschilderte Problematik datenschutzrechtlich belehrt. Seither sind mir keine weiteren Vorkommnisse dieser Art bekannt geworden.

2.5 Verkehr

2.5.1 Weitergabe personenbezogener Daten von Führerscheinbewerbern

Angeregt durch den Sächsischen Datenschutzbeauftragten habe ich Vordrucke, die in Mecklenburg-Vorpommern in Fahrerlaubnisangelegenheiten Verwendung finden, dahingehend überprüft, ob sie den Anforderungen des Datenschutzrechtes entsprechen. Es handelt sich um zwei Vordrucke des Verlages Heinrich Vogel GmbH München, die als "Gutachten über Ihre Eignung zum Führen von Fahrzeugen" und "Einverständniserklärung für die Erstellung eines Gutachtens über meine Eignung zum Führen von Kraftfahrzeugen" bezeichnet sind.
Die Vordrucke werden verwendet, wenn bei einem Führerscheinbewerber Tatsachen bekannt werden, die Bedenken gegen seine Eignung zum Führen von Kraftfahrzeugen begründen. In diesem Fall kann die Verwaltungsbehörde gemäß § 12 Abs. 1 der Straßenverkehrs-Zulassungs-Ordnung (StVZO) die Beibringung eines solchen Gutachtens in Form eines amts- oder fachärztlichen Gutachtens, eines Gutachtens eines amtlich anerkannten Sachverständigen oder Prüfers für den Kraftfahrzeugverkehr oder eines Gutachtens einer amtlich anerkannten medizinisch-psychologischen Untersuchungsstelle (MPU) anordnen. Dasselbe gilt gemäß § 15b Abs. 2 StVZO hinsichtlich eines Inhabers einer bereits vorhandenen Fahrerlaubnis, wenn bei diesem Anlaß zu der Annahme besteht, daß er zum Führen eines Kraftfahrzeuges ungeeignet oder nur noch bedingt geeignet ist. Im Falle des § 15c Abs. 3 StVZO - Entziehung der Fahrerlaubnis wegen wiederholten Verstoßes gegen verkehrsrechtliche Vorschriften oder Strafgesetze - muß die Verwaltungsbehörde sogar anordnen, daß vor der Neuerteilung einer Fahrerlaubnis die Beibringung eines Gutachtens erfolgt.

Auf dem Vordruck "Gutachten über Ihre Eignung zum Führen von Fahrzeugen" wird dem Führerscheinbewerber bzw. -inhaber mitgeteilt, warum eine Begutachtung bei ihm erforderlich ist, bei welchem Gutachter und bis zu welchem Termin sie erfolgen soll und welche Folgen es für ihn haben kann, wenn er nicht in die Begutachtung einwilligt.
Zu bemängeln war auf dem Vordruck insbesondere die gemäß § 7 Satz 5 DSG MV erforderliche Darstellung der Rechtsfolgen. Zum einen wurde nicht erwähnt, daß die Weigerung des Betroffenen, ein Gutachten beizubringen, nur dann zu einer Fahrerlaubnisversagung bzw. -entziehung führen kann, wenn diese Weigerung ohne ausreichenden Grund erfolgte. Der Betroffene muß aber - damit für ihn wirkliche Entscheidungsfreiheit besteht - bei seiner Einwilligung auch darüber aufgeklärt sein, daß es ausreichende Gründe geben kann, die eine Verweigerung rechtfertigen. Zum anderen stand auf dem Vordruck, daß die Verwaltungsbehörde bei einer Weigerung, das Gutachten beizubringen, zu der Annahme der Ungeeignetheit des Betroffenen gelangen muß. Diese Formulierung ist jedoch unrichtig; die Verwaltungsbehörde kann (sie muß aber nicht!) im Rahmen ihrer eigenen Urteilsbildung zu der berechtigten Annahme kommen, daß der Betroffene ungeeignet ist, wenn er sich ohne ausreichenden Grund weigert, der geforderten Begutachtung zuzustimmen. Die Verwaltungsbehörde darf aber aus der Nichtvorlage des Gutachtens nur dann auf die Nichteignung des Fahrerlaubnisbewerbers bzw. -inhabers schließen, wenn begründete Zweifel bestehen. Dies wurde zuletzt in einer Entscheidung des Bundesverfassungsgerichtes vom 24.06.1993 festgestellt. Dort hatte das Gericht entschieden, daß die Annahme der Verwaltungsbehörde, daß der Beschwerdeführer häufiger oder gar regelmäßig Haschisch oder andere Drogen zu sich nehme und dadurch zum Führen eines Kraftfahrzeuges ungeeignet sei, nicht damit gerechtfertigt werden kann, daß die Polizei in seinem abgestellten Fahrzeug 0,5 g Haschisch sichergestellt hat und der Haschisch-Konsum dem Beschwerdeführer deutlich anzumerken war.

Der Vordruck "Einverständniserklärung für die Erstellung eines Gutachtens über meine Eignung zum Führen von Kraftfahrzeugen" ist ebenfalls datenschutzrechtlich bedenklich. Er ist eine Anlage zu dem erstgenannten Vordruck. Auf ihm soll der Führerscheinbewerber bzw. -inhaber zum einen die Gutachterstelle, für die er sich entschieden hat, mitteilen, und zum anderen sein Einverständnis zur Begutachtung und zur Übersendung der für die Begutachtung erforderlichen Unterlagen an die entsprechende Gutachterstelle erklären.
Hinsichtlich dieser "Einverständniserklärung" bemängelte ich, daß die Formulierung, welche Unterlagen durch die Verwaltungsbehörde an die Gutachterstelle übersendet werden, zu pauschal war. Sie ließ nicht erkennen, daß nach Ziffer II, Nr. 5 der Eignungsrichtlinien grundsätzlich nur diejenigen Vorgänge übermittelt werden dürfen, die im Hinblick auf die gestellten Fragen Aufschluß über den Betroffenen geben können. Auch nur insoweit darf dann die Verwaltungsbehörde die Einwilligung des Betroffenen zur Übersendung von Unterlagen an die Gutachterstelle einholen.
Außerdem war auf diesem Vordruck an der Stelle, an der der Betroffene sein Einverständnis erklären sollte "mit der Mitteilung von Eignungsmängeln, die anläßlich der Untersuchung bekannt werden, aber nicht anlaßbezogen sind", in dem dazugehörigen Kästchen bereits ein Kreuz eingedruckt. Diese "erzwungene" Einwilligung ist deshalb unzulässig, weil die Verwaltungsbehörde - dem Grundsatz der Verhältnismäßigkeit entsprechend - als Hilfsmittel für ihre eigene Urteilsbildung vom Betroffenen nur ein anlaßbezogenes Gutachten verlangen kann. Für den Betroffenen, der eine derartige "automatische" Einwilligung nicht geben will, bestand daher auf dem Vordruck theoretisch nur die Möglichkeit, das vorhandene Kreuz durchzustreichen.

Ich habe meine Bedenken gegen beide Vordrucke unserem Wirtschaftsministerium mitgeteilt und empfohlen, daß in Zukunft von den zuständigen Stellen nur noch solche Vordrucke verwendet werden, die den datenschutzrechtlichen Anforderungen genügen. Daraufhin erhielt ich die Antwort, daß der Verlag Heinrich Vogel GmbH über meine vorgetragenen datenschutzrechtlichen Bedenken informiert worden sei und das Wirtschaftsministerium vorläufig keine Nachbestellung der alten Formulare vornehmen wird. Unmittelbar danach meldete sich der Verlag Heinrich Vogel GmbH bei mir, um mitzuteilen, daß meine Bedenken hinsichtlich der Vordrucke derzeit überprüft werden. Wenige Tage später erhielt ich die dort ausgearbeiteten Änderungsvorschläge. Der Verlag hat meine Forderungen in die neuen Formulare eingearbeitet.

2.5.2 Kein Pardon für Parksünder

Noch vor einiger Zeit war es in Mecklenburg-Vorpommern kein großes Risiko, ein "Knöllchen", welches man sich z. B. wegen falschen Parkens eingehandelt hatte, einfach wegzuwerfen. Eine solche Ordnungswidrigkeit wurde seitens der zuständigen Behörden häufig nicht weiter geahndet. Nach Einführung des automatisierten Ordnungswidrigkeitsverfahrens (OWI) ist jedoch jedem Parksünder dringend davon abzuraten.

Zu folgendem Sachverhalt war ich aufgefordert worden, Stellung zu nehmen:

Der Innenminister unseres Landes plante die Einführung des automatisierten OWI-Verfahrens. Das Verfahren wird von der Hansestadt Lübeck übernommen und vom Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ) bezüglich landeseigener Besonderheiten angepaßt. Nach dem Testbetrieb durch das DVZ sollte eine mehrwöchige Testphase durch die zukünftigen Anwender (zunächst zwei Polizeidirektionen) mit Testdaten erfolgen, um mögliche Fehlerquellen zu beseitigen und um die Anwender zu schulen. Im Anschluß daran war geplant, eine auf zwei Monate begrenzte Testphase mit maximal 2000 Echtdatensätzen durchzuführen. Nur eine Mitarbeiterin des DVZ sollte dabei die vollen Zugriffsrechte auf den Echtdatenbestand erhalten, um die Funktionsfähigkeit der Software ständig kontrollieren und mögliche Fehler im Verfahren feststellen zu können. Die Notwendigkeit der Benutzung von Echtdatensätzen in der Testphase wurde damit begründet, daß ein vollständiger Softwaretest nur so möglich sei. Der Datenträgeraustausch mit dem Kraftfahrt-Bundesamt (KBA) auf der Basis von Magnetbandkassetten mit Halteranfragen sei nur mit Echtdaten sinnvoll durchführbar.
Ich habe gegenüber dem Innenministerium die Auffassung vertreten, daß die Verwendung echter personenbezogener Daten für die Überprüfung von Software unzulässig ist. Im übrigen sind sich Fachleute ohnehin darin einig, daß Echtdatenbestände für Softwaretests praktisch weniger geeignet sind als gut durchdachte Testdatenbestände, da nur im letzteren Fall alle vorhersehbaren Sonderfälle sicher berücksichtigt werden können. Zudem ist es nicht mit der Pflicht zur ordnungsgemäßen Verarbeitung personenbezogener Daten vereinbar, wenn diese mit Programmen erfolgt, bei denen die Richtigkeit der Ergebnisse aus der Verarbeitung richtiger Daten noch in Zweifel gezogen werden muß. Ich verlangte daher, Softwaretests mit Testdatenbeständen durchzuführen und den Test erst dann als abgeschlossen anzusehen, wenn die Software mit diesen Testdatenbeständen fehlerfrei läuft.

Von meinen vorgenannten Überlegungen wird die Praxiserprobung fertiger, ausgetesteter und vorläufig freigegebener Programmsysteme mit Echtdaten und im Echtbetrieb nicht erfaßt.
Im vorliegenden Fall der Einführung des automatisierten Ordnungswidrigkeitsverfahrens war daher die entscheidende Frage, ob das Verfahren als ausgetestet bzw. vorläufig freigegeben bezeichnet werden kann, bevor der auf zwei Monate geplante Betrieb (auch als Testphase bezeichnet) mit Echtdaten beginnen konnte. Die Präsentation des OWI-Verfahrens durch das DVZ hatte jedoch den Eindruck vermittelt, daß noch eine engere Abstimmung mit den Anwendern notwendig ist, um Problemfälle abzuklären.

Insofern konnte ich einem Betrieb mit Echtdaten lediglich unter der Voraussetzung zustimmen, daß die Problemfälle weitestgehend im Vorfeld gelöst worden sind und der Test mit eigenen Testdatenbeständen bzw. solchen des KBA erfolgreich abgeschlossen worden ist. Ich begrüße es ausdrücklich, daß der Innenminister unseres Landes meinen o. g. Empfehlungen gefolgt ist.

2.6 Verfassungsschutz

2.6.1 Datenschutz und Verfassungsschutz

Aufgabe des Verfassungsschutzes ist es, die freiheitlich demokratische Grundordnung, den Bestand und die Sicherheit des Bundes sowie der Länder zu schützen. Aufgabe des Datenschutzes ist es, das Recht des einzelnen zu schützen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Der Datenschutz ist daher gerade im Zeitalter einer zunehmenden Technisierung bestrebt, den Umgang mit Daten für den einzelnen transparent zu machen. Der Bürger hat einen Anspruch darauf zu wissen, wer was wann über ihn gespeichert hat.

Der Verfassungsschutz hingegen sammelt Informationen über Personengruppen, die durch zielgerichtete Bestrebungen die freiheitlich demokratische Grundordnung beseitigen bzw. beeinträchtigen wollen, ohne das dies transparent wird. Da potentielle Verfassungsfeinde keine Kenntnis darüber erhalten sollen, daß sie beobachtet werden, arbeitet der Verfassungsschutz notwendigerweise im geheimen. Diese Art der Nachrichtenbeschaffung und Beobachtung kontrastiert (nicht widerspricht!) mit dem Anliegen des Datenschutzes, Datenflüsse transparent zu machen. Ich möchte dies anhand zweier Beispiele erläutern, die in der Praxis immer wieder zwischen Datenschützern und Verfassungsschützern diskutiert werden:

In den Verfassungsschutzgesetzen werden häufig Generalklauseln verwendet, die aus datenschutzrechtlicher Sicht oft nicht den Anforderungen an klar umrissene Eingriffsbefugnisse genügen. So ist im Verfassungsschutzgesetz von Mecklenburg-Vorpommern der Begriff "Bestrebung" gegen die freiheitliche demokratische Grundordnung nicht hinreichend genug konkretisiert. Es sollte klargestellt werden, daß eine für den Verfassungsschutz beachtliche Bestrebung eine aktiv kämpferische Haltung gegenüber der bestehenden Verfassungsordnung voraussetzt.

Ein weiteres Spannungsfeld liegt in der Regelung des Rechts auf Akteneinsicht und Auskunft des Betroffenen in Bezug auf die beim Verfassungsschutz über ihn vorgehaltenen Daten. Nach dem Landesverfassungsschutzgesetz muß der Betroffene bei seinem Auskunftsbegehren auf einen konkreten Sachverhalt hinweisen und ein besonderes Interesse an einer Auskunft darlegen. Zudem kann die Auskunft in einer Reihe von Fällen verweigert werden. Exemplarisch sei hier die Auskunftsverweigerung genannt, wenn eine Gefährdung der Aufgabenerfüllung durch die Auskunftserteilung zu befürchten ist. Es ist zwar verständlich, warum aus bestimmten Gründen, z. B. auch bei Gefährdung der öffentlichen Sicherheit, die Auskünfte unterbleiben müssen. Nicht einzusehen ist jedoch, warum es erforderlich sein soll, daß der Auskunftssuchende einen konkreten Sachverhalt und ein besonderes Interesse an der Auskunft darzulegen hat. So reicht es zur Darlegung des "besonderen Interesses" nicht aus, wenn der Bürger schlicht wissen will, was der Verfassungsschutz bei welcher Gelegenheit über ihn gespeichert hat. In der Praxis der Verfassungsschutzbehörden wird der Petent vielmehr aufgefordert darzulegen, weshalb er einen Anlaß zu haben meint, beim Verfassungsschutz registriert zu sein. Der Petent läuft damit unter Umständen Gefahr, sich selbst zu bezichtigen, obwohl er lediglich eine Auskunft haben möchte.
Auf diese Praxis der Auskunftserteilung werde ich anläßlich eines für den nächsten Berichtszeitraum geplanten Informations- und Kontrollbesuches ein besonderes Augenmerk legen.

2.6.2 Sicherheitsüberprüfungsgesetz

Mir lag der Entwurf eines Gesetzes über die Voraussetzung und das Verfahren von Sicherheitsüberprüfungen des Bundes (Sicherheitsüberprüfungsgesetz - SÜG), - BR-Drs. 97/93, Stand: Februar 1993 - zur Stellungnahme vor.

Ziel des Gesetzes ist es, die Voraussetzungen und das Verfahren zur Durchführung einer Sicherheitsüberprüfung, die derzeit lediglich in Verwaltungsvorschriften geregelt sind, auf eine bereichsspezifischeund normenklare Rechtsgrundlage zu stellen.

Die Forderung nach einer gesetzlichen Grundlage hätte im Hinblick auf die Eingriffe in das informationelle Selbstbestimmungsrecht, die mit einer Sicherheitsüberprüfung notwendigerweise verbunden sind, aus der Sicht der Datenschutzbeauftragten längst umgesetzt werden müssen. Im wesentlichen regelt der Gesetzentwurf, wann eine Sicherheitsüberprüfung erforderlich ist. Sie wird abgestuft durchgeführt. Je nachdem, ob der zu Überprüfende Zugang zu VS - VERTRAULICH-, GEHEIM- oder STRENG GEHEIM-Dokumenten erhalten soll. Die Sicherheitsüberprüfung ist abhängig von der vorherigen Zustimmung des Betroffenen.

Ich werde im folgenden nur auf einige wenige Punkte aus meiner Stellungnahme eingehen:

1. Ich habe empfohlen, den Begriff "eheähnliche Lebensgemeinschaften" klarer - unter Berücksichtigung des Zeitraumes des Bestehens - zu definieren. Diese Forderung ist insbesondere im Zusammenhang mit § 13 Abs. 1 Nr. 9 des Gesetzentwurfes zu sehen. Denn dann hat der Betroffene in der Sicherheitserklärung auch die Namen von im Haushalt lebenden Personen über 18 Jahren anzugeben.

2. Laut Gesetzesbegründung ist die Beschreibung der Umstände, die ein Sicherheitsrisiko im Sinne des Sicherheitsüberprüfungsgesetzes sind, ein Kernstück dieses Gesetzes. Daher sollte die Vorschrift insbesondere an dieser Stelle präziser gefaßt werden, beispielsweise durch Aufzählung von Kriterien, die Zweifel an der Zuverlässigkeit des Betroffenen begründen. Angesichts der Auswirkungen für den Betroffenen, als Sicherheitsrisiko zu gelten, sehe ich hier unbedingt Regelungsbedarf.

3. Es ist klarzustellen, daß die nächst höhere Art der Sicherheitsüberprüfung zur erfolgen darf, wenn der Betroffene dazu seine Zustimmung gibt, denn sie stellt eine höhere Eingriffsintensität in seine Privatsphäre dar. Deshalb reicht es nicht aus, wenn die ursprünglich gegebene Zustimmung zur Sicherheitsüberprüfung nach Ermessen der Behörde ausgedehnt wird. Im gleichen Zuge sollte auch die Durchführung von Einzelmaßnahmen der nächst höheren Art der Sicherheitsüberprüfung ebenfalls von der Zustimmung des Betroffenen abhängig gemacht werden.

4. Die in der Sicherheitsüberprüfung anzugebenden Daten sind auf ihre Erforderlichkeit hin zu überprüfen. Es sollte eine differenziertere Ausgestaltung nach den jeweiligen Prüfungsstufen erfolgen. Kritisch anzumerken ist, daß bei der einfachen Sicherheitsüberprüfung fast im gleichen Ausmaß wie für die nächst höhere Überprüfungsstufe Angaben vom Betroffenen verlangt werden.

5. Die sehr sensiblen Angaben, die bei der Sicherheitsüberprüfung erhoben und ermittelt werden, unterliegen einer strengen Zweckbindung. Der Begriff "Straftaten von erheblicher Bedeutung" ist zu konkretisieren - z. B. durch eine abschließende Aufzählung von Straftaten. Andernfalls ist nicht sichergestellt, für welche Straftaten im einzelnen Daten aus der Sicherheitsüberprüfung an die Strafverfolgungsbehörden weitergegeben werden dürfen.

6. Das Recht auf Akteneinsicht sollte nicht - wie im vorliegenden Gesetzentwurf geschehen - restriktiv gehandhabt werden. Dieses Recht ist eine wesentliche Voraussetzung für die Gewährleistung des informationellen Selbstbestimmungsrechts. Es sind daher die Gründe für eine eventuelle Auskunftsverweigerung aktenkundig zu machen. Die anfragende Person sollte auf die Rechtsgrundlage für das Fehlen der Begründung zur Einsichtnahme hingewiesen werden und darauf, daß sie sich in derartigen Fällen an den Bundesbeauftragten für den Datenschutz wenden könne.

Der Deutsche Bundestag hat am 02. Dezember 1993 das Sicherheitsüberprüfungsgesetz beschlossen. Einige Forderungen der Datenschutzbeauftragten sind darin berücksichtigt; so sind z.B. hinsichtlich des Umfangs der Personen, die mit überprüft werden, nur noch "Ehegatte" und "Partner" geblieben, aber nicht der oder die Verlobte. Hinsichtlich des Auskunftsrechtes, des Akteneinsichtsrechtes und auch der Verankerung des Zweckbindungsgrundsatzes bleibt das Gesetz hinter den von den Datenschutzbeauftragten aufgestellten Anforderungen zurück.

2.6.3 Bitte mehr Sensibilität bei Sicherheitsüberprüfungen

Nach den geltenden "Richtlinien für die Sicherheitsüberprüfung von Personen im Rahmen des Geheimschutzes" - Sicherheitsrichtlinien / SiR MV vom 15. Februar 1991 - II / S - sind die staatlichen Stellen verpflichtet, Sicherheitsvorkehrungen zum Schutze von im öffentlichen Interesse geheimhaltungsbedürftigen Tatsachen, Gegenständen oder Erkenntnissen zu treffen (zum grundsätzlichen Erfordernis eines Sicherheitsüberprüfungsgesetzes s.o. 2.6.2).

In einem Fall habe ich die Vorgehensweise der Verfassungsschutzbehörde unseres Landes als mitwirkende Behörde kritisiert. Es ging um die Überprüfung einer Sekretärin. Für diese fand die sogenannte Ü2 (erweiterte Sicherheitsüberprüfung) gem. Nr. 10 der o. g. Richtlinien Anwendung. Danach kann als Maßnahme - soweit ein sicherheitserheblicher Sachverhalt gem. Nr. 10 Abs. 2 i.V.m. Nr. 9 Abs. 3 Ziffer 4 b vorliegt - der Verfassungsschutz auch eine sogenannte "andere Person" zu der zu überprüfenden Person befragen. Die Sekretärin hatte eine Freundin als sogenannte "andere Person" benannt.

Die Kontaktaufnahme zwischen dem Mitarbeiter der Verfassungsschutzbehörde und der Referenzperson verlief nicht ganz reibungslos. Die Freundin der Sekretärin wollte sich, was sie für ihr gutes Recht hielt, im Innenministerium zunächst einmal erkundigen, ob der betreffende Mitarbeiter dort überhaupt bekannt sei. Sie erhielt eine negative Auskunft und teilte ihre Bedenken dem betreffenden Mitarbeiter des Verfassungsschutzes mit, als der später bei ihr anrief. Aufgrund weiterer Unstimmigkeiten kam es auch nicht zu einer Verabredung an einem neutralen Ort. Statt dessen verabschiedete sich der Mitarbeiter am Telefon mit den Worten: "Ich melde mich bei Ihnen im Amt". Er erschien dort später. Es entstand wieder ein Wortwechsel, in welchem die Freundin letztendlich deutlich zum Ausdruck brachte, daß sie nun nicht mehr befragt werden möchte. Daraufhin führte der Mitarbeiter des Verfassungsschutzes ein Gespräch mit dem unmittelbaren Vorgesetzten der Freundin, der dann seinerseits ein Gespräch mit dem Leiter des Amtes suchte. Über den Inhalt dieser Gespräche besteht keine Einigkeit. Für die Bewertung des Falles aus datenschutzrechtlicher Sicht erscheint mir das auch nicht wesentlich.

Für die Durchführung der erweiterten Sicherheitsüberprüfung kam als Rechtsgrundlage § 5 Abs. 2 Landesverfassungsschutzgesetz - LVerfSchG - i.V.m. Nr. 10 Abs. 2, Nr. 9 Abs. 3 Ziffer 4 b der Sicherheitsrichtlinien in Betracht. Danach ist für den Fall, daß im Sinne der Nr. 9 Abs. 3 Ziffer 4 b ein sog. sicherheitserheblicher Sachverhalt es erfordert, auch die Befragung "anderer Personen" zulässig.
Hier ist zunächst jedoch fraglich, wann ein Sachverhalt bei einer zu überprüfenden Person als sicherheitserheblich zu definieren ist. Seitens des Sicherheitsbeauftragten des Innenministeriums und eines Mitarbeiters der Verfassungsschutzbehörde wurde argumentiert, daß bei den Bürgern der ehemaligen DDR generell von einem sicherheitserheblichen Sachverhalt auszugehen sei und sogenannte "andere Personen" befragt werden. Der Terminus "sicherheitserheblicher Sachverhalt" ist jedoch mit den im Volkszählungsurteil aufgestellten Grundsätzen an normenklare Regelungen nicht vereinbar. Es handelt sich vielmehr um eine nichtssagende Generalklausel. Aus diesem Grunde ist auch in dem Entwurf eines Sicherheitsüberprüfungsgesetzes - SÜG - Stand Mai 1993 - Drucksache 12/4891 - nicht mehr von einem sicherheitserheblichen Sachverhalt die Rede, sondern von sicherheitserheblichen Erkenntnissen. Eine Erkenntnis wird dann als sicherheitserheblich eingestuft, wenn sich aus ihr ein Anhaltspunkt für ein Sicherheitsrisiko ergibt. Dies zeigt, daß offensichtlich auch der Gesetzgeber der Ansicht ist, daß die Richtlinien nicht normenklar ausformuliert sind. Die pauschale Annahme, daß bei einem Bürger der ehemaligen DDR generell ein sicherheitserheblicher Sachverhalt vorliegt, erscheint im Hinblick auf das Diskriminierungsverbot - Art. 3 Abs. 3 GG - bedenklich.

Als weiteren Punkt habe ich kritisiert, daß die Mitarbeiter des Verfassungsschutzes ohne Termin am Arbeitsplatz der Referenzperson erschienen und - als ein Gespräch nicht zustande kam - sich an den Vorgesetzten wandten. Bei einer Sicherheitsüberprüfung hat die Verfassungsschutzbehörde gem. § 7 Abs. 2 LVerfSchG den Grundsatz der Verhältnismäßigkeit zu beachten. Von mehreren möglichen und geeigneten Maßnahmen sind diejenigen zu treffen, die den einzelnen insbesondere in seinen Grundrechten voraussichtlich am wenigsten beeinträchtigen. Eine Maßnahme ist nur solange zulässig, bis ihr Zweck erreicht ist oder sich zeigt, daß er nicht erreicht werden kann. Die Verfassungsschutzbehörde hat nicht darlegen können, warum sie nicht dem Vorschlag der Referenzperson gefolgt ist, sich an einem neutralen Ort zu treffen. Die Befragung hatte erkennbar nichts mit dem beruflichen Umfeld der Person zu tun. Insofern sind auf der einen Seite das Persönlichkeitsrecht der Referenzperson, ihr schutzwürdiges Interesse an Integrität ihrer Privatsphäre und an unbeeinträchtigten beruflichen Beziehungen und auf der anderen Seite das evtl. Gewicht und die Bedeutung der angestrebten Information und mögliche Handlungsinitiativenzur gewünschten Informationsbeschaffung abzuwägen.
Im vorliegenden Fall war nach dem eindeutigen Verhalten der Auskunftsperson, sich nicht von den Mitarbeitern der Verfassungsschutzbehörde befragen lassen zu wollen, ein Herantreten an den Arbeitgeber weder geeignet noch verhältnismäßig. Geeignet war es deshalb nicht, weil der Arbeitgeber nichts mit den zu ergreifenden Maßnahmen im Rahmen einer Sicherheitsüberprüfung zu tun hat und die Tatsache, daß sich eine Person nicht befragen lassen will, nicht ihre berufliche Situation betrifft. Verhältnismäßig war die Maßnahme ebenfalls nicht, da sich der Mitarbeiter der Verfassungsschutzbehörde nach dem Weigern der Auskunftsperson auf andere Weise die notwendigen Informationen hätte beschaffen müssen. In diesem Fall hätte dann die Weigerung ohne weiteres hingenommen werden müssen. Mit der zu überprüfenden Person hätte über die Benennung einer anderen Auskunftsperson gesprochen werden müssen.
Im Ergebnis einer Aussprache mit dem Mitarbeiter des Verfassungsschutzes und dem Sicherheitsbeauftragten des Innenministeriums wurde von der Sekretärin eine andere Referenzperson benannt.

2.6.4 Lobenswerte Zusammenarbeit des Verfassungsschutzes mit Stellen der Jugendarbeit

Der Bundeskanzler hat in einer Regierungserklärung vor dem Deutschen Bundestag am 16. Juni 1993 u. a. zur Bekämpfung von Gewalt und Extremismus einige Vorschläge unterbreitet. Es sollte insbesondere geprüft werden, inwieweit eine informatorische Zusammenarbeit von Verfassungsschutzbehörden mit Jugend- und Sozialbehörden anzustreben sei. Ich habe aus diesem Grunde bei der Verfassungsschutzbehörde unseres Landes angefragt, wie diese Art der Zusammenarbeit in Mecklenburg-Vorpommern ausgestaltet werden soll. Gleichzeitig habe ich an die bereits in den siebziger Jahren stattgefundene Strategiedebatte erinnert, in der die Frage diskutiert wurde, ob den Sicherheitsbehörden die Aufgabe als quasi Diagnose- und Therapieinstrument für "Strukturdefizite der Gesellschaft" zukommen kann, und ich habe darauf hingewiesen, daß ich einer Ausweitung des Netzes sozialer Kontrolle grundsätzlich skeptisch gegenüberstehe.

Der Innenminister des Landes teilte mir daraufhin mit, daß keineswegs "eine Ausweitung des Netzes sozialer Kontrolle" vorgesehen sei. Vielmehr sei geplant bzw. werde schon praktiziert, daß Jugend- oder Sozialbehörden Informationen über strukturelle Sachverhalte zugehen, die den Rechtsextremismus bei Jugendlichen betreffen. Es soll jedoch kein Austausch von personenbezogenen Daten von Gruppierungen zwischen der Verfassungsschutzbehörde und Jugend- bzw. Sozialbehörden stattfinden.

Als weiterer Aspekt der Arbeit des Verfassungsschutzes wurde die Öffentlichkeitsarbeit - mit dem Ziel der Prävention - hervorgehoben. Mitarbeiter der Verfassungsschutzabteilung hätten bereits vor Mitarbeitern von Jugend- und Sozialbehörden Vorträge zur Lage des Rechtsextremismus' in Mecklenburg-Vorpommern gehalten. Die sich im Zuge dieser Veranstaltung entwickelnden Diskussionen seien im Sinne meiner Fragestellung auch als "informatorische Zusammenarbeit"zu bewerten.
Gegen diese Art der Zusammenarbeit von Sicherheitsbehörden und anderen öffentlichen Stellen unseres Landes ist aus datenschutzrechtlicher Sicht keineswegs etwas einzuwenden.

2.7 Stasi-Unterlagen

2.7.1 Der IM in öffentlicher bzw. nicht-öffentlicher Ratssitzung

In einer Kommune hatte die Stadtverordnetenversammlung beschlossen, die Namen der überprüften Stadtverordneten und der (künftigen) Dezernats- bzw. Amtsleiter, die als inoffizielle Mitarbeiter für die Stasi gearbeitet haben, in nicht-öffentlicherSitzung bekanntzugeben.

Es existiert keine Rechtsgrundlage, die den Umgang mit den Gauck-Bescheiden explizit regelt. In den §§ 19 - 21 Stasi-Unterlagen-Gesetz (StUG) ist lediglich normiert, daß Unterlagen durch öffentliche Stellen in dem erforderlichen Umfang unter bestimmten Voraussetzungen zum Zwecke einer Überprüfung von Mitgliedern kommunaler Vertretungskörperschaften verwendet werden dürfen. In welcher Form jedoch eine Auswertung und Verwendung des Überprüfungsergebnisses erfolgen darf, ist dort nicht benannt. Um die Informationen über die MfS/AfNS-Tätigkeit eines gewählten Vertreters in öffentlicher bzw. nicht-öffentlicher Sitzung bekanntzugeben, wäre es denkbar, mangels spezifischer gesetzlicher Regelungen hierzu hilfsweise die Grundsätze für die Veröffentlichung von personenbezogenen Informationen durch Presse, Rundfunk und Film gem. § 34 Abs. 1 i.V.m. § 32 Abs. 3 StUG heranzuziehen. Danach ist eine Veröffentlichung von Informationen über eine Mitarbeit beim MfS/AfNS nur möglich, wenn diejenige Person, deren Daten veröffentlicht werden sollen, eingewilligt hat oder aber durch die Veröffentlichung ihre überwiegenden schutzwürdigen Interessen nicht beeinträchtigt werden. Es hat demnach eine Abwägung zwischen dem öffentlichen Interesse an der Aufarbeitung der MfS-Vergangenheit einerseits und den schutzwürdigen Belangen der jeweiligen Person andererseits stattzufinden. Im Ergebnis erachte ich es daher als unangemessen und unzulässig, die Namen aller Personen, die als inoffizielle Mitarbeiter für das MfS tätig waren, in öffentlicher oder auch nicht-öffentlicher Sitzung bekanntzumachen, ohne die erforderliche Interessenabwägung im Einzelfallvorgenommen zu haben.

Vor diesem Hintergrund habe ich dem Stadtverordnetenvorsteher empfohlen, den entsprechenden Beschluß aufzuheben. Die Stadtverordnetenversammlung ist meiner Empfehlung gefolgt.

2.7.2 Daten über MfS-Mitarbeit an neuen Arbeitgeber

In einer Petition ging es um die Frage, ob ein früherer Arbeitgeber (öffentliche Stelle) an einen neuen Arbeitgeber Daten, die die Mitarbeit eines bereits ausgeschiedenen Mitarbeiters beim MfS betreffen, weiterleiten darf.

Während der Dienstzeit des Petenten als Amtsleiter des Senats einer Hansestadt hatte der Präsident der Bürgerschaft - mit Einwilligung des Petenten - einen Antrag auf Überprüfung bei der Gauck-Behörde gestellt. Noch bevor der Bescheid des Bundesbeauftragten für die Stasi-Unterlagen eintraf, war der Petent bereits als Amtsleiter ausgeschieden und hatte eine neue Aufgabe übernommen. Nach dem Eintreffen des Gauck-Bescheides setzte der ehemalige Dienstvorgesetzte den neuen Arbeitgeber davon in Kenntnis, daß sein früherer Mitarbeiter für das MfS gearbeitet hat. Der neue Arbeitgeber wiederum unterrichtete den Petenten fernmündlich über die ihm zugegangenen Informationen und bestellte ihn zu einem Gespräch. In diesem Gespräch wurde der Petent mit den belastenden Auskünften der Gauck-Behörde konfrontiert, und in dessen weiteren Verlauf wurde ihm die Kündigung bzw. die Aufhebung des Arbeitsvertrages (dies war zwischen den Parteien streitig) avisiert.

Bei meiner Korrespondenz mit dem Präsidenten der Bürgerschaft stellte sich heraus, daß dieser irrtümlich davon ausging, daß er gem. § 28 StUG berechtigt sei, personenbezogene Informationen über eine frühere Mitarbeit beim MfS an einen neuen Arbeitgeber weiterzugeben. Ich habe ihn dahingehend belehrt, daß sowohl § 27 als auch § 28 StUG sich ausdrücklich auf die Befugnisse des Bundesbeauftragten für die Stasi-Unterlagen beziehen. Nur dieser ist berechtigt, zur Erfüllung seiner Aufgaben Mitteilungen bezüglich einer hauptamtlichen oder inoffiziellen Mitarbeit für den Staatssicherheitsdienst öffentlichen Stellen (§ 27 StUG) bzw. nicht-öffentlichen Stellen (§ 28 StUG) weiterzuleiten. Es war auch keine weitere Rechtsgrundlage vorhanden, nach der der Präsident der Bürgerschaft die Daten hätte weitergeben dürfen. Ein Umgang mit personenbezogenen Daten bei Dienst- und Arbeitsverhältnissen ist nur in den engen Grenzen des § 31 DSG MV zulässig. Im vorliegenden Fall hätte der Petent demnach einwilligen müssen, bevor seine personenbezogenen Daten übermittelt werden.

Ich habe den Präsidenten der Bürgerschaft darauf hingewiesen, in Zukunft keine personenbezogenen Daten aus Stasi-Unterlagen bzw. Bescheiden der Gauck-Behörde an Dritte zu übermitteln. Im Fall eines erneuten Verstoßes gegen datenschutzrechtliche Vorschriften werde ich von meinem Beanstandungsrecht Gebrauch machen.

2.8 Finanzwesen

2.8.1 Änderung der Abgabenordnung

Zur Zeit liegt vom Bundesministerium der Finanzen (BMF) der Entwurf eines Gesetzes zur Änderung der Abgabenordnung (AOÄG 1994) vor. Die Datenschutzbeauftragten des Bundes und der Länder hatten bereits bei früheren Gesetzesentwürfen stets darauf gedrängt, daß die Finanzverwaltungen des Bundes und der Länder einheitliches Datenschutzrecht anwenden. Die Ergänzungen und Präzisierungen der bereichsspezifischen Datenschutzvorschriften in der Abgabenordnung (AO) sollten - darüber bestand bislang Einvernehmen - vor allem der neueren Datenschutzgesetzgebung Rechnung tragen und den Umgang mit Daten, die dem Steuergeheimnis unterliegen, klarer als bisher regeln.

Mit Verwunderung nahmen daher die Datenschutzbeauftragten ein Schreiben aus dem Hause des BMF zur Kenntnis, in welchem der Vorschlag enthalten war, die datenschutzrechtlichen Bestimmungen der Abgabenordnung aus dem Änderungsgesetz herauszunehmen und zunächst nicht weiter zu verfolgen. Später hieß es dann, daß die übrigen Vorschriften - auch die datenschutzrechtlichen - in den Entwurf eines Gesetzes zur Bekämpfung des Mißbrauchs und zur Bereinigung des Steuerrechts übernommen werden sollen.

Ich habe die Finanzministerin unseres Landes darauf aufmerksam gemacht, daß eine solche Entscheidung alle bisherigen Bemühungen, die Vorschriften der Abgabenordnung zum Umgang mit personenbezogenen Daten an die Rechtsprechung und neuere Datenschutzgebung anzupassen, vorerst gegenstandslos machen würde. Zum einen ist die Forderung nach Anpassung der AO in Bezug auf die Systematik, den Aufbau und die Terminologie der Vorschriften nur ein Teil der insgesamt aus datenschutzrechtlicher Sicht erforderlichen Ergänzungen und Präzisierungen. Zum anderen lassen die zitierten Entscheidungen des Bundesverfassungsgerichtes meiner Meinung nach keineswegs den Schluß zu, es bestehe "für eine Änderung der AO im Hinblick auf datenschutzrechtliche Vorschriften weder eine rechtliche noch eine praktische Notwendigkeit". Diese Urteile beziehen sich allein auf die jeweils zugrunde liegenden Tatbestände und erklären daher auch nur in diesen Fällen die Vorschriften der AO unter Berücksichtigung des Rechtes auf informationelle Selbstbestimmung als im Grundsatz verfassungskonform. Inwieweit die betreffenden Regelungen als solche mit den verfassungsrechtlichen Anforderungen an den Datenschutz übereinstimmen, war nicht Gegenstand der Entscheidung.

Ein Verzicht auf detaillierte bereichsspezifische Datenschutzvorschriften in der AO hätte im übrigen zur Folge, daß die Speicherung und Übermittlung personenbezogener Daten in bestimmten Fällen mangels einer ausreichenden Rechtsgrundlage unzulässig wäre. Hierzu zählen insbesondere die beabsichtigte Einrichtung einer automatisiert geführten bundesweiten Fahndungsdatei und die Zusammenführung aller Dateien der Finanzämter für Steuerstrafsachen und Steuerfahndung in der Informationszentrale für den Steuerfahndungsdienst.

Die Datenschutzbeauftragten des Bundes und der Länder haben diese "Verzögerungstaktik" gegenüber dem Vorsitzenden des Finanzausschusses des Deutschen Bundestages kritisiert. Das Bemühen um einheitliche datenschutzgerechte Formulierungen im Bereich der Steuerverwaltung geht weiter.

2.8.2 Informations- und Kontrollbesuch im LAROV

Einige Petitionen, die den Umgang mit personenbezogenen Daten im Bereich der Vermögensrückgabe betreffen, veranlaßten mich zu einem Informations- und Kontrollbesuch im Landesamt zur Regelung offener Vermögensfragen (LAROV) - Außenstelle Schwerin -. Sowohl im technisch-organisatorischen Bereich als auch bei allgemeinen Fragen des Datenschutzes waren Mängel zu konstatieren. Hinsichtlich der gem. § 17 Abs. 2 Nr. 1 DSG MV sicherzustellenden Zugriffskontrolle stellte ich folgendes fest:

Die Datenbank "EVA" ist mit einer eigenen Nutzerverwaltung versehen. Der Datenbankadministrator vergibt Schreib-, Lese- und Löschrechte. Diese Rechte gelten dann für den gesamten Datenbestand, so daß z. B. ein Schreibrecht nicht auf bestimmte Datenbereiche eingegrenzt werden kann. Eine solche Organisation genügt nicht den Anforderungen des Datenschutzes. Deshalb habe ich empfohlen, die Datenbank so einzurichten, daß neben den jetzt schon vorhandenen Zugriffsdifferenzierungen auch eine Eingrenzung bezüglich der zur Bearbeitung freigegebenen Datensätze möglich wird. Besonders bei der neu einzurichtenden Software ist auf die Einhaltung dieser Forderung zu achten.
Ein weiterer Schwachpunkt war die Anzahl der Nutzer mit Shell-Berechtigung. Da diese Berechtigung umfassende Möglichkeiten zur Benutzung des UNIX-Betriebssystems eröffnet, ist die Zahl dieser hochprivilegierten Nutzer so klein wie möglich zu halten. Ich habe empfohlen, die Anzahl auf maximal zwei Personen zu reduzieren. Datensicherungs- und "shut-down"-Aufgaben (definiertes Herunterfahren des Betriebssystems) können von Systemverwaltern wahrgenommen werden, so daß keine zusätzlichen Nutzer eingetragen werden müssen. Des weiteren habe ich empfohlen, die organisatorischen Regelungen in Form von Dienstanweisungen schriftlich festzuhalten. So sollten z. B. Benutzeranweisungen, Datensicherungsrichtlinien, Hinweise zum Virenschutz und Vertretungsregelungen erarbeitet werden.

Ein anderer Hinweis betraf die Formulierung einer Einwilligungserklärung. Zum Hintergrund: Zur beschleunigten Klärung offener Vermögensfragen bearbeitet die Gesellschaft zur Klärung offener Vermögensfragen mbH (GoV) im Auftrag des LAROV und der Ämter zur Regelung offener Vermögensfragen Mecklenburg-Vorpommerns (AROV) Restitutionsanträge. Diese sind mit personenbezogenen Daten behaftet. Nach Einwilligung des Restitutionsantragstellers und ggf. anderer am Verfahren Beteiligter erfolgt eine Auftragsübergabe an die GoV auf der Grundlage des § 4 DSG MV. Zur formellen Ausgestaltung sind ein Auftragsformular des LAROV/AROV zur Bearbeitung eines Antrages auf Restitution sowie ein Formular für die Einwilligungserklärung zu verwenden. Ich hatte hinsichtlich dieses Einwilligungsformulars auf § 7 DSG MV hingewiesen. Danach ist der Betroffene in geeigneter Weise über die Bedeutung und Tragweite der Einwilligung, insbesondere die Art und den Umfang der Erhebung, Verarbeitung und Nutzung sowie über Empfänger beabsichtigter Übermittlungen von Daten, aufzuklären. Ein pauschaler Hinweis auf den Zweck der Übergabe des Antrages auf Restitution an die GoV reicht nicht aus, weil der Antragsteller über die Empfänger beabsichtigter Datenübermittlungen damit noch nicht aufgeklärt ist. Ich habe eine dahingehende Empfehlung gegeben und in diesem Zusammenhang noch einmal darauf hingewiesen, daß grundsätzlich der Auftraggeber für die Einhaltung datenschutzrechtlicher Vorschriften bei seinem Aufragnehmer verantwortlich ist.

Des weiteren stellte ich fest, daß im Rahmen einer auf § 27 Vermögensgesetz (VermG) gestützten Beantragung eines Grundbuchauszuges das LAROV den Namen eines Alteigentümers an das Grundbuchamt mitgeteilt hat. Auf Befragen wurde mir mitgeteilt, daß diese Datenübermittlung an das Grundbuchamt zum besseren Auffinden des Grundbuchblattes dienen kann. Derartige Datenübermittlungen sollten jedoch sehr restriktiv gehandhabt werden, da es eine bereichsspezifische Rechtsgrundlage für die Übermittlung von Namen der Alteigentümer nicht gibt.

Bei der Durchsicht von Akten, in denen die "Mitteilung der beabsichtigten Entscheidung" (die Ämter zur Regelung offener Vermögensfragen haben die Pflicht, den Beteiligten bereits von der beabsichtigten Entscheidung Mitteilung zu machen) erfolgte, habe ich in einem Fall festgestellt, daß der nach § 32 Abs. 1 Satz 2 VermG zu erteilende Hinweis auf die Möglichkeit der Auskunftserteilung gem. § 31 Abs. 3 VermG (Recht des Antragstellers auf umfassende Auskunft durch die Behörde) sowie auf das Wahlrecht nach Abs. 2 (Wahlrecht zwischen Rückübertragung und Entschädigung) unterblieben ist. Das Unterlassen solcher Informationspflichten der Behörde gegenüber dem Antragsteller sehe ich als erheblichen Mangel an. Ich habe daher empfohlen, den Hinweis auf § 31 Abs. 3 VermG und auf § 32 Abs. 2 VermG aus Klarstellungsgründen im Text bzw. im Anschreiben zur beabsichtigten Entscheidung deutlich kenntlich zu machen.

In der überwiegenden Anzahl der von mir festgestellten Mängel konnte das LAROV meinen Hinweisen und Empfehlungen folgen und sagte Abhilfe zu.

2.8.3 Datenübermittlung an Immobilienmakler

Ein Alteigentümer teilte mir mit, daß ihm durch das AROV Schwerin ein Hausgrundstück zurückübertragen worden sei. Aber noch ehe der Bescheid bestandskräftig geworden war, hatte er zu seiner Überraschung bereits Post von einer Immobilienmaklerfirma. Diese bot ihm in einem formularmäßig abgefaßten Schreiben ihre Dienstleistung an.

Ich habe daraufhin eine Kontrolle beim AROV und bei der Schweriner Wohnungsverwaltung (SWV) durchgeführt und habe mir eingehend schildern lassen, wer wann an wen aufgrund welcher Rechtsgrundlage Daten übermittelt. Im AROV erfolgt eine Datenübermittlung nach den §§ 31 Abs. 2 und 32 Abs. 5 VermG. Im vorliegenden Fall käme allenfalls § 32 Abs. 5 VermG in Betracht. Danach kann jedem, der ein berechtigtes Interesse glaubhaft darlegt, Name und Anschrift des Antragstellers sowie des Vermögenswertes mitgeteilt werden, auf den sich die Anmeldung bezieht. Es geht folglich um die Interpretation des Begriffes "berechtigtes Interesse". Vorauszuschicken ist, daß diese Vorschrift durch das zweite Vermögensrechtsänderungsgesetz vom 14. Juli 1992 eingefügt worden ist; Sinn und Zweck dieser Vorschrift war es, daß sich die am Verfahren Beteiligten mit potentiellen Investoren schneller einigen können und dadurch langwierige Gerichtsverfahren vermieden werden sollten. Keinesfalls zählen jedoch zu dem Personenkreis mit berechtigtem Interesse im oben geschilderten Sinne Immobilienmakler. Ich habe immer darauf hingewiesen, daß die Vorschrift des § 32 Abs. 5 VermG das zuständige Amt nicht von der Verpflichtung enthebt, in jedem Einzelfall zu prüfen, ob tatsächlich ein berechtigtes Interesse glaubhaft dargelegt werden kann.

Im vorliegenden Fall nahm ich Einsicht in die Akte des Petenten. Daraus ergab sich jedoch kein Anhaltspunkt für eine unzulässige Datenübermittlung. Des weiteren wurde mir mitgeteilt, daß den Mitarbeitern die Problematik durchaus geläufig ist, obwohl auch mündlich keine personenbezogenen Daten aus Akten an Immobilienmakler weitergegeben werden. Alle Mitarbeiter des AROV und auch der SWV sind sowohl auf das Datengeheimnis als auch auf das Dienstgeheimnis verpflichtet und entsprechend belehrt worden.

Leider konnte ich dem Petenten nur mitteilen, daß es trotz gesetzlicher Regelungen und interner Dienstanweisungen nicht auszuschließen ist, daß Daten auf undurchsichtigen Wegen an Immobilienmaklerfirmen gelangen. Der Nachweis einer unzulässigen Datenübermittlung fällt gerade auf diesem Gebiet sehr schwer.

2.8.4 Informations- und Kontrollbesuche in der OFD und im Finanzamt

Im März 1993 meldete ich mich bei einem Finanzamt zu einem Informations- und Kontrollbesuch an. Daraufhin wurde mir telefonisch mitgeteilt, daß man der Meinung sei, ich hätte mich zunächst bei der Oberfinanzdirektion (OFD) als der übergeordneten Dienststelle anzumelden, um den vorgeschriebenen Dienstweg einzuhalten.
In diesem Fall war es tatsächlich sinnvoll, mir zunächst durch einen Besuch bei der OFD einen Überblick über die Art und Weise der Zusammenarbeit zwischen OFD und den Finanzämtern zu verschaffen. Sowohl der OFD als auch dem betreffenden Finanzamt gegenüber machte ich jedoch deutlich, daß ich durchaus berechtigt bin, jederzeit und ohne vorherige Anmeldung in öffentlichen Stellen meines Zuständigkeitsbereiches Kontrollen durchzuführen und besonders bei anlaßbezogenen Kontrollen nicht die Einhaltung des sonst üblichen Dienstweges zu berücksichtigen habe.

Der Leiter des betreffenden Finanzamtes machte dann aber geltend, daß das Steuergeheimnis nach § 30 der Abgabenordnung den Datenschutzvorschriften des Landes vorgehen würde und ich deshalb kein Recht zur Einsichtnahme in den vom Steuergeheimnis geschützten Bereich habe. Auch dieser Auffassung habe ich deutlich widersprochen.
Gemäß § 27 Abs. 1 Nr. 1 DSG MV sind die öffentlichen Stellen des Landes verpflichtet, mir Einsicht in alle Unterlagen zu gewähren, die im Zusammenhang mit dem Umgang mit personenbezogenen Daten stehen. Noch deutlicher als die Formulierung im DSG MV ist die Formulierung im Bundesdatenschutzgesetz hinsichtlich des Umfangs der Kontrolle. Gemäß § 24 Abs. 2 Satz 1 BDSG erstreckt sich die Kontrolle des Bundesbeauftragten auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen. Das Steuergeheimnis wird demnach vom Gesetz ausdrücklich erwähnt, um § 30 AO zu genügen (vgl. Simitis, Dammann, Kommentar zum BDSG, 4. Auflg., § 24 Rdnr. 22). Entsprechendes gilt gemäß § 24 Abs. 6 BDSG hinsichtlich der Kontrollbefugnis der Landesbeauftragten für die öffentlichen Stellen des Landes.

Während des Informations- und Kontrollbesuches bei der OFD konnte ich mich umfassend über die Art und Weise der Verarbeitung von personenbezogenen Daten informieren. Dabei wurde deutlich, daß besonders im Bereich der in § 17 DSG MV genannten Eingabekontrolle notwendige technisch-organisatorische Maßnahmen nicht ausreichend umgesetzt wurden. So habe ich u.a. empfohlen, Protokolle über nicht erfolgreiche Einlog- und Zugriffsversuche zu führen. Außerdem mußte ich darauf hinweisen, daß die Finanzämter selbst speichernde Stellen im Sinne des DSG MV sind und deshalb auch die im § 16 DSG MV genannten Dateibeschreibungen zu führen haben. Es reicht nicht aus, wenn die Dateibeschreibungen lediglich bei der OFD vorliegen. Dringend empfohlen habe ich, daß unverzüglich sowohl für die OFD als auch für die einzelnen Finanzämter behördliche Datenschutzbeauftragte benannt werden.

Der Informations- und Kontrollbesuch im Finanzamt zeigte, daß die hier getroffenen technisch-organisatorischen Maßnahmen ebenfalls nicht den Anforderungen genügten. So waren z. B. die eingesetzten Personalcomputer nicht ausreichend gegen unberechtigten Zugriff geschützt und die bautechnischen Maßnahmen zur Gewährleistung einer ausreichenden Zutritts- und Datenträgerkontrolle waren unzureichend. Die Empfehlungen, die ich hier gegeben habe, decken sich mit den in den Abschnitten 2.16 (Automatisierte Datenverarbeitung) und 2.19 (Baulicher Datenschutz) beschriebenen Forderungen.

Von der Finanzministerin erhielt ich die Zusage, daß nach Anhörung der OFD im wesentlichen meinen Empfehlungen gefolgt werden soll. So werden künftig die Dateibeschreibungen in den Finanzämtern vorliegen. Auch die Maßnahmen zur Zutritts-, Datenträger und Benutzerkontrolle sollen entsprechend meinen Empfehlungen durch Verwendung von PC-Sicherheitssoftware, Einbau von Rauchmeldeanlagen, regelmäßige Raumkontrollen usw. verbessert werden.

2.8.5 Saubere Straßen - verletzter Datenschutz?

In einer Petition wandte sich ein Bürger in der folgenden Angelegenheit an mich:

Eine Stadt beabsichtigte, erstmals eine Straßenreinigungsgebühr zu erheben. Zu diesem Zweck wurde dem Abgabenpflichtigen ein Straßenreinigungsgebührenbescheid zugestellt. In dem Bescheid war neben der Gebühr auch das Konto des Abgabenpflichtigen aufgeführt, von dem die Abbuchung zu den fälligen Terminen erfolgen sollte. Ferner wurde dem Abgabenpflichtigen mitgeteilt, daß, falls er keinen Einzug der Straßenreinigungsgebühr gemäß des dem Stadtsteueramt vorliegenden Abbuchungsauftrages wünscht, er bis zu einem bestimmten Termin dieses mitteilen sollte. Der Betroffene war darüber sehr verwundert, denn eine Einzugsermächtigung bzw. einen Abbuchungsauftrag für die Straßenreinigungsgebühr hatte er nicht erteilt. Wie aber ist dann die Stadt im Zusammenhang mit der Straßenreinigungsgebühr an seine Bankverbindung gelangt?

Die Stadt ist von Abbuchungsermächtigungen ausgegangen, in der die Abgabepflichtigen sich generell mit der Abbuchung aller Abgaben einverstanden erklärt hatten. Zum Zeitpunkt der Erteilung dieser Abbuchungsermächtigung wurde eine Straßenreinigungsgebühr jedoch noch nicht erhoben. Deshalb wählte die Stadt die oben beschriebene Widerspruchslösung. Pro Abgabenpflichtigen wird ein Einheitskonto, das sogenannte Personenkonto, beim Stadtsteueramt geführt. Die Stadt entnahm die Bankverbindung den in den Personenkonten zur Verfügung stehenden Finanzadreßdateien.

Ich habe meine Bedenken zur Verwendung von derartig pauschalen Abbuchungsermächtigungen geäußert, insbesondere auch im Hinblick darauf, daß zum Zeitpunkt der Erteilung der Abbuchungsermächtigung die Straßenreinigungsgebühr noch nicht erhoben wurde. Ferner habe ich mich gegen die von der Stadt praktizierte Widerspruchslösung ausgesprochen, weil es ausschließlich ein Recht des Abgabepflichtigen ist, selbst zu entscheiden, welche Abgaben abgebucht werden sollen und welche nicht. Die von der Stadt gewählte Widerspruchslösung entspricht diesem Recht in keiner Weise. Der auf die Finanzadreßdatei erfolgte Zugriff war unzulässig. Ich habe darauf hingewiesen, und der Bürgermeister hat mir mitgeteilt, daß die Formulare für eine pauschale Einwilligung der Abbuchung aller Abgabearten bereits seit über einem Jahr nicht mehr verwendet werden. Auf den jetzt genutzten Formularen sind neben der Angabe der Bankverbindung die im Lastschriftverfahren einzuziehenden Abgabearten durch den Abgabepflichtigen konkret zu kennzeichnen. Die Finanzadreßdatei wird in diesem Zusammenhang überarbeitet, so daß die Kontoinhaberdaten nicht mehr allgemein unter der Abgabepflicht, sondern jeweils eingeschränkt auf die in der Lastschriftvereinbarung mitgeteilten Abgabearten in der Finanzadreßdatei hinterlegt werden. Die Abgabenpflichtigen wurden darüber informiert, daß eine Abbuchung entgegen der Ankündigung im Straßenreinigungsgebührenbescheid erst erfolgen wird, wenn dies ausdrücklich für die Straßenreinigungsgebühr gewünscht wird. Hierzu werden die neuen Vordrucke übersandt.
Die vom Stadtsteueramt nunmehr gewählte Verfahrensweise wird meinen Forderungen gerecht und ist datenschutzrechtlich nicht mehr zu beanstanden.

2.9 Datenschutz im Fernsehen - Die Hölle von Ueckermünde

In der Öffentlichkeit wird zur Zeit zunehmend über Probleme der Verletzung der Persönlichkeitssphäre und der Menschenwürde durch eine bestimmte Art der Berichterstattung in den Medien diskutiert. Menschen werden in hilflosen, entwürdigenden oder schlicht peinlichen Situationen dargestellt. Ein Beispiel hierfür war die am 14.04.1993, 21.45 Uhr von der ARD ausgestrahlte Sendung "Die Hölle von Ueckermünde". Es wurden dort schwer psychisch gestörte Menschen im Christophorus - Krankenhaus Ueckermünde in äußerst entwürdigenden Situationen und teilweise recht langen Sequenzen gezeigt.

Aus juristischer Sicht handelt sich hier um ein Spannungsverhältnis zwischen dem Recht auf freie Berichterstattung einerseits und dem Recht der Betroffenen zur Wahrung ihrer Persönlichkeits- bzw. Intimsphäre andererseits. Grundsätzlich gilt gem. § 41 BDSG das sogenannte Medienprivileg. Danach fällt der journalistisch-redaktionelle Bereich prinzipiell nicht unter die staatliche Aufsicht. Trotzdem sind die Rundfunkanstalten jedoch nicht von der Beachtung der Grundrechte enthoben. Dies ergibt sich ausdrücklich auch aus § 41 Abs. 3 Satz 1 BDSG. Danach kann jemand, der durch eine Berichterstattung der Rundfunkanstalten in seinem Persönlichkeitsrecht beeinträchtigt wird, Auskunft über die der Berichterstattung zugrunde liegenden zu seiner Person gespeicherten Daten verlangen.

Das Aufzeigen von Mißständen in der Psychiatrie hätte demnach auch auf eine Weise geschehen können, die die psychisch Kranken weniger in ihrem allgemeinen Persönlichkeitsrecht beeinträchtigt. So hätten die Betroffenen beispielsweise so gefilmt werden können, daß sie als Person unerkannt bleiben. Frontalaufnahmen verletzten daher meines Erachtens auch das sog. Recht am eigenen Bild. Die Einholung der Einwilligung der Klinikleitung zur Sendung solcher Beiträge sehe ich als nicht ausreichend an. Ich bin hierfür jedoch nicht unmittelbar zuständig und habe meine Auffassung daher lediglich in Form einer Presseerklärung geäußert.

2.10 Statistik

2.10.1 Erteilung von statistischen Auskünften auf Postkarten

In einer Petition wurde mir eine Postkarte zur Kenntnis gegeben, mit deren Hilfe durch das Statistische Landesamt Erhebungen über Umsatz und Anzahl der Beschäftigten in Unternehmen durchgeführt werden. Die Auskunftspflicht für die Inhaber oder Leiter von Unternehmen hinsichtlich dieser Angaben ergibt sich aus § 8 Handelsstatistikgesetz i.V.m. den §§ 15 und 26 Abs. 4 Satz 1 Bundesstatistikgesetz (BStatG). Die erhobenen Einzelangaben unterliegen nach § 16 BStatG der Geheimhaltungspflicht und dürfen grundsätzlich nur für statistische Zwecke verwendet werden.
Vom Petenten wurden nun hinsichtlich der Geheimhaltungspflicht Bedenken gegen die Verwendung von Postkarten bei derartigen Erhebungen geäußert. Gegen das Auskunftsverfahren selbst bestehen jedoch grundsätzlich keine Bedenken.
Ich habe dem Petenten mitgeteilt, daß das Unternehmen auf der Antwortkarte nicht aufgeführt werden muß und somit die in der Postkarte enthaltenen Angaben keinem bestimmten Unternehmen zugeordnet werden können.Somit bleibt die Anonymität jedoch gewahrt. Dem Auskunftspflichtigen steht es ferner frei, die Karte in einem verschlossenen Umschlag einzusenden. Darauf wird der Auskunftspflichtige vom Statistischen Landesamt im Heranziehungsbescheid hingewiesen. Es besteht die Gefahr, daß der Auskunftspflichtige den Hinweis zur Sicherung der Anonymität der Daten im Heranziehungsbescheid nicht beachtet und so ungewollt Dritten den Zugang zu seinen Daten ermöglicht. Um die Gefahr der ungewollten Deanonymisierung durch den Auskunftspflichtigen zu minimieren, war das Statistische Landesamt auf meine Anfrage hin bereit, künftig die Postkarte mit einem entsprechenden Hinweis zu versehen. Nach meiner Auffassung wird damit das Interesse des Auskunftspflichtigen hinsichtlichder Geheimhaltung seiner Daten in geeigneter Weise gewahrt.

2.10.2 Statistik im Kommunalbereich

Der interne Datenschutzbeauftragte einer Kommune wandte sich mit der Frage an mich, ob aufgrund einer Satzung über die Kommunalstatistik

a) Daten in anonymisierterForm
b) personenbezogene Daten (zum Aufbau der sogenannten kleinräumigenGliederung)

aus dem Einwohnermelderegister an die Statistikstelle innerhalb der Behörde übermittelt werden dürften. Ich habe dazu wie folgt Stellung genommen:

Zu a)

Gegen die Weitergabe von Daten in anonymisierter Form ist aus datenschutzrechtlicher Sicht grundsätzlich nichts einzuwenden. Das DSG MV findet keine Anwendung, soweit ein Rückschluß auf Personen nicht möglich ist. Ob die Satzung der Kommune gegen anderes höherrangiges Recht verstößt, unterliegt nicht meiner Beurteilung.

Zu b)

Die Weitergabe von personenbezogenen Daten aus dem Einwohnermelderegister an die kommunale Statistikstelle halte ich für bedenklich. Eine derartige Datenübermittlung - in diesem Fall würde es sich um eine regelmäßige Datenübermittlung handeln - kann nicht auf eine Satzung über die Kommunalstatistik gestützt werden. Außerdem war der vorliegend geschilderte beabsichtigte Fall einer Datenübermittlung in der Satzung noch nicht einmal geregelt.

Einschlägig ist hier § 31 Landesmeldegesetz. Regelmäßige Datenübermittlungen sind gem. § 31 Abs. 6 LMG unter strenger Beachtung des Zweckbindungsgrundsatzes in einer Rechtsverordnung näher zu regeln. In der Meldedaten-Übermittlungsverordnung (MeldDÜV MV) ist eine Datenübermittlung vom Einwohnermelderegister an die kommunale Statistikstelle ebenfalls nicht vorgesehen. Sie ist aus den vorgenannten Gründen unzulässig. Es wäre zu überlegen, Kompetenzen und Übermittlungsbefugnisse einer kommunalen Statistikstelle in einem Landesstatistikgesetz zu regeln.
Von der Kommune wurden meine vorstehend genannten datenschutzrechtlichen Bedenken akzeptiert und eine Datenübermittlung in der o. g. Form nicht weiter in Erwägung gezogen.

2.10.3 Mikrozensus

Für Ende April/Anfang Mai 1993 hatte das Statistische Landesamt eine statistische Erfassung der Bevölkerungsstruktur (Mikrozensus) angekündigt. Der Mikrozensus hat den Zweck, statistische Angaben in tiefer fachlicher Gliederung über die Bevölkerungsstruktur, die wirtschaftliche und soziale Lage der Bevölkerung und der Familien, den Arbeitsmarkt, die berufliche Gliederung und Ausbildung der Erwerbsbevölkerung sowie die Wohnverhältnisse bereitzustellen. Rechtsgrundlage ist das Mikrozensusgesetz vom 10. Juni 1985. Nachdem die ersten Interviewer vor der Tür standen, erhielt ich einige mündliche Anfragen. Die Anrufer wollten wissen, ob und in welcher Form sie zur Auskunft verpflichtet seien.

Aus datenschutzrechtlicher Sicht ist vor allem bedeutsam, daß die Anonymität der Erhebung hinreichend gewährleistet ist. Das Bundesverfassungsgericht hat in seinem Beschluß vom 15.04.1988 darauf hingewiesen, daß das Recht auf informationelle Selbstbestimmung angesichts der verfassungsrechtlichen Bedeutung der amtlichen Statistik (Artikel 73, Abs. 11 GG) nicht absoluten Geheimnisschutz fordern kann, sondern die Herstellung relativer, faktischer Anonymisierung ausreichend ist. So hat auch das OVG Hamburg (Beschluß vom 12.02.1991) im Leitsatz bekräftigt: "Die rein theoretische Möglichkeit, eine Person, deren Daten in die Statistik eingegangen sind, zu ermitteln und dem Interessierten die Kenntnisse und Daten dieser Person zu erschließen, bietet keinen Grund, die Auskunft des Mikrozensus zu verweigern."

Ich habe mich von den Mitarbeitern des Statistischen Landesamtes ausführlich über den Ablauf des Verfahrens zum Mikrozensus informieren und mir die einzelnen Arbeitsetappen von der Auswahl der Wohnungen bis zur Datenerfassung und -verarbeitung schildern lassen. Aufgrund der Vorgehensweise bin ich der Auffassung, daß mit den Daten im Statistischen Landesamt ordnungsgemäß verfahren wird.

Einen Schwachpunkt stellt meines Erachtens jedoch die Auswahl der Interviewer dar. Wenn die Kleinzählung geplant wird, werden die Stellen für Interviewer ausgeschrieben und interessierte Bürger können sich hierfür bewerben. Die Auswahl geschieht nach Treu und Glauben. Später sucht jeder Interviewer ca. 30 Haushalte auf und füllt gemeinsam mit dem Haushaltsvorstand den statistischen Fragebogen aus. Die Interviewer werden zwar belehrt, die personenbezogenen Daten geheimzuhalten und müssen das durch ihre Unterschrift bestätigen, aber eine weitergehende Überprüfung ihrer Person findet nicht statt. Sie müssen lediglich noch eine Erklärung unterschreiben, daß sie nicht als offizieller oder inoffizieller Mitarbeiter des MfS/AfNS der ehemaligen DDR tätig waren. Da jedoch eine Überprüfung dieser Angaben nicht vorgesehen ist, habe ich Bedenken hiergegen geäußert. Diesen Bedenken wurde vom Statistischen Landesamt entgegengehalten, daß es für die Betroffenen auch möglich ist, auf die Unterstützung durch den Interviewer zu verzichten und den Fragebogen allein auszufüllen, zu versiegeln und an das Landesamt abzusenden. Dennoch habe ich empfohlen, nach Möglichkeit einen festen Personenkreis von Interviewern einzusetzen, die sich bereits in der Vergangenheit als zuverlässig erwiesen haben.

2.11 Soziales und Sozialwesen

2.11.1 Vorgedrucktes und Vertrauliches im Jugendamt

Von den Jugendämtern werden u. a. Formulare verwendet, die noch das Jugendwohlfahrtsgesetz (JWG) als Rechtsgrundlage für die Datenerhebung beinhalten, obwohl das Kinder- und Jugendhilfegesetz (KJHG) mit einigen Einschränkungen bereits zum 03. Oktober 1990 in den neuen Bundesländern in Kraft getreten ist. Einige Jugendämter nutzten Vordrucke, in denen bei Angaben, die auf freiwilliger Basis erhoben werden, z. B. beim Ehegatten des Unterhaltspflichtigen, ein entsprechender Hinweis zur Freiwilligkeit im Vordruck fehlte. Die im Bereich Hilfe zur Erziehung von einem Jugendamt genutzten Formulare zur Antragstellung enthielten keine Angaben über die Rechtsgrundlage der Erhebung und den Erhebungs- bzw. Verwendungszweck. In diesem Zusammenhang habe ich die Jugendämter auf die Regelungen des § 62 KJHG hingewiesen, wonach Zulässigkeit und Umfang der Datenerhebung an die entsprechende Aufgabenerfüllung gekoppelt sind, Rechtsgrundlage und Verwendungszweck im jeweiligen Vordruck enthalten sein müssen und die Betroffenen hierüber aufzuklären sind.

Probleme zeigten sich auch im Zusammenhang mit der Beratung der Bürger. Es ist insbesondere durch die räumlichen Gegebenheiten nicht in allen Bereichen eine Einzelberatung möglich, so daß zur Zeit noch zwei oder mehr Bürger gleichzeitig in einem Raum beraten werden müssen. In einem Jugendamt konnte aufgrund der schlechten Schalldämmung der Türen die Beratung des Antragstellers im Bereich der Kindertagesstätten auf dem Flur mitgehört werden. Ich halte diese Zustände für nicht akzeptabel und habe die Jugendämter aufgefordert, die entsprechenden technisch-organisatorischen Maßnahmen (Trennwände, Einzelabfertigung, Schalldämmung der Türen) zur Herstellung eines ausreichenden Datenschutzes einzuleiten. In den Jugendämtern werden meine Bedenken geteilt und es wurde zugesichert, die Mißstände abzustellen.

2.11.2 Sozialhilfeempfänger - Freiwild der Ausforschung?
"Überprüfungsbogen - Wohn- und Wirtschaftsgemeinschaft -"

Von einem Kollegen erhielt ich ein Formular "Überprüfungsbogen - Wohn- und Wirtschaftsgemeinschaft/eheähnliche Gemeinschaft -", das in Sozialämtern seines Landes bei der Überprüfung des Vorliegens einer Wohn- und Wirtschaftsgemeinschaft verwendet wird. Ich wurde um eine rechtliche Bewertung dieses Formulares und um die Darstellung der entsprechenden Handhabung in Sozialämtern Mecklenburg-Vorpommerns gebeten.
Der Überprüfung des Vorliegens einer Wohn- und Wirtschaftsgemeinschaft kommt insbesondere bei der Gewährung von Wohngeld entscheidende Bedeutung zu. Nach dem Wohngeldgesetz wird zunächst einmal vermutet, daß Personen, die gemeinsam einen Wohnraum bewohnen, auch eine Wirtschaftsgemeinschaft haben. Diese gesetzliche Vermutung kann aber vom Antragsteller widerlegt werden. Dafür muß er u. a. mit Hilfe des Überprüfungsbogens darlegen und glaubhaft machen, daß er entgegen der auf der allgemeinen Lebenserfahrung gründenden Regel ausnahmsweise keine Wirtschaftsgemeinschaft mit der anderen Person hat. Weil daraus ein insgesamt höherer Wohngeldanspruch erwachsen kann, kommt es vor, daß es Partnerschaften fingiert darauf anlegen, zwar als Wohn-, aber nicht als Wirtschaftsgemeinschaft zu gelten. Der zu prüfenden Frage, ob der Antragsteller die gesetzliche Vermutung glaubhaft widerlegt hat, muß erhebliche Aufmerksamkeit gewidmet werden.

Auf dem zu beurteilenden Überprüfungsbogen war nun dieser Frage aus datenschutzrechtlicher Sicht etwas zuviel Aufmerksamkeit gewidmet worden. So mußte der Antragsteller beispielsweise beantworten, wo seine Wäsche und wo die seines Mitbewohners/Partners gelagert werde, wer diese Wäsche reinigt und bügelt und wer sie dann in den Schrank zurück sortiert. Eine derartige Erhebung von personenbezogenen Daten ist aber nach den Grundsätzen des Datenschutzrechtes nur dann zulässig, wenn u.a. deren Kenntnis zur rechtmäßigen Erfüllung einer in der Zuständigkeit der erhebenden Stelle liegenden Aufgabe erforderlich ist. Bei diesem Überprüfungsbogen war die "Erforderlichkeit" einzelner Fragen von Petenten zu Recht angezweifelt worden. Die Erforderlichkeit ist grundsätzlich nur dann gegeben, wenn die Aufgabe sonst gar nicht, nicht vollständig oder in nicht rechtmäßiger Weise erfüllt werden kann.

Die Überprüfung eines in Mecklenburg-Vorpommern von einem Amt für Wohnungswesen, Abteilung Wohngeldstelle, verwendeten Formulares ("Anlage - Wohn- und Wirtschaftsgemeinschaft -") ergab jedoch, daß die darauf befindlichen Fragen datenschutzrechtlich unbedenklich sind. Dieses Formular unterscheidet sich gerade in den wesentlichen - bedenklichen - Punkten von dem o. g. Überprüfungsbogen; insbesondere fehlen die Fragestellungen nach der Reinigung und Lagerung der Wäsche. Der in Mecklenburg-Vorpommern verwendete Überprüfungsbogen kann sogar als gutes Beispiel dafür dienen, daß das Bestehen oder Nicht-Bestehen einer Wohn- und Wirtschaftsgemeinschaft auch mit Hilfe eines reduzierteren Fragenkataloges ausreichend zuverlässig beurteilt werden kann.

PROSOZ-Datei

Anläßlich einer Kontrolle in der Hauptfürsorgestelle (HFSt) des Landes habe ich die Verarbeitung der Daten von Schwerbehinderten und Kriegsopfern geprüft. Die Hauptfürsorgestelle verwendet dazu Programme der PROSOZ GmbH. In diesen Dateien sind für die Anwender frei verfügbare Datenfelder vorgesehen. Nach Auskunft der HFSt ist das für spezifische Anpassungen notwendig, da die Softwareentwickler das Produkt bundesweit vertreiben und somit nicht alle Besonderheiten in den Ländern und Sozialämtern berücksichtigen können. Bei einer weiteren Kontrolle in einem Sozialamt wurden in einer anderen PROSOZ-Datei ebenfalls vom Anwender frei zu definierende Datenfelder gefunden.

Die Datenschutzbeauftragten des Bundes und der Länder stimmen darin überein, daß für den Anwender frei verfügbare Datenfelder sich nicht mit den Grundsätzen des Datenschutzes vereinbaren lassen (s.a. 2.14.2.). Entweder müssen diese Datenfelder gesperrt werden, oder es sind in einer Dienstvereinbarung ihr Zweck und ihre Nutzung festzuschreiben. Würden derartige Einschränkungen nicht vorgenommen, so wären Mißbrauchsmöglichkeiten gegeben; beispielsweise wäre denkbar, daß unzulässige Vermerke über das Verhalten von Antragstellern gemacht werden. In jedem Fall muß die Verwendung der Datenfelder einer Datei revisionsfähig sein. Da nach Aussage der HFSt die freien Datenfelder gegenwärtig nicht benötigt werden, habe ich die Sperrung der Felder empfohlen. Die unverzügliche Umsetzung meiner Empfehlung wurde zugesichert.

2.11.3 Sozialdatenschutz bei Gericht

Ein Altenpflege- und Pflegeheim informierte mich, daß bei der Durchführung des Betreuungsgesetzes (BtG) der Datenschutz durch das zuständige Amtsgericht verletzt worden sei. Was war geschehen?

Das Amtsgericht hat elf Bewohner des Heimes vom Vorschlag, einen Betreuer zu bestellen, durch Übermittlung einer nur für das Amtsgericht bestimmten Liste in Kenntnis gesetzt. Das Pflegeheim hatte die Liste zusammengestellt und sie gemäß § 2 BtG dem Gericht zur Entscheidung vorgelegt. Sie enthielt den Namen, den Vornamen und das Geburtsdatum des zu Betreuenden sowie den Vornamen, den Namen und die Adresse des vorgeschlagenen Betreuers und das Verwandtschaftsverhältnis zueinander. In einem weiteren Schreiben, das ebenfalls einigen Heimbewohnern zuging, wurde um eine schnelle Entscheidung für einen namentlich benannten Bewohner gebeten, "da aus medizinischen Gründen (zunehmende Aggressivität und damit Gefährdung anderer Heimbewohner) u. U. eine schnelle Verlegung notwendig wird."
Das Pflegeheim wiederum erhielt Kenntnis von der Übermittlung an die Bewohner, weil ein Betroffener das Personal um Hilfe bei der Beantwortung der Fragen des Amtsgerichtes bat. Am gleichen Tag telefonierten daraufhin die Betreiber des Heimes mit dem zuständigen Richter und wiesen auf den Verstoß gegen Grundsätze des Datenschutzes hin. Der Fehler wurde durch den Richter zwar eingeräumt, aber er führte an, daß die Angelegenheit nicht mehr rückgängig zu machen sei, da bereits alle Schreiben versandt worden seien. Tatsächlich jedoch erhielten fünf weitere Bewohner drei Wochen nach dem Telefonat die entsprechenden Schreiben des Amtsgerichtes ohne Anonymisierung der anderen Heimbewohner. Es wäre also sehr wohl möglich gewesen, die Offenbarung der Daten der anderen Betroffenen zu vermeiden.

Auf meine Anfrage beim Direktor des Amtsgerichtes wurde die Schilderung des Heimes bestätigt. Der Richter ging bei seinem Telefonat mit den Betreibern davon aus, daß bereits alle Betroffenen diese Mitteilung erhalten hätten, weil die Schreiben ein Datum trugen, das vierzehn Tage vor dem Telefongespräch lag. Tatsächlich hätten sich die Schreiben jedoch noch gegenständlich im Geschäftsgang befunden und ihre Weiterleitung gestoppt werden können. Aufgrund meines Schreibens wurde der Vorfall im Gericht ausgewertet und mir versichert, daß die datenschutzrechtlichen Bestimmungen künftig beachtet werden.

2.11.4 Landesversicherungsanstalt

Kontrolle der Landesversicherungsanstalt

Eine meiner ersten Kontrollen habe ich bei der Landesversicherungsanstalt Mecklenburg-Vorpommern (LVA MV) durchgeführt. Die LVA MV ist eine Körperschaft des öffentlichen Rechts und unterliegt gemäß § 79 Sozialgesetzbuch Zehntes Buch (SGB X) dem BDSG. Weil es sich hierbei jedoch um eine Landesinstitution handelt, wird die Kontrolle der Einhaltung des BDSG in diesem Fall von mir wahrgenommen.
Die Rentenanträge der Versicherten werden in den Auskunfts- und Beratungsstellen erfaßt und danach der LVA MV zugestellt. Teilweise müssen fehlende Angaben zu Beschäftigungszeiten aufwendig recherchiert werden. Zur Unterstützung dieser Recherche sind u.a. Hebekarten der Finanzämter aus der Zeit von 1946 bis 1950 durch ein Archiv der LVA MV in Schwerin übernommen worden. Andererseits kann der Rentenanspruch durch Beibringung von Zeugen glaubhaft gemacht werden, wenn durch den Antragsteller kein schriftlicher Nachweis einer Beschäftigungszeit und des Verdienstes erbracht werden kann.
Die eingehenden Rentenanträge werden nach festgelegten Kriterien auf die Arbeitsbereiche der LVA MV aufgeteilt und dort maschinell erfaßt. Die Speicherung erfolgt in einer Zentraldatei der Landesversicherungsanstalten der neuen Bundesländer. Die LVA MV hat direkten Zugriff zu dieser Zentraldatei. Die Zugriffsrechte der Mitarbeiter auf die Datei sind hierarchisch geregelt und durch Paßwörter geschützt. Die Zugriffe selbst werden protokolliert und gestatten eine eindeutige Zuordnung. Die Zugriffsprotokolle werden stichprobenartig kontrolliert.
Diese Datenschutzmaßnahmen entsprechen soweit dem üblichen Standard. Auf meine Frage nach der Dateibeschreibung wurde jedoch darauf verwiesen, daß sie nur am Standort der Zentraldatei geführt wird. Ich habe darauf hingewiesen, daß es nicht nur im Interesse der Versicherten notwendig ist, eine Dateibeschreibung vorzuhalten, sondern auch zur Information der Mitarbeiter und auf die dazu im BDSG enthaltenen Bestimmungen aufmerksam gemacht. Nach Verständigung der an der Zentraldatei beteiligten Landesversicherungsanstalten untereinander wurde meinem Hinweis gefolgt, und die Dateibeschreibung ist nun ebenfalls in der LVA MV angelegt.

Angabe von Heilstätten gegenüber Arbeitgebern

Nach einem Hinweis des Hamburgischen Datenschutzbeauftragten habe ich das Verfahren zur Angabe der Behandlungsstätte auf einer "Bescheinigung für den Arbeitgeber gem. § 7 Abs. 2 Lohnfortzahlungsgesetz" bei der LVA MV geprüft. Kritikwürdig an dem bisherigen Verfahren ist, daß der Arbeitnehmer, wenn ihm eine Kur bewilligt wird, von der LVA die o. g. Bescheinigung zur Vorlage beim Arbeitgeber bekommt und aufgefordert wird, den Beginn der Behandlung und den Entlassungstag durch Bescheinigungen der Behandlungsstätte nachzuweisen. Ein erfahrener Personalsachbearbeiter kann aus der Angabe der Behandlungsstätte, mitunter allein schon aufgrund des Behandlungsortes, auf die Art der zu behandelnden Erkrankung schließen.
Entsprechend eines Vorschlages meines Hamburger Kollegen habe auch ich empfohlen, daß die LVA die beschriebene Ankündigung unterläßt und den Arbeitnehmern auf Wunsch eine neutrale Bescheinigung ausstellt und ihnen das in einem Merkblatt auch ausdrücklich anbietet. Die LVA MV hat sich zu dem Vorschlag positiv geäußert und verfährt inzwischen entsprechend.

2.11.5 Krankenkassen

Datenweitergabe bei Beantragung von Hilfsmitteln

Der Inhaber einer Firma für Rehabilitationstechnik hat im Juli 1993 die Frage an mich gerichtet, in welchen Fällen eine Krankenkasse die Patientendaten einem Zweitanbieter übermitteln darf. Er führte an, daß die Krankenkasse einem Mitbewerber ohne Zustimmung des Patienten dessen Namen, Adresse und spezifische Merkmale des Hilfsmittels übermittelt hätte. In Abstimmung mit der Krankenkasse sei der Patient zunächst bei ihm gewesen und hätte für ein bestimmtes Hilfsmittel einen Kostenvoranschlag gewünscht. Da es sich nicht um ein Standardprodukt handelte, waren umfangreiche Messungen von Körpermerkmalen des Patienten notwendig. Der Kostenvoranschlag sei dann zusammen mit den Meßergebnissen an die Krankenkasse gesandt worden. Der Patient erkundigte sich nach einiger Zeit bei der Reha-Technik Firma nach seinem Hilfsmittel. Da aber noch keine Auftragsbestätigung vorlag, wurde bei der Krankenkasse nachgefragt, dort jedoch die Auskunft erteilt, daß erst noch ein Konkurrenzangebot eingeholt werden müßte. Der Patient ist bei keinem anderen Sanitätshaus vorstellig geworden. Daraus hat der Erstanbieter geschlossen, daß die personenbezogenen Daten einschließlich der gemessenen Körpermerkmale an einen Zweitanbieter übermittelt wurden.

Zur Klärung des in der Beschwerde angesprochenen Sachverhaltes habe ich Informationsbesuche in den Hauptverwaltungen der Allgemeinen Ortskrankenkasse und der Innungskrankenkasse durchgeführt und in beiden Fällen unterschiedliche Verfahrensweisen vorgefunden.
Die AOK holt nur Zweitangebote bei anderen Sanitätshäusern ein, wenn es sich um Standardprodukte handelt. Die Übermittlung personenbezogener Daten wäre deshalb in dieser Phase nicht notwendig, sondern erst dann, wenn der Zweitanbieter den Auftrag erhält. In diesem Fall werden der Name und die Anschrift des Versicherten an das Sanitätshaus übermittelt.

Von der Innungskrankenkasse werden in bestimmten Fällen auch die Maße für spezielle Anfertigungen übermittelt, jedoch ohne Personenbezug. Erhält der Zweitanbieter den Auftrag, so werden ihm Name und Anschrift des Versicherten sowie die Verordnung und die Diagnose des Arztes übermittelt. Kopien des Kostenübernahmeformulares erhalten sowohl der Leistungserbringer als auch der Versicherte, der dadurch erfährt, daß er sein Hilfsmittel von einem anderen Anbieter (Zweitanbieter) erhält.

Die geschilderte Verfahrensweise bei den Krankenkassen macht deutlich, daß sehr unterschiedliche Auffassungen zur Gewährleistung des Datenschutzes bestehen und es dringend notwendig ist, daß sich die Landesverbände der Krankenkassen auf der Grundlage des § 127 Abs. 3 SGB V (Verträge mit Leistungserbringern) auf ein Verfahren einigen, das den Prinzipien des Datenschutzes entspricht. Bis zur Inkraftsetzung dieser notwendigen Regelung habe ich den Krankenkassen empfohlen, vor der Übermittlung personenbezogener Daten an einen Zweitanbieter den Patienten zu informieren und ihm ein Widerspruchsrecht gegen die Übermittlung in einer angemessenen Frist einzuräumen.

Kontrolle in einer Betriebskrankenkasse

Betriebskrankenkassen (BKK) wird wegen ihrer Nähe zum Arbeitgeber häufig unterstellt, daß ein konsequenter Datenschutz hier nicht zu realisieren ist. Für mich war es deshalb von besonderem Interesse, die Organisation und Arbeitsweise einer BKK näher kennenzulernen, um mir ein eigenes Bild von diesem häufig erwähnten Vorurteil machen zu können.
Die besuchte BKK hat gegenwärtig einen Mitgliederbestand von ca. 6 800 Versicherten und ca. 2 000 mitversicherten Familienangehörigen. Sie ist Mitglied des Landesverbandes Nord, in dem BKKn der Länder Mecklenburg-Vorpommern, Hamburg und Schleswig-Holstein zusammengeschlossen sind. Zur Datenverarbeitung wird gegenwärtig noch ein Rechnernetz mit dem Betriebssystem Amboss eingesetzt. Die Anmeldung zum DV-System erfolgt über die Systemkennung, ein anwenderspezifisches Kennwort sowie ein persönliches Paßwort, das in regelmäßigen Abständen gewechselt wird. Die Anmeldungen zum System werden protokolliert, ausgedruckt und stichprobenartig ausgewertet. Die notwendigen technisch-organisatorischen Datenschutzmaßnahmen halte ich damit für realisiert. Ende des Jahres 1993 soll ein Rechnerverbund des Landesverbandes Nord genutzt und die Datenverarbeitung dann auf einer UNIX-Anlage durchgeführt werden. In den Geschäftsstellen der BKK werden nur noch Bildschirme und Tastaturen vorhanden sein, und die Kommunikation mit dem Zentralrechner wird über Leitungen der DBP Telekom erfolgen. Eine weitere Kommunikationsstrecke besteht zum Bundesverband der Betriebskrankenkassen, von der der BKK Veränderungen der Versichertendaten übermittelt und an die statistische Daten weitergegeben werden. Die Unterlagen der Versicherten werden in verschließbaren Schränken in den Räumen der BKK aufbewahrt. Neben einem üblichen Schließsystem sind die Räume mit einer Diebstahl- und Brandwarnanlage ausgerüstet.

Eine Bestätigung für das Vorurteil, daß der Datenschutz in einer BKK nur schwer zu realisieren sei, habe ich nicht gefunden. Gleichwohl hat der Geschäftsführer bestätigt, daß der Auftrag der Gesundheitsprophylaxe wegen dieser Nähe zum Arbeitgeber nur mit sehr viel Behutsamkeit wahrgenommen werden kann.

2.11.6 Bald Chipkarte statt Krankenschein?

Die Krankenkassen planen die Einführung von Chipkarten anstelle der bisher üblichen Krankenscheine mit dem Ziel, die jetzt noch aufwendige Abrechnung ärztlicher Leistungen zu vereinfachen. Allein mit dem Ersetzen des Krankenscheines ist aber das Potential einer solchen Chipkarte noch lange nicht ausgeschöpft. Deshalb gibt es Überlegungen, auf ihr auch wichtige Gesundheitsdaten bis hin zur ganzen Krankengeschichte zu speichern, um beispielsweise in Notfallsituationen schnell helfen zu können (s.a. 2.21.2). Weil die Datenschutzrisiken gegenwärtig nicht vollständig abgeschätzt werden können, bleibt es auf Initiative des BfD vorläufig bei dem Ersetzen des Krankenscheines und damit lediglich der Speicherung von Beitragsdaten, wie Name, Vorname, Geburtsdatum, Anschrift, Krankenversicherungsnummer, Versichertenstatus und Beginn des Versicherungsschutzes auf der Chipkarte. In einigen Gebieten der Bundesrepublik wird die Chipkarte bereits probeweise eingesetzt, um Erfahrungen zu sammeln, die dann bei der geplanten bundesweiten Einführung berücksichtigt werden.

Ich hatte die Kassenärztliche Vereinigung Mecklenburg-Vorpommern (KV MV) um Auskunft über den Stand der Einführung der Chipkarte in unserem Land und des damit verbundenen Datenflusses bei der Abrechnung kassenärztlicher Leistungen gebeten. Bei diesem Informationsgespräch habe ich auf die notwendigen datenschutzrechtlichen Maßnahmen aufmerksam gemacht. Der Geschäftsführer der KV MV stellte zunächst mögliche Ausstattungsvarianten der Arztpraxen mit Hard- und Software vor. Die Wahl einer Variante trifft der jeweilige Kassenarzt, wobei er finanziell zu einem bestimmten Teil sowie beratend von der KV MV bzw. den Krankenkassen unterstützt wird. Ziel ist es, einen durchgängigen Datenfluß mittels maschinenlesbarer Datenträger (Diskette) vom Arzt über die KV MV zur Krankenkasse zu erreichen.
Bei der KV MV werden pro Abrechnungszeitraum hunderte Disketten der niedergelassenen Ärzte eingehen, deren Daten nach der Verarbeitung fachgerecht vernichtet werden müssen. Nach Aussage der Mitarbeiter der KV MV ist die direkte Vernichtung der Disketten zu teuer. Deshalb habe ich empfohlen, die entsprechende Technik zur physischen Löschung der Daten auf der Diskette einzusetzen und die gelöschten Datenträger anschließend an die Arztpraxen zurückzugeben.

Durch die mit der Einführung der Chipkarte verbundene Ausrüstung der Arztpraxen mit Rechentechnik wird es den Krankenkassen erstmals möglich sein, umfangreiche Auswertungen und Statistiken der ärztlichen Tätigkeiten und über die Patienten zu erstellen. So gesehen besteht neben der latenten Gefahr des "gläsernen Patienten" nun auch die Gefahr des "gläsernen Arztes". Was bisher nur durch umfangreiche, zeitaufwendige und teure Recherchen, beispielsweise der Krankenscheine mit den Diagnose- und Verordnungsdaten eines Arztes, an Auswertungen möglich gewesen wäre, wird dann durch einfache Programme jederzeit realisierbar. Ich sehe es deshalb als eine meiner wesentlichen Aufgaben auf diesem Gebiet an, darauf zu achten, daß Auswertungen, die zwar technisch möglich, aber durch Rechtsvorschriften nicht geregelt oder nicht zugelassen sind, auch tatsächlich nicht vorgenommen werden.
Ein genauer Zeitpunkt zur Einführung der Chipkarte in Mecklenburg-Vorpommern steht noch nicht fest.

2.11.7 Welche Daten darf die Kurverwaltung erheben?

Ich erhielt die Eingabe eines Bürgers aus Ulm, der zusammen mit seiner Ehefrau seinen Urlaub in Heringsdorf (Usedom) verbrachte. Dort hatte er bei der Kurverwaltung die fällige Kurabgabe entrichtet und sollte in diesem Zusammenhang auch sein Geburtsdatum und das seiner Ehefrau auf der Kurkarte eintragen. Der darüber erboste Urlauber bat mich um die Überprüfung der Zulässigkeit einer derartigen Datenerhebung.

In § 11 des Kommunalabgabengesetzes ist geregelt, daß ein Kurbeitrag als Gegenleistung dafür erhoben werden kann, daß denjenigen Personen, die sich als Ortsfremde in Kurorten eine Unterkunft nehmen, die Möglichkeit geboten wird, die dort vorhandenen Einrichtungen und Anlagen in Anspruch zu nehmen und an den durchgeführten Veranstaltungen teilzunehmen. Dabei können die Beherbergungsstätten in einer Satzung - hier die Satzung über die Erhebung einer Kurabgabe in der Gemeinde Seebad Heringsdorf - dazu verpflichtet werden, die beherbergten Personen der Gemeinde, dem Landkreis oder dem Gemeindeverband zu melden, den Kurbeitrag einzuziehen und an die Gemeinde, den Landkreis oder den Gemeindeverband abzuliefern. Aus diesem Grunde haben beherbergte Personen gemäß § 26 LMG am Tage ihrer Ankunft in der Beherbergungsstätte einen besonderen Meldeschein auszufüllen und zu unterschreiben. Dabei können mitreisende Ehegatten auf dem Meldeschein mit aufgeführt werden. Welche Angaben auf dem Meldeschein gemacht werden müssen, ist in § 27 LMG normiert; so sind der Tag der Ankunft und der der voraussichtlichen Abreise, der Familienname, der gebräuchliche Vorname, die Anschrift, die Staatsangehörigkeit und auch das Geburtsdatum anzugeben. Ebenfalls ist in § 27 LMG geregelt, daß für Zwecke der Erhebung des Kurbeitrages und auch für Zwecke der Fremdenverkehrsstatistik von den ausgefüllten Meldescheinen Durchschriften gefertigt werden dürfen. Falls die jeweilige Beherbergungsstätte eine solche Durchschrift fertigt, muß sie jedoch die beherbergte Person im Meldeschein darauf hinweisen. Auf der Durchschrift "Kurkarte" erscheinen allerdings nicht mehr alle Daten, die auf dem Meldeschein erhoben wurden, denn die Angaben "Geburtstag", "Staatsangehörigkeit" und "Herkunftsland" werden nicht durchgedruckt, da die entsprechenden Stellen auf der Kurkarte geschwärzt sind.

Die in den Meldescheinen für Beherbergungsstätten enthaltenen Daten dürfen gemäß § 29 LMG grundsätzlich nur von der Meldebehörde ausgewertet und verarbeitet werden und dieses auch nur dann, wenn es für ihre Aufgabenerfüllung erforderlich ist. Darüber hinaus dürfen die Daten auf den Durchschriften von den Gemeinden zur Erhebung des Kurbeitrages sowie für Zwecke der Fremdenstatistik ausgewertet und verarbeitet werden.

Wie die Meldescheine und wie die Durchschriften auszusehen haben, ist in der "Landesverordnung über Meldescheine und die amtliche Meldebestätigung (Meldescheinverordnung)" Mecklenburg-Vorpommerns geregelt. Die in der Meldescheinverordnung abgebildeten Muster für einen "Meldeschein für Beherbergungsstätten" und für eine "Kurkarte" sind vom Zweckverband "Seebäder Insel Usedom" in der dort vorgegebenen Form übernommen worden. Im Ergebnis war daher nicht zu beanstanden, daß der Urlauber und seine Ehefrau zumindest auf dem Meldeschein bestimmte Daten, darunter auch ihr Geburtsdatum, angeben mußten und dann Teile der gemachten Angaben - jedoch nicht mehr das Geburtsdatum - auf der Durchschrift "Kurkarte" erscheinen.

2.12 Gesundheitswesen

2.12.1 Gesetze und Gesetzentwürfe

Wenige Tage nach meiner Wahl bat mich der Sozialausschuß des Landtages um eine Stellungnahme zu den datenschutzrechtlichen Passagen des Gesetzentwurfes für ein Landeskrankenhausgesetz (LKHG). Trotz der damals noch vielfältigen Probleme beim Aufbau meiner Dienststelle war das frühe Einbeziehen in die Gesetzesarbeit wichtig, da hierdurch exemplarisch zumindest noch die Übereinstimmung des Begriffssystems des Gesetzentwurfes mit unserem ebenfalls erst kurz zuvor in Kraft getretenen Landesdatenschutzgesetz hergestellt und die wichtigsten Vorschläge zu inhaltlichen Änderungen eingebracht werden konnten.

Im Abschnitt Patientendatenschutz des Landeskrankenhausgesetzes ist das informationelle Selbstbestimmungsrecht der Patienten geregelt. Meine Empfehlungen zu § 14 LKHG - Anwendungsbereich und Begriffsbestimmungen - wurden nicht voll übernommen. Wünschenswert wäre nach meiner Auffassung eine weitergehende Untergliederung des Absatzes 1 gewesen, um den Anwendungsbereich der Datenschutzvorschriften von den Definitionen abzugrenzen. Auch die Verwendung des Terminus "Umgang mit Daten" anstelle des Bezugs auf die Verarbeitung wäre hier umfassender gewesen. Denn der Umgang mit Daten schließt gemäß § 3 Abs. 4 DSG MV das Erheben, Verarbeiten und Nutzen der Daten ein, und somit wäre vom Grundsatz her eine generelle Anwendung der Datenschutzbestimmungen möglich gewesen. Allerdings sind in den §§ 15 ff LKHG Bestimmungen zum Erheben und Nutzen der Daten enthalten, so daß insgesamt kein datenschutzfreier Raum für die Betroffenen entsteht.
Meine Stellungnahme zur Datenübermittlung von Religionszugehörigen hat positiven Niederschlag im Landeskrankenhausgesetz gefunden. In § 17 LKHG wird nunmehr explizit darauf hingewiesen, daß auch zur seelsorgerischen Betreuung Daten an Religionsgesellschaften übermittelt werden dürfen, wenn der Patient eingewilligt hat oder es sein mutmaßlicher Wille ist.

Im Gesetzentwurf über Hilfen und Schutzmaßnahmen für psychisch Kranke (PsychKG) wurde im Abschnitt IX - Datenschutz, Akteneinsicht - ausgeführt, daß die Vorschriften des Landesdatenschutzgesetzes und des Landeskrankenhausgesetzes für personenbezogene Daten anzuwenden sind. Deshalb habe ich lediglich eine Empfehlung zum § 38 PsychKG - Erkennungsdienstliche Maßnahmen - des Abschnittes VII gegeben. Ursprünglich hieß es in § 38 Abs. 1 Satz 1 PsychKG: "Zur Sicherung des Vollzugs der Maßregel werden erkennungsdienstliche Unterlagen angefertigt." Nach meiner Empfehlung lautet dieser Satz jetzt wie folgt: "Zur Sicherung des Vollzugs der Maßregel dürfen erkennungsdienstliche Maßnahmen angeordnet werden." Im Rahmen dieser neuen Formulierung besteht hier ein Ermessensspielraum, so daß nicht in jedem Fall erkennungsdienstliche Unterlagen angefertigt werden müssen, sondern im Einzelfall nach den Grundsätzen der Erforderlichkeit und Notwendigkeit entschieden werden kann.

Krebsregistergesetzentwürfe

Für die neuen Bundesländer ist zur vorläufigen Fortführung der Datensammlung des "Nationalen Krebsregisters" der ehemaligen DDR ein Krebsregistersicherstellungsgesetz vom Bundestag und Bundesrat beschlossen worden. Es erlaubt die Fortführung des Registers jedoch nur bis zum 31.12.1994. Um die wissenschaftlich wertvolle und zur Ursachenforschung von Krebserkrankungen wichtige Datensammlung auch über diesen Zeitpunkt hinaus weiterführen und auf andere Bundesländer ausdehnen zu können, hat der Bundesminister für Gesundheit den Entwurf eines Bundeskrebsregistergesetzes vorgelegt. Noch herrscht jedoch keine Einigkeit zwischen Bund und Ländern über die Gesetzgebungskompetenz.
Zur Vorbeugung der Gefahr des Abbruches des ehemaligen "Nationalen Krebsregisters" ab 1995 haben die Referenten der Gesundheitsministerien der neuen Bundesländer und des Berliner Senats sowie des Bundesministeriums für Gesundheit (BMG) verschiedene Modelle für ein gemeinsames Krebsregistergesetz entwickelt und mit den Landesdatenschutzbeauftragten der neuen Bundesländer beraten. Die Modelle weisen unterschiedliche Varianten zur Realisierung der Datenschutzbestimmungen auf. In dem von den Landesdatenschutzbeauftragten der neuen Länder bevorzugten Modell ist vorgesehen, daß eine Vertrauensstelle die Identitätsdaten von den epidemiologischen Daten (Daten der Krebserkrankung) trennt. Die Identitätsdaten werden anschließend verschlüsselt. In der Registerstelle werden die epidemiologischen Daten gespeichert und stehen dann zur wissenschaftlichen Nutzung bereit. Die Meldung an das Krebsregister erfolgt in der Regel, wenn der Patient eingewilligt hat. Es wird aber auch die Möglichkeit eingeräumt, im Anschluß an eine Meldung die Einwilligung des Betroffenen nachzuholen und bei Nichteinwilligung die gespeicherten Daten zu löschen. Wegen der hohen Kosten für die Länder haben die Referenten der Gesundheitsministerien der neuen Länder und des Berliner Senats vorgeschlagen, eine verwaltungsorganisatorisch einheitliche Vertrauens- und Registerstelle mit abgeschotteten Aufgabenbereichen einzurichten. Dieser Lösung habe ich zunächst vorbehaltlich einer eingehenden Prüfung des Gesetzentwurfes zugestimmt.

2.12.2 Altakten in den Gesundheitsämtern

Die Frage der Behandlung von Altakten im Gesundheitswesen wurde vor allem durch die teilweise chaotische Auflösung der Polikliniken akut. In einigen Städten mußten quasi "über Nacht" Lösungen für die Aufbewahrung von hunderttausenden von Patientenakten gefunden werden. Auf diesen Ansturm war keine Institution des Gesundheitswesens eingerichtet. Es war einfach versäumt worden, in Vorbereitung der Liquidation der Polikliniken geeignete Wege für die weitere Behandlung und Nutzung der Akten aufzuzeigen.
Aus datenschutzrechtlicher Sicht gab es bei der Auslagerung der Patientenkarteien aus den Polikliniken vielfach haarsträubende Zustände und es ist nur glücklichen Umständen zu verdanken, daß kein Mißbrauch mit den Akten geschah. Letzten Endes wurden die Patientenakten den Gesundheitsämtern "vor die Tür" gelegt und es ist anzuerkennen, daß sie sich der Verantwortung gestellt haben. Wegen dieser höchst bedenklichen Situation habe ich gleich zu Beginn meiner Amtszeit verschiedene Kontrollen in Gesundheitsämtern durchgeführt und auf einer Amtsärzteberatung zu diesem Thema referiert. Die Gesundheitsämter haben die Aufgabe auf sehr unterschiedliche Art und Weise gelöst.

In einem Gesundheitsamt lagen die Akten ungeordnet auf dem Fußboden eines Raumes in einem verfallenen Gebäude. Die Zimmerdecke war stark einsturzgefährdet und mit Balken provisorisch abgestützt, die Fenster undicht und ohne Kraftanstrengung von außen einzudrücken - der Raum lag ebenerdig. Eine Sicherung gegen Brand oder Diebstahl war nicht gegeben. Die Akten selbst lagen in dem Zustand der Anlieferung in diesem Raum, d. h., nur ein Bruchteil des Schriftgutes war sortiert. Die frühere Ordnung des Bestandes war bereits bei der Auslagerung und während des Transportes zerstört worden. Allerdings gab es auch Aktenbündel - so z. B. aus einer ehemaligen Betriebspoliklinik -, in denen alle asbestose- und silikosegefährdeten Patienten zusammengefaßt waren. Weitere Akten befanden sich an neun verschiedenen Stellen der Stadt. Auch hier entsprachen die Aufbewahrungsbedingungen für das sensible Schriftgut nicht den Anforderungen. In einigen Räumen steht bei Regenwetter das Wasser regelmäßig zentimeterhoch. Das Gesundheitsamt hat erklärt, daß es weder materiell noch personell in der Lage ist, den gegenwärtigen Zustand zu beheben.
Ich habe den Umgang mit den Patientenakten in der Kommune beanstandet und auf schnelle Beseitigung der schlimmsten Mängel gedrungen. Das ist inzwischen geschehen. Trotzdem kann immer noch nicht von einer den Anforderungen entsprechenden Aufbewahrung gesprochen werden.

Daß es auch anders geht, zeigte die Kontrolle im Gesundheitsamt in Rostock, der größten Stadt unseres Landes. Hier war sogar die Sortierung aller Gesundheitsakten (ca. 1 Mio.) schon abgeschlossen. Die Unterbringung der Akten und der Umgang mit ihnen entsprechen den datenschutzrechtlichen Anforderungen an die Schriftgutlagerung. Durch Einflußnahme auf die Auslagerung der Akten aus den Polikliniken konnte die ursprüngliche Sortierung größtenteils erhalten und die Akten deshalb effektiv in das Archiv übernommen werden. In dieser Phase wurde übergangsweise medizinisches Personal der aufgelösten Poliklinikenim Archiv eingesetzt.

Auf der o. g. Amtsärzteberatung habe ich die wesentlichen Forderungen zum datenschutzgerechten Umgang mit Patientenakten erläutert und bin insbesondere auf Gebäudeschutz- und technisch-organisatorische Maßnahmen eingegangen. Ich habe außerdem vorgeschlagen, die Akte jedes Patienten in einem Umschlag zu versiegeln, mit Namen, Vornamen, Geburtsdatum, der letzten bekannten Anschrift, der Poliklinik und Anschrift des behandelnden Arztes zu versehen. Da das bei einem Aktenbestand von ca. einer Million Stück schwer zu realisieren ist, sollte das Vorgehen vom Inhalt der Akten und den weiteren Bedingungen der Aufbewahrung abhängig gemacht werden. Schließlich sollte die Archivierung der Patientenakten in den Gesundheitsämtern nur eine vorübergehende Aufgabe sein und das Ziel bestehen, den Bestand durch Übergabe an die jetzt behandelnden Ärzte bzw. durch Vernichtung nach Ablauf der Aufbewahrungsfristen und in Abstimmung mit den Kranken-, Renten- und Unfallversicherungsträgern unter Beachtung der Ansprüche der Patienten abzubauen.

2.12.3 Entscheidung des BVerfG zu § 218 StGB

Das Bundesverfassungsgericht hat in seiner Entscheidung zu § 218 StGB (s.a. NJW 1993, Heft 28, S.1751 ff) vom Mai diesen Jahres verkündet, daß ein Abbruch der Schwangerschaft ohne Feststellung einer Indikation nach einer Beratung unter bestimmten, klar genannten Bedingungen straffrei vorgenommen werden kann. Die Schwangere muß aber in jedem Fall vorher eine staatlich zugelassene Beratungsstelle aufgesucht haben und den Nachweis der Teilnahme an der Beratung erbringen. Gleichzeitig wird in dem Urteil der Schwangeren auch die Anonymität bei der Beratung zugesichert. Dieses Verfahren ist mit einigen datenschutzrechtlichen Aspekten verknüpft, die ich mit dem zuständigen Referat des Sozialministeriums erörtert habe. Nach meinen Anregungen sind schließlich die "Hinweise für die Beachtung des Datenschutzes bei der Beratungstätigkeit entsprechend dem Urteil des Bundesverfassungsgerichtes vom 28. Mai 1993" vom Sozialministeriumherausgegeben worden.
Bei der Erarbeitung der Hinweise ging es vor allem darum, wie trotz Wahrung der Anonymität der Nachweis erbracht werden kann, daß die Schwangere an der Beratung teilgenommen hat. Die Bescheinigung ist dem Arzt vorzulegen, an den sich die Beratene wegen des Schwangerschaftsabbruches wendet. Inhalt der Hinweise ist u. a.:

- Der Name der Schwangeren wird ausschließlich in die Bescheinigung über die Beratung eingetragen. Eine anderweitige Erfassung ist nicht zulässig.
- Gegenüber der Beratenden kann die Schwangere anonym bleiben, weil eine andere Person der Beratungsstelle die Bescheinigung ausstellt.
- Das Beratungsprotokoll ist anonym zu führen.

Der Sozialminister hat festgelegt, daß die Datenschutzhinweise für alle zugelassenen Beratungsstellen bindend sein sollen.

2.12.4 Heilpraktikerprüfung

Aufgrund des Hinweises eines Kollegen habe ich das Verfahren der Heilpraktikerprüfung in unserem Land geprüft. Es war die Frage zu klären, ob es mit dem informationellen Selbstbestimmungsrecht vereinbar ist, wenn bei den Prüfungen Tonbandprotokollierungen gemacht werden und der Betroffene nicht ausdrücklich darauf hingewiesen wird.

In Mecklenburg-Vorpommern wird die Tonbandprotokollierung bei der Heilpraktikerprüfung vom Sozialministerium abgelehnt. Die Prüfung selbst entspricht den "Leitlinien für die Überprüfung von Heilpraktikeranwärtern gemäß § 2 Abs. 1 Buchst. i) der Ersten Durchführungsverordnung zum Heilpraktikergesetz des Bundesministeriums für Gesundheit" vom 2. September 1992. Die Prüfung besteht aus einem schriftlichen und einem mündlichen Teil und wird vom Amtsarzt und einem von ihm zu berufenden gutachtlich mitwirkenden Heilpraktiker durchgeführt. Bei Heilpraktikern für Psychotherapie wird sie nach Aktenlage vorgenommen, wenn der Antragsteller ein abgeschlossenes Hochschulstudium auf einem angrenzenden Gebiet nachweisen kann; anderenfalls wird auch schriftlich und mündlich vom Amtsarzt und einem Gutachter geprüft. Dieses Verfahren verletzt nicht das informationelle Selbstbestimmungsrecht.

2.12.5 Genomanalyse im Arbeitsschutzrahmengesetz

Die Genomanalyse ermöglicht die Untersuchung des Erbmaterials und soll nach dem Entwurf des Arbeitsschutzrahmengesetzes (ASRG) bei Vorsorgeuntersuchungen eingesetzt werden, um den eventuellen Ausbruch einer Erkrankung durch das Zusammentreffen einer bestimmten Erbanlage mit einer bestimmten Arbeitsplatzbelastung zu verhindern. Die Bundesregierung hat einen Gesetzentwurf für das ASRG Ende 1992 vorgelegt. Im April 1993 wurde es von den Datenschutzbeauftragten des Bundes und der Länder anläßlich einer Arbeitskreisberatung diskutiert. Ich habe mich sowohl bei dieser Gelegenheit als auch bei einer Beratung mit der zuständigen Abteilung des Sozialministeriums unseres Bundeslandes gegen die dort eingeräumte Möglichkeit genomanalytischer Vorsorgeuntersuchungen nach Aufklärung und schriftlicher Einwilligung des Beschäftigten gewandt, weil ich der Meinung bin, daß trotz Einwilligungslösung der Arbeitnehmer nicht immer frei entscheiden kann und der Arbeitgeber Möglichkeiten hat, den Beschäftigten de facto zu einer Genomanalyse zu zwingen. So wäre beispielsweise denkbar, daß der Arbeitgeber die weitere Beschäftigung auf einem bestimmten Arbeitsplatz davon abhängig macht, ob der Beschäftigte sich einer Genomanalyse unterzieht.

Ich meine, daß das informationelle Selbstbestimmungsrecht des Arbeitnehmers auch ein Recht auf "Nichtwissen" einschließt und habe deshalb vorgeschlagen, daß die Entscheidung zur Durchführung der Genomanalyse, wie auch die Bekanntgabe des Ergebnisses gegenüber dem Arbeitgeber, allein vom Beschäftigten getroffen werden sollte. Dieses Verfahren entspricht schließlich dem anderer Vorsorgeuntersuchungen, bei denen es dem Patienten überlassen ist, ob er beispielsweise das Angebot der Krebsvorsorgeuntersuchung wahrnimmt oder nicht. Damit wird meines Erachtens das informationelle Selbstbestimmungsrecht gewahrt. Unabhängig von Vorsorgeuntersuchungen sollte der Arbeitgeber durch das Arbeitsschutzrahmengesetz verpflichtet werden, sein Wissen über Zusammenhänge zwischen genetischen Anlagen und dem Gefährdungspotential von Arbeitsplätzen den Beschäftigten zu vermitteln.
Der Gesetzentwurf zum Arbeitsschutzrahmengesetz befindet sich weiterhin in der Diskussion. Ich werde die Entwicklung des inzwischen vorliegenden neuen Gesetzentwurfes verfolgen und meine oben beschriebene Position vertreten.

2.12.6 Patientendaten in Krankenhäusern

Kontrolle eines Krankenhauses

Jeder Patient eines Krankenhauses hat schon erfahren, wie umfangreich er über seine Person in der "Aufnahme" berichten muß und kann vermuten, wie groß der Datenkatalog ist, der über ihn gespeichert wird. Da es sich hierbei um sensible Gesundheitsdaten handelt und außerdem umfangreiche Datenübermittlungen an die Krankenversicherungsträger stattfinden, erwächst der Einhaltung datenschutzrechtlicher Bestimmungen in Krankenhäusern eine besonders hohe Bedeutung.

Ich habe ein Krankenhaus besucht, um mich einerseits über den Umgang mit personenbezogenen Daten zu informieren und um andererseits die Mitarbeiter in Datenschutzfragen zu beraten. Bei dem Besuch wurde darauf verwiesen, daß neben den medizinisch notwendigen Daten vor allem detaillierte Datensammlungen wegen der Kostenkontrolle durch die Krankenkassen und wegen des hohen Dokumentationsbedarfes aus haftungsrechtlichen Gründen angelegt werden müssen. Eine erneute Zunahme der Erhebung und Speicherung personenbezogener Daten ist - so die weitere Aussage - durch das geänderte Gesundheitsstrukturgesetz entstanden.
Das Verfahren und die Organisation der Datenverarbeitung im Krankenhaus wurden aus Schleswig-Holstein übernommen. Die Datenverarbeitung wird mit dem Projekt DATAPLAN realisiert, das nach Aussage der Mitarbeiter bundesweit verbreitet ist und von einer großen Anzahl Krankenhäuser genutzt wird. Für Wartungszwecke hat die Entwicklerfirma unzulässigerweise Zugriff auf die Patientendaten. Die Fernwartung kann allerdings nur auf Initiative des Systemadministrators gestartet werden. Die Datensicherung erfolgt täglich. Die installierte Software erlaubt eine Vielzahl von Auswertungen, zu deren Nutzung sechs Mitarbeiter autorisiert sind. Die Möglichkeit der Datenaus- und -eingabe per Diskette ist an zwei Stellen des Netzes möglich, zu denen nur ein bestimmter eingeschränkter Personenkreis Zugang hat. Die Datenzugriffe werden dokumentiert und stichprobenartig ausgewertet.

In Auswertung des Besuches habe ich den leitenden Mitarbeitern des Krankenhauses Empfehlungen zur Paßwortvergabe, zum Zugriff bei der Fernwartung, zu Auswertungen von Patientendaten und zur Aufbewahrung von Sicherungskopien gegeben (s.a. Abschnitt 2.16). Gleichzeitig hatte ich um die Zusendung von Auszügen aus dem Wartungsvertrag mit den entsprechenden datenschutzrechtlichen Regelungen gebeten, was zunächst abgelehnt wurde, aber nach meinem Hinweis auf § 27 DSG MV schließlich doch geschah. Im wesentlichen wurde meinen Empfehlungen gefolgt. Die Hinweise zur Fernwartung konnten noch nicht in vollem Umfang realisiert werden (s.a. Punkt 2.21.4).

Aufbau eines Tumorzentrums

Das Klinikum in R. plant die Einrichtung eines Tumorzentrums und bat mich bereits in der Vorbereitungsphase um Hinweise zur Einhaltung des Datenschutzes. Dadurch war es mir möglich, wichtige datenschutzrechtliche Regelungen rechtzeitig mit einzubringen.

Das Ziel des Tumorzentrums ist die Einführung einer Tumorbasisdokumentation als Grundlage eines klinischen Krebsregisters, das die medizinische Betreuung der Patienten durch effektivere Kommunikation der Fachabteilungen verbessern und der Nachsorge der Patienten dienen soll. Außerdem kann die im Krebsregistersicherstellungsgesetz vorgesehene Datenübermittlung von Krebserkrankungen an das Nationale Krebsregister erfolgen.

Kernproblem des Datenschutzes war die Klärung der Frage, welche personenbezogenen Daten der Patienten in das klinische Register aufgenommen und unter welchen Voraussetzungen Daten an das Nationale Krebsregister übermittelt werden dürfen. Weiterhin war zu klären, welche Daten unter welchen Voraussetzungen bei den im Tumorzentrum vereinigten medizinischen Einrichtungen und Ärzten, die nicht dem Klinikum R. angehören, erhoben werden dürfen. Vom Tumorzentrum ist eine den Anforderungen entsprechende Einwilligungserklärung erarbeitet worden, die allen Patienten mit malignen Erkrankungen vorgelegt wird. Der Patient wird darin über den Umfang, den Zweck und die Stelle der Datenspeicherung aufgeklärt. In dieser Einwilligungserklärung wird der Patient auch gefragt, ob er einer Übermittlung seiner Daten an das Nationale Krebsregister zustimmt. Die bisher getroffenen Datenschutzmaßnahmen genügen den gesetzlichen Vorschriften und entsprechen denen anderer Tumorzentren und klinischer Krebsregister in Deutschland. Noch nicht vollständig geklärt ist die technische Realisierung der Verschlüsselung bei der Datenübermittlung zwischen den einzelnen Partnern. Bis zur Inbetriebnahme des System soll eine datenschutzgerechte Lösung implementiertsein.

"Zentrale Rechnungserfassung"

In einem Krankenhaus wurde die sog. "Zentrale Rechnungserfassung" eingeführt, um die Rechnungen in der eingehenden Post schneller bearbeiten zu können. In einer Hausmitteilung wurde dazu ausgeführt, daß "jede Postsendung, die nicht mit dem Vermerk ´persönlich` versehen ist und eine Rechnung enthalten könnte, geöffnet wird." Ein Petent hat daraus geschlossen, daß prinzipiell alle Postsendungen ohne den Vermerk "persönlich" geöffnet werden und deshalb die Daten von Patienten nicht genügend geschützt sind. Er bat mich um eine datenschutzrechtliche Prüfung des Verfahrens.

Auf meine Anfrage beim Verwaltungsdirektor des Krankenhauses erhielt ich die Antwort, daß diese Verfahrensweise deshalb beibehalten werden soll, weil sie die Ordnungsmäßigkeit des Postablaufes verbessere. Im übrigen sei die Anregung und Aufforderung, so zu verfahren, aus Krankenhäusern der alten Bundesländer gekommen.
Eine entsprechende Nachfrage bei meinen Kollegen ergab, daß es auch nach ihrer Auffassung unzulässig ist, Postsendungen zu öffnen, die unmittelbar an eine namentlich benannte Person im Krankenhaus adressiert sind. Es besteht dann immer die Gefahr, daß Schreiben geöffnet werden, die Patientendaten enthalten. Solche Daten unterliegen aber einem besonderen Schutz, der aus der ärztlichen Schweigepflichtresultiert.

In einem mit dem Verwaltungsdirektor des Krankenhauses geführten Gespräch stellte sich allerdings heraus, daß die tatsächliche Verfahrensweise nicht so ist. Der Verwaltungsdirektor hat erklärt, daß nur Postsendungen geöffnet werden, die nicht an einen medizinischen Bereich oder eine namentlich benannte Person gerichtet sind und aus deren Adressierung hervorgeht, daß sie eine Rechnung enthalten könnten. Er hat aber eingeräumt, daß seine Hausmitteilung mißverständlich ausgelegt werden kann und eine Klarstellung zugesagt.

2.13 Personalwesen

2.13.1 Landesbesoldungsamt

Das Landesbesoldungsamt Mecklenburg-Vorpommern (LBA MV) in Neustrelitz verarbeitet Daten von ca. 42.000 Angestellten und ca. 9.000 Beamten und gehört hinsichtlich des Umfanges der zu verarbeitenden personenbezogenen Daten zu einer der größten öffentlichen Stellen in Mecklenburg-Vorpommern. Anfang 1991 nahm das LBA MV seine Arbeit auf und hat ab September 1991 alle Zahlfälle der vom Land beschäftigten Mitarbeiter des öffentlichen Dienstes berechnet.
Ich informierte mich während der Kontrolle über den Datenfluß, die Organisation sowie über die in den Abteilungen getroffenen organisatorischen, technischen und baulichen Datenschutzmaßnahmen. Im LBA MV wird das DV- und Organisationsprojekt des Landes Schleswig-Holstein zur Berechnung der Besoldung und Vergütung von Beamten und Angestellten verwendet. Jeder Mitarbeiter hat auf einen festgelegten Datenbereich Zugriff und kann nur den ihm zugewiesenen Bereich öffnen und auf dem Terminal einsehen. Ein differenziertes Paßwortsystem sichert den Zugriff. Das System fordert den Bearbeiter in bestimmten Abständen auf, sein Paßwort zu ändern. Schließlich werden stichprobenartig die im Zentralrechner gespeicherten Zugriffsdaten durch die Systemadministratoren ausgewertet. Das Zugriffsprotokoll wird zu Revisionszwecken aufbewahrt.

Im Ergebnis meiner Kontrolle konnte ich umfangreiche und gut wirksame Maßnahmen zur Einhaltung des Datenschutzes sowie einen insgesamt sorgsamen Umgang mit Akten und Schriftgut konstatieren.

2.13.2 Wie muß ein Erklärungs- oder Fragebogen aussehen?

Beschäftigte des öffentlichen Dienstes der neuen Bundesländer müssen viele Fragen zu ihrer Vergangenheit beantworten. Ich habe mich auch dazu öffentlich geäußert und darauf hingewiesen, daß ich diese Befragung unter bestimmten Voraussetzungen als notwendig erachte, gleichzeitig aber geltend gemacht, daß damit nicht das Datenschutzrecht in Frage gestellt werden darf.
Erklärungs- bzw. Fragebogen müssen grundsätzlich so präzise formuliert sein, daß der Betroffene weiß, was er in welchem Umfang anzugeben hat. Des weiteren ist der Betroffene gemäß § 8 Abs. 3 DSG MV über den Zweck der Erhebung, die Art und den Umfang der Verarbeitung und Nutzung der Daten sowie den Empfänger bei beabsichtigter Übermittlung aufzuklären.
Auch hier lassen sich die datenschutzrechtlichen Aspekte am besten am Beispiel einer Petition erläutern. Der Petent bezog sich auf einen Erklärungsbogen, den Polizisten abgeben sollten, die einen Antrag auf Übernahme in das Beamtenverhältnis gestellt hatten. Einige Formulierungen darin standen nicht im Einklang mit dem DSG MV bzw. dem LBG MV.

Meine Kritikpunkte und Empfehlungen dazu waren folgende:

1. Der Erklärungsbogen enthielt keine Anschrift der datenerhebenden und speichernden Stelle.
2. In einem einleitenden Satz sollte der Antragsteller bekunden, daß er kein hauptamtlicher oder inoffizieller Mitarbeiter des MfS/AfNS der ehemaligen DDR oder "vergleichbarer Institutionen" war. Der Begriff "vergleichbare Institutionen" ist aber nicht definiert, deshalb habe ich seine Streichung empfohlen.
3. Der Antragsteller sollte unterschreiben, daß er dem MfS/AfNS "keinen mündlichen oder schriftlichen Bericht" geliefert hat. Hierbei gibt es jedoch zu bedenken, daß Polizisten in der ehemaligen DDR von Dienst wegen zu berichten hatten. Deshalb habe ich empfohlen zu fragen, ob der Antragsteller unter einem "Decknamen" berichtet hat, also IM war, denn nur darum geht es bei dieser Erklärung.
4. Es war zu erklären, daß der Antragsteller "keine" Schweigeverpflichtung gegenüber dem MfS/AfNS abgegeben hat. Ich habe vorgeschlagen zu formulieren, daß keine "persönliche" Schweigeverpflichtung gegenüber dem MfS/AfNS abgegeben wurde, die über die Dienstschweigepflicht hinausging.
5. Der Antragsteller wurde aufgefordert zu bestätigen, daß er zu keiner Zeit "inoffizielle" Treffs mit Angehörigen des MfS/AfNS durchgeführt hat. Es ist aber eindeutiger, statt "inoffizielle Treffs" den Terminus "konspirative Treffs" zu verwenden.
6. Schließlich sollte erklärt werden, daß der Antragsteller dem MfS/AfNS "keine Räumlichkeiten" (auch keine dienstlichen) zur Verfügung gestellt hat. Es trägt der Realität des Polizeidienstes in der DDR besser Rechnung, wenn erklärt wird, daß "außer Diensträumen" keine weiteren Zimmer oder Wohnungen dem MfS/AfNS zur Verfügung gestellt wurden, denn selbstverständlich waren Polizisten der DDR verpflichtet, MfS-Mitarbeitern auf Anforderung Diensträume zur Verfügung zu stellen.
7. Der abschließende Satz des Erklärungsbogen lautete: "Mit der Überprüfung meiner personenbezogenen Daten bin ich einverstanden." Es wird darin nicht deutlich, wer die Überprüfung vornimmt und daß es sich nur um die Überprüfung der angegebenen und nicht aller personenbezogenen Daten handelt. Deshalb mein Vorschlag: "Mit einer Überprüfung obenstehender Angaben durch (Behörde/Institution) bin ich einverstanden."

Meine Empfehlungen wurden im Innenministerium berücksichtigt und der Erklärungsbogen entsprechend neu gestaltet.

Ich habe die Petition zum Anlaß genommen, die Erklärungen zur inoffiziellen/hauptamtlichen Mitarbeit beim MfS/AfNS von allen obersten Landesbehörden unter datenschutzrechtlichen Gesichtspunkten zu überprüfen. Es zeigte sich, daß die Inhalte der Erklärungen sehr unterschiedlich sind. So fragen einige Landesbehörden zum Beispiel nach der Mitgliedschaft und Funktion in einer Partei oder sogenannten Massenorganisation der ehemaligen DDR, andere nur nach einer Funktion in der SED oder in Massenorganisationen/gesellschaftlichen Organisationen. In allen mir zugegangenen Erklärungsbogen fehlte die Angabe der datenerhebenden und speichernden Stelle. Wegen der unterschiedlichen Inhalte dieser Erklärungen, die meines Erachtens nicht gerechtfertigt sind, empfehle ich, daß sich zumindest alle obersten Landesbehörden auf ein einheitliches und mit dem DSG MV konformes Muster einigen.

2.13.3 Wohin mit den Gauck-Bescheiden?

In den Personalämtern und -referaten der öffentlichen Stellen des Landes wurde diese Frage, besonders zu Beginn der Überprüfungen der Beschäftigten auf eine Mitarbeit beim MfS/AfNS, häufig gestellt. Da keine eindeutigen Regelungen existieren, werden sehr unterschiedliche Verfahrensweisenpraktiziert.
Nachdem ein Beschäftigter des öffentlichen Dienstes einen Erklärungsbogen ausgefüllt und bestätigt hat, kein hauptamtlicher oder inoffizieller Mitarbeiter des MfS/AfNS gewesen zu sein, wird durch die personalaktenführende Stelle eine Überprüfung beim Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (Gauck-Behörde) beantragt. Nach Abschluß der Recherchen wird von dort entweder ein Positivbescheid, d. h., es wurden Unterlagen gefunden, aus denen eine Mitarbeit beim MfS/AfNS ersichtlich ist, oder ein Negativbescheid, d. h., es liegen keine Erkenntnisse einer Stasi-Mitarbeit vor, erteilt. Der Negativbescheid ist jedoch nur vorläufig, weil die Erschließung der Akten noch nicht abgeschlossen ist und die Prüfroutine darum zu einem späteren Zeitpunkt wiederholt wird. Die Bescheide werden der beantragenden Stelle zugestellt. Sie ist für die weitere Behandlung der Bescheide verantwortlich.
Ich habe das Personalamt einer Stadt kontrolliert und mich über das dort übliche Verfahren informiert. Die von der Gauck-Behörde zugestellten Überprüfungsbescheide werden ausschließlich vom Personalleiter geöffnet. Bei negativen Bescheiden wird sowohl der Betroffene als auch eine von den Beschäftigten gewählte Kommission informiert und der Bescheid im versiegelten Umschlag in die Personalakte übernommen. Der Umschlag darf auch danach nur durch den Personalleiter geöffnet werden. Liegt dagegen ein positiver Bescheid vor, so spricht der Personalleiter zunächst mit dem Betroffenen und entscheidet nach Beratung mit der Kommission in Abhängigkeit von den konkreten Ergebnissen der Überprüfung und der Tätigkeit des Beschäftigten über eine Kündigung des Arbeitsverhältnisses oder eine Weiterbeschäftigung. In diesem Fall wird lediglich die Tagebuchnummer des Bescheides im geschlossenen Umschlag in die Personalunterlagen aufgenommen. Der Bescheid selbst wird an die Gauck-Behörde zurückgesandt.

Unter den gegebenen Umständen beurteile ich das Verfahren als eine datenschutzgerechte Lösung, die für den Betroffenen keine Beeinträchtigung seines informationellen Selbstbestimmungsrechtes darstellt und die Entscheidung der Personalstelle in notwendigen Ausnahmefällen nachvollziehbar macht. Allerdings sollten die Bescheide nicht unmittelbar Bestandteil der Personalakte sein, sondern in einer Sonderakte angelegt werden. Zu dieser Frage haben sich die Mitglieder der Arbeitsgruppe "Datenschutz in den neuen Bundesländern" verständigt. Der BfD hat als weiteres Argument zur gesonderten Aufbewahrung der Bescheide in der Personalabteilung angeführt, daß sie für die künftige Entwicklung des Beschäftigten, außer in sicherheitssensiblen Bereichen, nicht mehr relevant sein wird. Dieser Auffassung schließe ich mich an. Gleichzeitig würde ich es begrüßen, wenn auch hier eine landeseinheitliche datenschutzgerechte Regelung zur Aufbewahrung der Gauck-Bescheide in Kraft gesetzt werden könnte.

2.13.4 Wenn nun ein Beamter seine Miete nicht bezahlt?

Der folgende Fall erscheint mir sehr geeignet für die Erläuterung einiger Grundsätze des Datenschutzrechtes; ich werde ihn deshalb etwas ausführlicher darstellen.

Ich erhielt die Eingabe eines Beamten aus Schleswig-Holstein, der im Rahmen der Aufbauhilfe zeitweilig in einem Amt in Mecklenburg-Vorpommern tätig war. Während seines Aufenthaltes hatte er ein Zimmer angemietet. Vermieter dieses Zimmers war der Direktor des entsprechenden Landesamtes, an das der Beamte abgeordnet war. Folgerichtig wurde zwischen diesen beiden Parteien der Mietvertrag abgeschlossen. Im Laufe des Aufenthaltes des Beamten kam es dann zwischen dem Direktor und ihm zu Meinungsverschiedenheiten über die Höhe des Mietpreises. Der Streit nahm scharfe Formen an, was u. a. dazu führte, daß der Direktor des Landesamtes den Präsidenten des Amtes in Schleswig-Holstein - Dienstherr der abordnenden Dienststelle - über die Angelegenheit unterrichtete.

Datenschutzrechtlich handelt es sich hierbei um eine Übermittlung von personenbezogenen Daten. Der Umgang mit personenbezogenen Daten und damit auch diese Übermittlung ist gemäß § 6 DSG MV nur dann zulässig, wenn

1. die Vorschriften des Landesdatenschutzgesetzes von Mecklenburg-Vorpommern den Umgang mit personenbezogenen Daten zulassen oder
2. eine andere Rechtsvorschrift den Umgang mit personenbezogenen Daten erlaubt oder ihn zwingend voraussetzt oder
3. der Betroffene eingewilligt hat.

Eine Einwilligung des abgeordneten Beamten zur Datenübermittlung lag nicht vor. Ich bat den Direktor, mir mitzuteilen, auf welcher gesetzlichen Grundlage die Informationen über seine Mietstreitigkeiten mit dem Petenten an den Dienstherrn des Beamten übermittelt wurden. Er war der Auffassung, daß im vorliegenden Fall § 54 Satz 3 des Bundesbeamtengesetzes (BBG) - das Landesbeamtengesetz war zum Zeitpunkt der Abordnung noch nicht in Kraft - als Rechtsgrundlage für die Datenübermittlung anzusehen sei. In § 54 Satz 3 BBG heißt es: "Sein (des Beamten) Verhalten innerhalb und außerhalb des Dienstes muß der Achtung und dem Vertrauen gerecht werden, die sein Beruf erfordert". Danach unterliegt also das außerdienstliche Verhalten dann auch der dienstlichen Beurteilung, wenn es dienstliche Relevanz hat. Im vorliegenden Fall - so teilte mir der Direktor mit - erachtete er das eines Beamten unwürdige (außerdienstliche) Verhalten des abgeordneten Beamten als dienstlich relevant und sah es deshalb als seine Pflicht an, die entsprechenden Daten weiterzuleiten.

Unabhängig davon, ob hier das Verhalten des abgeordneten Beamten überhaupt als dienstlich relevant zu bewerten war, kann ich jedenfalls nicht der Auffassung folgen, daß § 54 Satz 3 BBG als Rechtsgrundlage für eine Datenübermittlung in Betracht kommt. Dazu müßte diese Vorschrift des Bundesbeamtengesetzes eine "andere Rechtsvorschrift, die den Umgang mit personenbezogenen Daten erlaubt oder ihn zwingend voraussetzt", i.S.d. § 6 Nr. 2 DSG MV darstellen.

Nun ist aber nicht jede Rechtsvorschrift eine solche "andere Rechtsvorschrift"; vielmehr muß diese "andere Rechtsvorschrift" - um das grundrechtlich geschützte informationelle Selbstbestimmungsrecht des einzelnen einschränken zu können - bestimmten verfassungsrechtlichen Anforderungen genügen, d.h. dem rechtsstaatlichen Gebot der Normenklarheit entsprechen und verhältnismäßig sein. Als "andere Rechtsvorschrift" kommt daher ohnehin nur ein Gesetz, eine Rechtsverordnung, ein Staatsvertrag oder eine (kommunale) Satzung, die auf einer gesetzlichen Ermächtigung beruht, in Betracht. Jede von diesen Rechtsvorschriften muß - wie bereits erwähnt - zudem den Umgang mit personenbezogenen Daten ausdrücklich für zulässig erklären. Für den einzelnen muß sich aus der Vorschrift klar und erkennbar ergeben, "für welche konkreten Zwecke des Verwaltungsvollzuges seine personenbezogenen Daten bestimmt und erforderlich sind" (aus dem sog. Volkszählungsurteil, BVerfGE 65, S. 1 (62)). Genau diese Anforderung wird jedoch von § 54 Satz 3 BBG nicht erfüllt. Mit keinem Wort ist in dieser Vorschrift eine Aussage zum Umgang mit personenbezogenen Daten getroffen. § 54 Satz 3 BBG kann daher - entgegen der Ansicht des Direktors des entsprechenden Landesamtes in Mecklenburg-Vorpommern - auch keine Rechtsgrundlage für eine Datenübermittlung darstellen.

Ebensowenig kommt § 31 Abs. 1 DSG MV als Rechtsgrundlage für die Übermittlung von Informationen über die Mietstreitigkeiten zwischen dem Petenten und dem Direktor des entsprechenden Landesamtes an den Präsidenten des gleichnamigen - abordnenden - Amtes in Schleswig-Holstein in Betracht. Nach § 31 Abs. 1 DSG MV dürfen öffentliche Stellen mit Daten ihrer Beschäftigten u.a. umgehen, wenn und soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher organisatorischer, sozialer oder personeller Maßnahmen erforderlich ist. Die hier in Rede stehende Übermittlung müßte also zum einen für den Direktor als übermittelnde Stelle im Rahmen der rechtmäßigen Erfüllung seiner Aufgaben erforderlich gewesen und zum anderen auf den gesetzlich festgelegten Zweck begrenzt geblieben sein. Dabei ist an das Kriterium der "Erforderlichkeit" ein strenger Maßstab anzulegen: Die Erforderlichkeit ist grundsätzlich nur dann gegeben, wenn die Aufgabe sonst gar nicht, nicht vollständig oder in nicht rechtmäßiger Weise erfüllt werden kann. Selbst wenn man nun davon ausgeht, daß die Übermittlung der Daten des Petenten zur Durchführung einer innerdienstlichen personellen Maßnahme - nämlich zur Verhinderung einer künftigen Abordnung des entsprechenden Beamten - erfolgen sollte, so war es jedenfalls nicht erforderlich, daß der Direktor des Landesamtes den Präsidenten des gleichnamigen Amtes in Schleswig-Holstein laufend über die Mietstreitigkeit als solche informiert; eine Mitteilung darüber, daß er von der zukünftigen Abordnung des entsprechenden Beamten absehen möge, hätte völlig gereicht.

Im Ergebnis war die Übermittlung der Informationen über die Mietstreitigkeiten zwischen dem Direktor des Amtes in Mecklenburg-Vorpommern und dem abgeordneten Beamten an den Präsidenten des Landesamtes in Schleswig-Holstein unzulässig. Darüber habe ich den Direktor belehrt.

2.13.5 Wer darf Personalvorgänge bearbeiten?

Ist diese Frage überhaupt erörterungsbedürftig? An sich nicht, denn Personalangelegenheiten werden von Mitarbeitern der Personalabteilung bearbeitet. Die gesetzlichen Regelungen dazu sind klar und eindeutig. Jeder Beschäftigte hat schließlich auch ein berechtigtes Interesse, daß seine in den Akten enthaltenen personenbezogenen Daten besonders geschützt werden und nur einem begrenzten Personenkreis verfügbar sind. Trotzdem beschwerte sich bei mir ein Mitarbeiter einer Behörde, daß mehrere Personalangelegenheiten - auch seine eigene - ohne Zustimmung der Betroffenen außerhalb des Personalreferats bearbeitet werden.
Der Hintergrund war, daß durch personelle Umbesetzungen innerhalb der Verwaltung der ehemalige Leiter des Personalreferates ein anderes Referat übernommen hatte. Der Direktor hat ihn aber angewiesen, einige von ihm schon angearbeitete Vorgänge abzuschließen. Nach meiner Anfrage beim Direktor zu den gesetzlichen Grundlagen dieser Verfahrensweise wurde die Weisung an den ehemaligen Leiter des Personalreferates sofort zurückgenommen und die Vorgänge wieder an das Personalreferat übergeben. Damit war die Sache selbst erledigt und von einer Beanstandung habe ich in diesem Fall Abstand genommen.
Trotz Rücknahme der ursprünglichen Entscheidung teilte mir der Direktor jedoch mit, daß er meiner Rechtsauffassung nicht folgen könne. Zunächst bezweifele er, daß § 31 DSG MV einschlägig sei. Nach seiner Auffassung gestatte § 100 Abs. 3 LBG MV die Bearbeitung der Personalakten auch außerhalb des zuständigen Referates.
Ich halte es für angebracht, an dieser Stelle darauf hinzuweisen, daß in Personalangelegenheiten bei größeren Behörden nicht nur die Abschottung nach außen, sondern sogar innerhalb des Personalreferates notwendig ist. Nicht jeder Sachbearbeiter darf Zugriff auf die Daten und Akten des gesamten Personalbestandes haben. Es sollte ihm ein Bereich zugewiesen werden, den nur er bearbeitet. In einer Vertretungsregelung ist festzulegen, auf welche weiteren Bereiche der Bearbeiter in AusnahmefällenZugriff haben darf.

2.14 Bildung, Kultur, Wissenschaftund Forschung

2.14.1 Sensible Daten - aber keiner weiß, wo sie sind

Im Zuge der Hochschulerneuerung konnte das wissenschaftliche Personal der ehemaligen DDR-Hochschulen die Weiterbeschäftigung an den staatlichen Hochschulen des Landes beantragen. Das entsprechende Verfahren ist im Hochschulerneuerungsgesetz (HEG MV) geregelt. Zur Vorbereitung der Entscheidungen war von Ehren-, Überleitungs- und Übernahmekommissionen zu prüfen, ob die im Gesetz genannten Voraussetzungen im Einzelfall erfüllt sind. Dazu wurden bei den Betroffenen personenbezogene Daten erhoben und in den Kommissionen sowie im Kultusministerium verarbeitet und genutzt. Außerdem wurden Gutachten über die Leistungen der Antragsteller in Lehre und Forschung von anerkannten Fachleuten auf Anforderung der Überleitungskommissionenangefertigt.

Ich hatte verschiedene Petitionen vorliegen, die es angebracht erscheinen ließen, den Umgang mit diesen Daten im Kultusministerium zu kontrollieren und durch eine Beratung weitere Beschwerden zu vermeiden. Meinen Besuch hatte ich zwei Wochen vor dem Termin bei der Kultusministerinschriftlichangekündigt und den Gegenstand der Kontrolle mitgeteilt.

Das Ministerium verfügt über Akten und Dateien mit personenbezogenen Daten aus der Arbeit der genannten Kommissionen. Ich konnte mich vom sachgemäßen und sorgsamen Umgang mit den Akten überzeugen. Die technisch-organisatorischen Maßnahmen sowie der bauliche Datenschutz entsprechen im wesentlichen dem erforderlichen Standard. Empfehlungen zur weiteren Verbesserung des Niveaus habe ich in meinem Bericht gegeben.

Einige Betroffene hatten Anträge auf Einsichtnahme der in den Überleitungsakten befindlichen Fachgutachten gestellt. Für ihre berufliche Entwicklung sind die Gutachten von besonderer Bedeutung, und es ist ihr gutes Recht, den Inhalt zur Kenntnis zu nehmen. Die Gutachten enthalten aber auch personenbezogene Daten der Gutachter. Deshalb waren sie erst nach Anonymisierung von den Antragstellern einzusehen. Dieses Verfahren entspricht den datenschutzrechtlichen Anforderungen und zeigt auch, welche Bedeutung das Kultusministerium dem Schutz der darin enthaltenen Daten beimißt.

Mit der Ankündigung meiner Kontrolle hatte ich um Zusendung der nach § 16 DSG MV vorzuhaltenden Dateibeschreibungen- und Geräteverzeichnisse gebeten. Diese Unterlagen wurden mir erst während meines Besuches übergeben. Sie enthalten die erforderlichen Angaben zur Struktur und zum Inhalt der Dateien sowie zur verwendeten Hardware. Die automatisierte Verarbeitung war zum Zweck der Kontrolle und Unterstützung der Vorgangsbearbeitung notwendig. Die Dateien befanden sich auf den Festplatten der Rechner und lagen in Form von Sicherungskopien auf Disketten oder Magnetbandkassetten vor. Die Zugriffsregelungen entsprachen den datenschutzrechtlichen Erfordernissen.
Die Dateien zu den Überleitungs- und Übernahmeverfahren konnte ich nicht kontrollieren, weil das verwendete Rechnernetz wegen Auflösung der Geschäftsstelle außer Betrieb gesetzt und demontiert worden war. Die Rechentechnik selbst befand sich in Obhut des IT-Referates in einem gesicherten Lagerraum des Ministeriums. Ein Konzept für die weitere Nutzung der sensiblen Daten durch das Personalreferat sollte noch erarbeitet werden. Meine Frage nach dem Ort der Aufbewahrung der Sicherungskopien - in diesem Fall der Magnetbandkassetten - konnte von niemandem beantwortet werden. Die Kopien waren trotz intensiver Suche der Verantwortlichen des IT-Referates während der Kontrolle nicht auffindbar. Erst Tage später erhielt ich einen Anruf, in dem mir mitgeteilt wurde, daß sich die Sicherungskopien nunmehr angefunden hätten. In meinem Bericht habe ich gegenüber der Kultusministerin allein deswegen eine förmliche Beanstandung gemäß § 28 DSG MV ausgesprochen. In einem abschließenden Gespräch mit dem Staatssekretär habe ich nochmals auf die Einhaltung der Bestimmungen des Datenschutzes hingewiesen und dringend empfohlen, einen internen Datenschutzbeauftragten zu benennen.

2.14.2 Frei verfügbare Datenfelder auch an der Uni

Eine beim Rektor der Universität Rostock schriftlich angekündigte Kontrolle sollte zeigen, ob beim Umgang mit personenbezogenen Daten der Studenten und Mitarbeiter die datenschutzrechtlichen Bestimmungen eingehalten werden. Zu Beginn der Kontrolle wurde mir mitgeteilt, daß wegen personeller Probleme bisher noch kein interner Datenschutzbeauftragter benannt wurde. Die im folgenden beschriebenen und bei meiner Kontrolle festgestellten Mängel belegen jedoch, wie wichtig er in dieser Einrichtung ist.

In den Dateibeschreibungen waren nicht ausreichende oder falsche Rechtsgrundlagen angegeben, bzw. es war nur die auf der jeweiligen Verwaltungsebene erlassene Dienstanweisung ohne Bezug zur geltenden gesetzlichen Grundlage genannt.

Bei der Überprüfung der Datenbankanwendung eines Dezernates stellte ich fest, daß nicht genutzte Datenfelder frei verfügbar waren. Bei weiteren Kontrollen in meinem Zuständigkeitsbereich habe ich dies in gleicher Weise in anderen Datenbanken vorgefunden (siehe Punkt 2.11.2). Frei zugängliche Datenfelder, die für die Erfüllung der Fachaufgabe nicht benötigt werden, schaffen Mißbrauchsmöglichkeiten und sind deshalb nicht zu billigen. Ich habe gefordert, daß durch die Programmentwickler die nicht benötigten Felder gesperrt werden.

Die Universität hat die in meinem Kontrollbericht angesprochenen Mängel inzwischen beseitigt und die Dateibeschreibungen überarbeitet sowie die Rechtsgrundlagen nunmehr richtig aufgeführt. Ein interner Datenschutzbeauftragter wurde vierzehn Tage nach meiner Kontrolle benannt.

2.14.3 Forschungsvorhaben und datenschutzrechtliche Bestimmungen

Im Berichtszeitraum habe ich mehrere Anträge zur Nutzung personenbezogener Daten für Forschungszwecke erhalten, hauptsächlich aus dem medizinischen und soziologischen Bereich. Ich schließe daraus, daß das in § 30 DSG MV normierte Genehmigungsverfahren sowohl bei den Antragstellern als auch bei den Behörden noch nicht hinreichend bekannt ist. Deshalb werde ich demnächst eine Informationsschrift zu diesem Thema herausgeben.

Grundsätzlich können personenbezogene Daten, die zu einem bestimmten Zweck erhoben wurden, ohne Einwilligung des Betroffenen für ein Forschungsvorhaben nur dann genutzt werden, wenn die zuständige oberste Aufsichtsbehörde die Genehmigung erteilt und wenn

1. die schutzwürdigen Belange des Betroffenen wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Nutzung nicht beeinträchtigt werden
   oder
2. die zuständige oberste Aufsichtsbehörde festgestellt hat, daß das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen erheblich überwiegt und der Zweck nicht anders erreicht werden kann.

Weiterhin ist zu beachten, daß die personenbezogenen Daten zu anonymisieren sind, sobald der Forschungszweck erfüllt ist. Bis dahin aber sind die personenidentifizierenden Merkmale gesondert zu speichern. Die Genehmigung des Forschungsvorhabens ist dem LfD gem. § 30 Abs. 2 Satz 2 DSG MV von der obersten Aufsichtsbehörde mitzuteilen.

In der medizinischen Forschung werden häufig Daten beim Betroffenen mit dessen Einwilligung erhoben und anschließend für wissenschaftliche Zwecke verarbeitet und genutzt. In solchen Fällen sind die in den §§ 6 bis 19 DSG MV enthaltenen allgemeinen Bestimmungen zum Umgang mit personenbezogenen Daten und zum Inhalt der Einwilligungserklärung zu beachten. Eine Genehmigung von den zuständigen obersten Aufsichtsbehörden wird aus datenschutzrechtlicher Sicht hier nicht ausdrücklich verlangt.

Mißverständnisse habe ich auch zum Geltungsbereich von Einwilligungen vorgefunden. Wird die Verarbeitung oder Nutzung personenbezogener Daten für einen anderen Zweck beabsichtigt, z. B. wenn Patientendaten eines Krankenhauses für ein bestimmtes Forschungsvorhaben genutzt werden sollen, ist entweder eine erneute Einwilligung einzuholen oder für das Forschungsvorhaben nach dem zuerst beschriebenen Verfahren die Genehmigung zu beantragen.

Eine Veröffentlichung von personenbezogenen Daten aus Forschungsvorhaben bedarf ebenfalls immer der Einwilligung des Betroffenen. Gegen die Veröffentlichung aggregierter Daten, z. B. in Form von Statistiken, bestehen aus datenschutzrechtlicher Sicht hingegen keine Bedenken. Voraussetzung ist allerdings, daß aus dem Material kein Personenbezug hergestellt werden kann.

2.14.4 Noch immer kein Archivgesetz - so geiht dat nich, Fru Ministerin !

Eine besondere Form der Altlasten in den neuen Bundesländern sind personenbezogene Daten, die von Behörden der ehemaligen DDR erhoben, verarbeitet und genutzt wurden, nun aber von den öffentlichen Stellen nicht mehr benötigt werden. Sie werden auch als Altdaten bezeichnet und befinden sich in Akten, aber auch auf Datenträgern wie Disketten und Magnetbändern. Teilweise wurde mit diesen alten Beständen sorglos umgegangen und oft fehlte den Behörden der notwendige Platz, um sie sicher aufzubewahren. Ich wurde häufig gefragt, was damit geschehen soll.

Das DSG MV enthält zwar grundlegende Bestimmungen zur Festlegung der zuständigen Stelle für die Daten ehemaliger Einrichtungen, aber eine bereichsspezifische gesetzliche Regelung für historisches Material kann es freilich nicht ersetzen - das kann nur ein Landesarchivgesetz. Mecklenburg-Vorpommern hat als einziges der neuen Länder noch nicht einmal einen Regierungsentwurf für ein Archivgesetz. Anhand zweier Petitionen möchte ich die durch das Fehlen eines Landesarchivgesetzes aufgetretenen Schwierigkeiten darlegen.

Im Dezember 1992 wurde mir von einem Ausschußvorsitzenden eines zeitweiligen Untersuchungsauschusses des Kreistages S. mitgeteilt, daß man bei der Suche nach Akten über geplante Internierungslager auf Schriftstücke der ehemaligen Abteilung Inneres, Referat Kirchenfragen, gestoßen sei. Die Schriftstücke enthielten u.a. Spitzelprotokolle über kirchliche Mitarbeiter und die Tätigkeit kirchlicher Organisationen. Die betroffenen Pastoren hatten ein Interesse daran, das gesammelte Material einzusehen.

Der Ausschußvorsitzende hatte sich mit seinen Fragen zur weiteren Behandlung der Akten und den Modalitäten der Einsichtnahme durch die Betroffenen bereits an die Gauck-Behörde gewandt, konnte dort allerdings keine Klärung erreichen und hat mich deshalb gebeten, Antworten auf die Fragen zu finden. Weil es heute ein Referat Kirchenfragen in den Kreisverwaltungen nicht gibt, habe ich gemäß § 34 Abs.1 DSG MV den Innenminister gebeten, die zuständige öffentliche Stelle für die Akten zu bestimmen. Des weiteren hatte ich im Kultusministerium über den Stand der Gesetzgebung zum Landesarchivgesetz nachgefragt und um die Zusendung eines Entwurfes gebeten, falls ein solcher vorliegt.
Ende März 1993 wurde mir vom Innenminister als zuständige speichernde Stelle das Kultusministerium benannt. Im April habe ich schließlich beim Kultusministerium nachgefragt, unter welchen Voraussetzungen die Betroffenen Einsicht nehmen können und darauf hingewiesen, daß in den Schriftstücken personenbezogene Daten von Dritten enthalten sind. Im Juli wurde durch das Kultusministerium der weitere Umgang mit den Akten unter Berücksichtigung der Interessen der Betroffenen entschieden. Ein Landesarchivgesetz hätte diesen umständlichen und zeitaufwendigen Weg erspart.

In einem anderen Fall bat mich ein Mitarbeiter des Landeshauptarchivs Schwerin in folgender Angelegenheit um Rat:
Ein Journalist des NDR wollte anläßlich des Jahrestages (12. Dezember 1986) des Absturzes eines sowjetischen Flugzeuges, das mit einer Schulklasse von Schweriner Kindern besetzt war, einen Fernsehbeitrag senden. Bei diesem Absturz kamen 19 Kinder ums Leben. Es wurde damals gemutmaßt, daß der Pilot betrunken gewesen sei.
Es ging dem Journalisten nach eigenem Bekunden allein um die Darstellung, wie damals DDR-Behörden versucht haben sollen, die Umstände, die zu dem Flugzeugabsturz führten, zu vertuschen. Zu diesem Zwecke begehrte er nun Einsicht in archivierte Akten, die vom Rat des Bezirkes Schwerin durch das Landeshauptarchiv übernommen worden waren (ca. 80 - 100 Seiten).
Es stellten sich hier gleich mehrere Fragen, die sowohl datenschutzrechtliche als auch archivrechtliche Aspekte tangieren. Zum Hintergrund:

Grundsätzlich wird Archivgut 30 Jahre nach Entstehung der Unterlagen für die Benutzung freigegeben. Unbeschadet dieser allgemeinen Schutzfrist dürfen Akten und Daten, die sich auf natürliche Personen beziehen (personenbezogenes Archivgut) erst nach einer bestimmten Zeit nach dem Tod (die Fristen hierfür sind in den einzelnen Archivgesetzen der Länder unterschiedlich geregelt) durch Dritte genutzt werden. Nach dem Willen des Gesetzgebers (§ 2 a des Gesetzes zur Änderung des Bundesarchivgesetzes vom 13. März 1992, BGBl. 1992, Teil I, S. 506) soll jedoch für Unterlagen der Sozialistischen Einheitspartei Deutschlands (SED), der mit dieser Partei verbundenen Massenorganisationen und juristischen Personen nicht die 30-jährige Schutzfrist gelten. Sinn und Zweck dieser Gesetzesnovellierung war und ist es, die Aufarbeitung der DDR-Geschichte nicht zu behindern. Die vorstehend genannten Archivmaterialien sollen ohne lange Schutzfristen den Bürgern bei Vorliegen eines berechtigten Interesses grundsätzlich offenstehen. Wenn man also danach zu dem Ergebnis käme, daß die 30-jährige Frist nicht greift, ist fraglich, ob eine weitere zeitliche Frist - beispielsweise 10 Jahre nach Tod - einzuhalten ist. Von einer solchen Bestimmung kann dann wieder eine Ausnahme gemacht werden, wenn die Einsichtnahme bzw. Nutzung des Archivgutes im öffentlichen Interesse liegt. Wiederum wird in einem solchen Fall unterschieden, ob es sich um personenbezogenes oder nicht personenbezogenes Archivgut handelt. Im konkreten Fall waren also sehr unterschiedliche rechtliche Probleme und Interessen abzuwägen:

Nicht nur die Interessen des Journalisten, sondern auch die Interessen der Eltern der verunglückten Schulkinder sind zu berücksichtigen. Es können hier nur Vermutungen angestellt werden, ob diese an einer Aufklärung interessiert sind oder ob sie einer Berichterstattung eher ablehnend gegenüber stehen.
Angesichts des ohne Landesarchivgesetz weitgehend rechtsfreien Raumes, habe ich empfohlen, dem Journalisten allenfalls Fotokopien zur Verfügung zu stellen, in denen alle personenbezogenen Daten anonymisiert sind. Das Landeshauptarchiv hatte, da die Entscheidung kurzfristig zu treffen war, wegen des Verwaltungsaufwandes, der mit einer Anonymisierung verbunden gewesen wäre, folgende Lösung gewählt: Die Akten, die keine personenbezogenen Daten enthielten, wurden dem Journalisten zur Einsicht überlassen. Aus den Archivunterlagen, in denen personenbezogene Daten vorhanden waren, wurde ihm der Inhalt der Unterlagen von einer Mitarbeiterin des Archivs - ohne Nennung von Namen - vorgetragen. Gegen diese Verfahrensweise hatte ich aus datenschutzrechtlicher Sicht keine Bedenken; aber viele Überlegungen wären uns erspart geblieben, wenn wir ein Landesarchivgesetz hätten.

Die bestehende Rechtsunsicherheit sowohl beim Archivpersonal als auch bei den Bürgern macht es dringend erforderlich, ein Landesarchivgesetz in Kraft zu setzen. Leider hat die Kultusministerin noch im September 1993 keinen Handlungsbedarf hierfür gesehen. Fru Ministerin - so geiht dat nich.

2.15 Umwelt, Landwirtschaft

2.15.1 InVeKoS - The big eye in space?

Das Integrierte Verwaltungs- und Kontrollsystem (InVeKoS) soll vor allem die verwaltungstechnischen Probleme bei verschiedenen Regelungen für flächenbezogene Beihilfen in der Landwirtschaft lösen helfen. Hierzu werden in den Ländern der Europäischen Gemeinschaft (EG) Datenbanken eingerichtet und die Antragsdaten der Betriebe gespeichert. Dazu gehört ein System zur Identifikation des Betriebsinhabers, der Flächen und der Tiere sowie die Forderung nach einer wirksamen Kontrolle. Der Mindestanteil der jährlich stichprobenartig zu kontrollierenden Betriebe soll 5 % betragen, eine Obergrenze ist nicht festgelegt. Die Kontrolle kann durch Fernerkundung mittels Satellit oder als eine direkte Kontrolle der Betriebe erfolgen. Die Fernerkundung wird finanziell gefördert, doch wegen der dennoch hohen Kosten wurde sie bisher nur zu Testzwecken angewendet.
Bei Bekanntwerden der EG-Verordnung wurden von den Datenschutzbeauftragten des Bundes und der Länder erhebliche Bedenken dahingehend geäußert, daß versucht wird, über eine Datenbank alle landwirtschaftlichen Betriebe mit ihren Wirtschaftsdaten zu erfassen und u.U. großflächig und lückenlos aus der Luft zu kontrollieren. Die Datenbanken werden gegenwärtig zweckgebunden nur auf Länderebene eingerichtet. Eine Übermittlung an das Bundesministerium für Landwirtschaft (BML) und an die EG-Kommission erfolgt nur in aggregierter Form, also nicht personenbezogen.
Die Gefahr einer überproportionalen Kontrolle besteht aber weiterhin, zumal die Entwicklung des Systems noch nicht abgeschlossen ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung hierzu Stellung genommen (siehe Anlage 8).

2.15.2 Umweltinformationen

Umweltinformationen sind immer dann mit dem Datenschutzrecht in Einklang zu bringen, wenn sie personenbezogene Daten, z. B. von Verursachern, enthalten. Grundsätzlich hat nach Art. 6 Abs 3 der vorläufigen Verfassung des Landes Mecklenburg-Vorpommern jeder das Recht auf Zugang zu Informationen über die Umwelt, die bei öffentlichen Stellen des Landes vorliegen. Bereits hier wird auf den Zusammenhang zwischen Informationsrechten und Datenschutzvorschriften hingewiesen. Spezialgesetzliche Regelungen zum Recht auf Zugang zu Informationen über die Umwelt wurden erstmals in der EG-Umweltrichtlinie vom 07. Juni 1990 (90/313/EWG) normiert. Diese Richtlinie ist allerdings noch nicht in nationales Recht umgesetzt worden. Gegenwärtig befindet sich das Umweltinformationsgesetz des Bundes (UIG) noch in der Abstimmung, wobei nicht abzusehen ist, wann es in Kraft treten wird. In unserem Land ist darum ein gemeinsamer Erlaß des Umwelt-, Innen-, Wirtschafts-, Landwirtschafts-, Kultus- und Sozialministeriums zur Umsetzung der EG-Richtlinie seit dem 1.1.1993 zwischenzeitlich gültig, der dem Datenschutzrecht genügt.

2.16 Automatisierte Datenverarbeitung

Nach § 17 DSG MV sind alle öffentlichen Stellen, die personenbezogene Daten automatisiert verarbeiten, zu einer Reihe technisch-organisatorischer Maßnahmen verpflichtet, die den datenschutzgerechten Betrieb von DV-Anlagen sicherstellen sollen.
Bei einigen Beratungs- und Kontrollbesuchen habe ich auf diesem Gebiet Mängel festgestellt. Dazu gehören insbesondere bauliche Unzulänglichkeiten wie ungeeignete Türen, fehlende Fenstergitter, unzureichende Einbruchs- und Feuermeldeanlagen (s.a. Abschnitt 2.19.) sowie organisatorische Defizite bei der Paßwortvergabe und der Erarbeitung von Dienstanweisungen.

Die Ursachen für organisatorische Defizite liegen zumeist bei der Verwendung von DV-Projekten, die die Benutzer- und Zugriffskontrolle nicht in dem gewünschten Umfang realisieren. Eine Nachbesserung ist infolge des hohen finanziellen Aufwandes häufig nicht mehr möglich. Andererseits wurden oft schon die vorhandenen Möglichkeiten des Betriebssystems und der Anwendungen nicht genutzt, weil die Kenntnisse der Systemverwalter ungenügend waren.

2.16.1 Speicher- und Benutzerkontrolle

Um den unbefugten Zugriff auf personenbezogene Daten zu verhindern, muß jeder Benutzer eine eigene Benutzerkennung und ein persönliches Paßwort erhalten. Nur so ist anhand von Protokollauswertungen zweifelsfrei nachvollziehbar, wer wann welche Aktivitäten ausgelöst hat. Dem Benutzer sollte angezeigt werden, wann seine Kennung zuletzt verwendet wurde. Bei längerem Nichtbenutzen des Terminals sollte sich der Bildschirm verdunkeln und die Weiterarbeit erst nach Eingabe des persönlichen Paßwortes möglich sein.
Die Vergabe des persönlichen Paßwortes muß durch jeden Benutzer selbst erfolgen. Dabei kann die Geltungsdauer (4 - 8 Wochen) oft schon vom System vorgegeben werden, ebenso die Mindestlänge (6 - 8 Stellen) und die Information, nach wieviel Paßwortgenerationen eine Wiederholung möglich ist. Sinnvoll ist eine automatische Prüfung auf Trivialität. Bestehen diese Möglichkeiten systemseitig nicht, müssen entsprechende organisatorische Regelungen getroffen werden. Das persönliche Paßwort darf weder schriftlich festgehalten noch darf die Paßwortkontrolle umgangen werden können. Wie ich bei einer Kontrolle festgestellt habe, wurde aber gerade diese Möglichkeit dauerhaft genutzt.
Paßwort und Benutzername sind in Dateien zu speichern, die nur dem Systemverwalter zugänglich sind. Nur er hat die Möglichkeit, ein vergessenes persönliches Paßwort durch ein neues zu ersetzen. Bei Anwendungen zur Verarbeitung besonders sensibler personenbezogener Daten ist für Systemverwaltungsfunktionen das Vier-Augen-Prinzip anzuwenden. In jedem Fall ist das Systempaßwort für Vertretungsfälle in einem verschlossenen Umschlag sicher zu hinterlegen. Um das unbefugte Benutzen zu erschweren, sind Zeitsperren nach mehrfachen fehlerhaften Anmeldeversuchen ein wirksamer Schutz. Ein häufiger Mangel in der Systemverwaltung ist das Beibehalten der von der Installation oder der vom Betriebssystem vorgegebenen Paßwörter. Für das sofortige Ändern dieser Standardpaßwörter nach Systemübergabe ist der Systemadministrator verantwortlich.

2.16.2 Zugriffs- und Eingabekontrolle

Zugeordnet zu seiner Benutzerkennung sollte jeder Benutzer nur die für seine Arbeit nötigen Zugriffsrechte erhalten. In Verbindung mit seinem Paßwort ist dann eine eindeutige Zuordnung der Anwendung sowie die Erteilung von Rechten wie Lesen, Schreiben und Ändern von Daten möglich. Die Aktivitäten sind in einer Protokolldatei zu speichern und mindestens ein Jahr lang aufzubewahren. Der Umfang der Aufzeichnung richtet sich nach der Sensibilität der Daten und kann Aktivitäten von der An- und Abmeldung im System bis zur Registrierung jedes Lese- und Schreibzugriffs umfassen. Dabei gilt der Grundsatz: Nur soviel wie nötig! Entsprechend der Sensibilität sollte nur aufgezeichnet werden, wofür auch Kontrollpflichten bestehen. Ausreichend Speichermöglichkeiten müssen vorhanden sein.
Um Protokolldateien effektiv auswerten zu können, sollten sie in einem solchen Format erzeugt werden, das Recherchen in Standarddatenbanken (z. B. Paradox als Landesstandard) ermöglicht. So wird die Bereitschaft zur regelmäßigen Auswertung gefördert. Lange Protokollisten müssen dann nicht mehr mit viel Zeitaufwand "zu Fuß" nach bestimmten Ereignissen durchsucht werden.

2.16.3 Datenträgerkontrolle

Datenträger müssen in dafür geeigneten feuer- und einbruchssicheren Schränken aufbewahrt werden. Eine vernünftige Lösung sind feuersichere Einsätze für normale Sicherheitsschränke. Die Datenträger sind zu kennzeichnen, zu inventarisieren und nur befugten Personen gegen Nachweis auszuhändigen. Bei meinen Kontroll- und Beratungsbesuchen mußte ich feststellen, daß der Datenträgerkontrolle in vielen Fällen noch nicht genug Aufmerksamkeit geschenkt wird. Ein Beispiel hierfür habe ich in Punkt 2.14.1 geschildert.
Auch hinsichtlich der aus verschiedenen Gründen notwendigen Löschung von Datenträgern sind große Unsicherheiten zu verzeichnen. Sollen z. B. Disketten oder Magnetbänder, auf denen personenbezogene Daten gespeichert waren, für andere Zwecke wiederverwendet werden, sind diese physisch durch zerstörendes Formatieren oder mittels starker Magnetfelder (entsprechende Löschgeräte werden im Handel angeboten) zu löschen. Wenn Datenträger vernichtet werden sollen und eine lückenlose Kontrolle der Vernichtung (z. B. mechanische Zerkleinerung) bei einen Auftragnehmer nicht möglich ist, muß vorher ebenfalls gelöscht werden. Bei der Mehrzahl der Entsorgungsunternehmen ist jedoch eine vom Auftraggeber kontrollierte Vernichtung möglich. Allerdings ist dann der Transport in eigener Verantwortung durchzuführen. Für den Großanwender lohnen sich eventuell eigene Zerkleinerungs- oder Löschgeräte.
Zu einem besonderen Problem kann die Löschung von Festplatten werden. Dafür sind spezielle Programme und vor allem viel Zeit erforderlich. Eine besonders kritische Situation ist der Defekt einer Festplatte. Eine Reparatur ist, wenn auch mit hohem Aufwand, durchaus denkbar. Eine vorherige Löschung über das System ist allerdings oft nicht mehr möglich und kann deshalb nur durch mechanische Zerstörung oder mit speziellen Löschgeräten erfolgen, die die magnetische Abschirmung überwinden. Während der Garantie ist dieser Weg durch Restriktionen des Garantiegebers normalerweise ausgeschlossen. Hier ist durch entsprechende Verträge (§ 11 BDSG, § 4 DSG MV) die Löschung zu vereinbaren. Da sich die Hersteller oft im Ausland befinden, wo nicht die gleichen Datenschutzregelungen gelten, ist abzuwägen, ob bei besonders sensiblen Daten auf den Austausch im Rahmen der Gewährleistung verzichtet werden sollte.

2.16.4 Organisationskontrolle

In öffentlichen Stellen sollten die Maßnahmen zur Sicherung eines datenschutzgerechten Arbeitsablaufs in Dienstanweisungen geregelt sein. Der Maßnahmenkatalog reicht von der Festlegung der Rechte und Pflichten des Datenschutzbeauftragten, der Verpflichtung der Mitarbeiter auf das Datengeheimnis, den technisch-organisatorischen Maßnahmen bis hin zu den Richtlinien für die Programmentwicklung, -tests und -freigabe.

Dienstanweisungen nützen jedoch wenig, wenn sie nicht umgesetzt werden und ihre Einhaltung nicht kontrolliert wird. Es sind deshalb interne Kontrollinstanzen einzurichten, die mit den nötigen Befugnissen auszustatten sind. Geeignet hierfür ist der interne Datenschutzbeauftragte. In kleineren Dienststellen kann aber auch die Beratung und Kontrolle durch den Datenschutzbeauftragten der übergeordneten Dienststelle erfolgen.

2.16.5 Viren

Wie auch Untersuchungen meiner Kollegen in den anderen Ländern zeigen, sind Computerviren eine ernst zu nehmende Gefahr für die Datensicherheit. Zum vorbeugenden Schutz kann nur immer wieder auf organisatorische Maßnahmen hingewiesen werden. Die wichtigsten sind:

- Einsatz von Virensuchprogrammen zur Überprüfung von PC und Disketten,
- keine Nutzung privater Disketten,
- keine private Nutzung von dienstlichen Disketten,
- keine Nutzung von Programmdisketten ohne Schreibschutz,
- Einsatz von Sicherheitssoftware an Einzelplatz-PC.

Bei meinen Kontrollen mußte ich feststellen, daß diesem Thema keine oder nur geringe Aufmerksamkeit geschenkt wurde. In den meisten Fällen war weder eine Antivirensoftware noch eine entsprechende Dienstvorschrift vorhanden.

2.16.6 Datenfernverarbeitung

Verschiedene Ämter und Krankenkassen, aber auch die OFD und Finanzämter, nutzen schon jetzt die Möglichkeiten der Datenfernübertragung zur Bearbeitung ihrer Fachaufgaben in einem Rechenzentrum. Dabei wird oft übersehen, daß der Auftraggeber grundsätzlich für seine Daten und für die Einhaltung des Datenschutzes gem. § 4 DSG MV verantwortlich bleibt. Deshalb müssen auch diese Stellen, selbst wenn sie ihre Daten nicht vor Ort speichern, die nach § 16 DSG MV geforderten Dateibeschreibungen und Geräteverzeichnisse vorhalten (s.a. Punkt 2.11.4).

Ein Schwachpunkt aus der Sicht des Datenschutzes ist die Sicherheit der Datenfernübertragung über Telefonleitungen. Als relativ unproblematisch sind Standleitungen anzusehen, da die geschaltete Telefonverbindung und damit der Kommunikationspartner bekannt ist. Anders ist das bei Wählleitungen. Hier ist eine gesicherte Identifizierung der Wählpartner nicht möglich. Durch Manipulieren und Probieren können Gerätekennungen simuliert und Paßworte überwunden werden. Größere Sicherheit schafft nur ein Verbindungsaufbau durch die zentrale Verarbeitungsstelle mittels Einsatz automatischer oder manueller Rückrufverfahren. Oben gesagtes gilt ebenso für den Verbindungsaufbau zur Fernwartung von DV-Systemen (s.a. Punkt 2.21.4).

2.16.7 Kryptografie

Ab einer bestimmten Sensibilität der Daten (z. B. bei sicherheitsrelevanten Daten oder Sozial- und Gesundheitsdaten) sollten bei der automatisierten Datenverarbeitung Verschlüsselungsverfahren angewendet werden. Das gilt insbesondere für den Transport. Bei der Verwendung von Datenträgern (Disketten, Magnetbänder) und bei der Datenfernübertragung (s.a. Punkt 2.16.6) ist die Gefahr des Verlustes, des unberechtigten Kopierens und der unberechtigten Kenntnisnahme von personenbezogenen Daten besonders groß.

In einer Beratung zum Aufbau des Tumorzentrums Rostock, welches im weiteren Ausbau ausgewählten Ärzten den Zugriff auf den Datenbestand über Modem und Telefonleitungen gestatten will, spielte dieses Thema beispielsweise schon eine Rolle (s.a. Punkt 2.12.6). Dem Datenschutz muß gerade in diesem Bereich besondere Beachtung geschenkt werden. Technische Möglichkeiten sind vorhanden, um in angemessener Weise den Schutz besonders sensibler Daten zu gewährleisten. Die Industrie bietet Hard- und Software an, die leicht zu handhaben und preiswert ist.

2.17 Umgang mit Schriftgut in konventionellen Akten

Akten sind vorwiegend in Schriftform vorliegende, dienstlichen oder amtlichen Zwecken dienende Unterlagen, die nicht nach bestimmten Merkmalen geordnet oder ausgewertet werden können. Sie unterliegen nach §§ 3 Abs. 3 und 17 Abs. 3 i.V.m. § 26 Abs. 1 DSG MV ebenfalls meiner Kontrolltätigkeit. Vor allem zur Frage der Schriftgutvernichtung gab es im Berichtszeitraum besonders krasse Fälle der Verletzung datenschutzrechtlicher Bestimmungen, so daß ich zu Beanstandungen gezwungen war.

2.17.1 Schriftgutlagerung

In den Amtsstuben reichte das Spektrum der vorgefundenen Aufbewahrungsmöglichkeiten von offenen Karteikästen bis zu stabilen, mit Sicherheitsschlössern versehenen Aktenschränken.
Selbstverständlich muß auch bei Akten eine ordnungsgemäße Zugangskontrolle gewährleistet sein. Mitarbeiter dürfen nur zu solchen Akten Zugang haben, die sie zur Erfüllung ihrer Aufgabe benötigen. Dafür sind verschließbare Behältnisse erforderlich.
Auf vielfach vorhandene Mißstände diesbezüglich wurde von Mitarbeitern der von mir kontrollierten öffentlichen Stellen immer wieder hingewiesen. In den meisten Fällen war offensichtlich eine ausreichende Sensibilität für Fragen des Datenschutzes vorhanden, so daß vorhandene Mängel zwar erkannt wurden, aber nicht abgestellt werden konnten, weil die dafür nötigen finanziellen Mittel fehlten. Natürlich sind auch finanzielle Aufwendungen notwendig, denn ein feuersicherer Aktenschrank läßt sich nun mal nicht durch organisatorische Regelungen ersetzen.

2.17.2 Schriftgutvernichtung - Stiefkind des Datenschutzes?

Die Ursache für den häufig recht sorglosen Umgang mit Akten ist jedoch nicht immer fehlende finanzielle Ausstattung. In einigen Fällen führt die Unterschätzung der Datenschutzproblematik zu organisatorischen Defiziten, wie die folgenden drei Beispiele zeigen:

Der Ministerialrat auf dem Müll

So oder so ähnlich wird wohl der Titel eines Buches lauten, in welchem ein Schriftsteller seinen "Aktenfund" auf der Mülldeponie bei Hohen Viecheln verwerten will.

Ich hatte einen Hinweis erhalten, daß Schriftstücke auf einer Mülldeponie gefunden worden waren, die personenbezogene Daten enthielten und deren Inhalt darauf hindeutete, daß sie aus unserem Innenministerium stammten. Eine erste Sichtung ergab, daß es sich bei den meisten Schriftstücken um Entwürfe zu Schreiben, Doppelexemplare und handschriftliche Vermerke handelte. Im einzelnen ging es u. a. um eine komplette Klageschrift, um ein Schreiben an Landräte zum Asylverfahrensgesetz, ein Telefax der Rostocker Polizeidirektion zu dem Überfall auf ein Asylbewerberheim und einen handschriftlichen Brief eines Ministerialrats a.D. an den damaligen Innenminister, in welchem in ironischer Weise die Verbeamtungspraxis in Mecklenburg-Vorpommern kommentiert wird.

Der Fund veranlaßte mich, am darauffolgenden Tag im Innenministerium eine Kontrolle durchzuführen. Ziel der Kontrolle war es, die einzelnen Schriftstücke den entsprechenden Akten zuzuordnen, diese auf Vollständigkeit zu überprüfen und, wenn möglich, den weiteren Weg der Schriftstücke aus dem Innenministerium zur Mülldeponie zu verfolgen.

Die Kontrolle ergab, daß es sich bei dem Fund um Papierkorbinhalte aus dem Innenministerium handelte. Daraufhin habe ich im wesentlichen folgende Schwachstellen bzw. organisatorische Mängel bei der Vernichtung von Schriftgut festgestellt und beanstandet:

Zunächst einmal bestand zwischen dem Innenministerium und der mit der Vernichtung des Altpapiers beauftragten Entsorgungsfirma lediglich eine mündliche Vereinbarung zur Entsorgung des Altpapiers als Sonderabfall "Schriftgut". Es hätte jedoch ein schriftlicher Vertrag abgeschlossen sein müssen, in dem genau festzulegen gewesen wäre, durch welche technischen Mittel und nach welchem Verfahren die Unterlagen zu vernichten sind. Der Auftraggeber hätte im weiteren darauf achten müssen, einen Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen auszuwählen. Da kein schriftlicher Vertrag existierte, in dem die Entsorgungsfirma detailliert auf ihre Pflichten hingewiesen wird, ist dementsprechend auch die Eignung der von dem Unternehmen getroffenen technischen und organisatorischen Maßnahmen nur schwer zu überprüfen bzw. zu kontrollieren gewesen. Soweit es sich bei dem Auftragnehmer um eine nicht-öffentliche Stelle handelt, hätten die mit dem Vernichten beschäftigten Personen bei der Aufnahme der Tätigkeit auf das Datengeheimnis verpflichtet werden müssen. Des weiteren hätte schriftlich vereinbart werden müssen, in welchem Zustand sich die Unterlagen zu befinden haben, um als vernichtet zu gelten. Das Innenministerium hat es unterlassen, selbst ein Verfahren zu wählen, z. B. Zerkleinerung des Schriftgutes, um zu verhindern, daß eine Kenntnisnahme personenbezogener Daten durch Dritte tatsächlich ausgeschlossen ist.

Der speichernden Stelle war es nicht möglich, sich bis zum Ende ihrer Verantwortlichkeit, d. h. bis zum Abschluß der Vernichtung der Unterlagen, durch Kontrollen von der ordnungsgemäßen Durchführung zu überzeugen, weil grundsätzliche schriftliche Regelungen zwischen dem Auftragnehmer und dem Innenministerium fehlten. Wegen des Fehlens der o. g. Sicherheitsmaßnahmen hat das Innenministerium gegen Grundsätze der Auftragskontrolle, Transportkontrolle und Organisationskontrolle nach § 17 DSG MV verstoßen. Nach Auskunft der Staatsanwaltschaft Schwerin war der in den Medien geäußerte Verdacht auf eine strafbare Handlung auszuschließen. Aufgrund der gravierenden Mängel habe ich in diesem Fall eine förmliche Beanstandung ausgesprochen. Positiv zu vermerken ist, daß das Ministerium kurzfristig in allen Punkten den von mir gegebenen Empfehlungen zur Verbesserung des Datenschutzes gefolgt ist. Eine Nachkontrolle hat dies bestätigt. Ich habe den Vorfall zum Anlaß genommen, eine Organisationshilfe zur Vernichtung von Schriftgut zu erarbeiten, die ich allen obersten Landesbehörden mit der Bitte um Durchsetzung in ihrem Verantwortungsbereich zur Verfügung gestellt habe.

Aktenfund auf einem Friedhof

Ich wurde über einen Aktenfund in Rostock informiert und setzte mich umgehend mit dem Finder in Verbindung. Dieser schilderte, daß er die Akten bei einem Spaziergang auf einem stillgelegten Friedhof in Rostock-Dierkow gefunden hat. Seine Vermutung, daß es sich um Akten der Deutschen Vermögensberatungs-AG (DVAG) handelte, bestätigte sich. Unter den Schriftstücken waren Unterlagen von 26 Klienten, wie zum Beispiel Fragebögen und Computerausdrucke mit Angaben über Vermögensverhältnisse und Versicherungsverträge. Wie aber gelangten diese Akten auf den Friedhof?
Einem Mitarbeiter der o. g. Firma war das Auto gestohlen worden und offensichtlich hatten die Diebe für die im Auto liegenden Akten keine Verwendung und warfen sie einfach weg. Da die DVAG als nicht öffentliche Stelle jedoch nicht meiner Kontrolle unterliegt, habe ich die weitere Bearbeitung dem zuständigen Referat im Innenministerium übergeben.
Gleichwohl unterstreicht dieses Beispiel auch für den öffentlichen Bereich die Notwendigkeit einer ordnungsgemäßen Transportkontrolle, insbesondere das Beaufsichtigen der Akten beim Transport mit dem Kfz.

Sparkassenbelege auf dem Müll

"Machenschaften privater Müllentsorgungsfirmen - weiterer spektakulärer Aktenfund". Mit solchen Schlagzeilen geriet Ende Februar 1993 die Sparkasse Schwerin in die Presse und unter den Verdacht der illegalen Müllentsorgung sowie des nicht sorgsamen Umgangs mit den personenbezogenen Daten ihrer Kunden. Was war geschehen?
In einem vor der Deponie Stralendorf abgestellten Bauschuttcontainer wurden neben Büromüll auch Unterlagen und Belege der Sparkasse Schwerin gefunden. Darunter waren Empfangsbescheinigungen, Überweisungsanträge, Kontoauszüge, Kreditanträge, Kündigungs- und Mahnschreiben.

Ich habe daraufhin sofort bei der Sparkasse Schwerin eine Kontrolle durchgeführt. Die Finder hatten zwischenzeitlich die betreffenden Schriftstücke an die Sparkasse zurückgegeben. Im wesentlichen bestätigte der Vertreter der Sparkasse den Sachverhalt und erklärte, daß möglicherweise Reinigungskräfte und auch Mitarbeiter einen halbvollen Bauschuttcontainer zur bequemen Entsorgung nicht nur des Mülls, sondern auch der o. g. Unterlagen nutzten. Der genaue Hergang, wie diese Unterlagen in den Müll gelangen konnten, war nicht mehr zu rekonstruieren. Der Vertreter der Sparkasse erläuterte die übliche Verfahrensweise zur Entsorgung von Schriftgut und betonte, daß der unsachgemäße Umgang mit personenbezogenen Daten nur in diesem einen Fall durch die besonderen Umstände möglich gewesen sei. Normalerweise wird das zu vernichtende Schriftgut in einem verschließbaren Behälter gesammelt und von der Entsorgungsfirma vernichtet. Allerdings mußte ich feststellen, daß keine Dienstanweisung für die Beseitigung von Schriftgut vorhanden war. Ebenso fehlte ein schriftlicher Vertrag zur Vernichtung des Schriftgutes mit der Entsorgungsfirma. Eine Kontrolle der Vernichtung durch Mitarbeiter der Sparkasse erfolgte bisher ebenfalls nicht. Diese Mängel wurden von mir beanstandet, verbunden mit der Auflage, die vorgefundenen Mißstände schnellstmöglich zu beheben. Die Sparkasse reagierte sofort mit der Ausarbeitung eines Ablaufplanes zur Beseitigung von Schriftgut und dem Abschluß eines ordentlichen Vertrages mit einem spezialisierten Entsorgungsunternehmen.

2.18 Post- und Fernmeldewesen

2.18.1 Einsatz moderner Telekommunikationsanlagen - nur "Telefonieren mit Komfort"?

In den öffentlichen Stellen des Landes werden in zunehmendem Maße moderne Telekommunikationsanlagen eingesetzt. Diese Anlagen besitzen alle technische Voraussetzungen, die ein "Telefonieren mit Komfort" ermöglichen. Aus datenschutzrechtlicher Sicht erfordern die dafür vorhandenen Leistungsmerkmale jedoch eine kritische Betrachtung.
Es besteht z. B. die Möglichkeit, von jedem Gespräch die sogenannten Verbindungsdaten abzuspeichern. Mit diesen Daten ist nachvollziehbar, wer wann mit wem ein Telefongespräch geführt hat. Problematisch sind die Daten deshalb, weil mit ihnen Kommunikationsprofile erstellt werden können. Erhebungs-, Verarbeitungs- und Nutzungsregelungen sind zudem nur in der Telekom-Datenschutzverordnung (TDSV) vorhanden. Nach einer Entscheidung des Bundesverfassungsgerichtes entbehren diese Regelungen jedoch einer ausreichenden parlamentarischen Ermächtigung. Eine Überprüfung der Inhalte der TDSV und auch der für den privaten Bereich geltenden Teledienstunternehmen-Datenschutzverordnung (UDSV) scheint also dringend notwendig. Dabei sollte die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 8. März 1991 (s.a. Anlage 1) unbedingt berücksichtigt werden. Sie empfiehlt besonders folgende Maßnahmen:

- Verbindungsdaten müssen grundsätzlich nach Gesprächsende gelöscht werden,
- die Zielnummern müssen um die letzten vier Ziffern bei der Erstellung von Einzelentgeltnachweisen verkürzt werden,
- es darf nicht möglich sein, Kommunikationsprofile zu erstellen,
- die Anzeige der Rufnummer muß unterdrückbar sein.

Wo können nun beim Einsatz moderner Telekommunikationsanlagen in der Praxis Probleme auftreten?
Ein Schwachpunkt aus datenschutzrechtlicher Sicht entsteht durch den Anschluß von Personalcomputern an Telekommunikationsanlagen, um z. B. die Gebührenabrechnung durchführen zu können. In diesem Personalcomputer können die Verbindungsdaten aller Gespräche gespeichert werden. Diese Tatsache erfordert eine sehr restriktive Regelung der Zugangs-, Benutzer- und Organisationskontrolle.
Die o. g. Verkürzung der Zielnummern muß in jedem Falle realisiert sein. Die Programme zur Erfassung und Verarbeitung der Verbindungsdaten müssen ausreichend getestet und von der jeweils zuständigen Stelle freigegeben sein. In Organisationsregelungen ist eindeutig festzuhalten, wer zu welchen Daten Zugang haben darf.
Weiterhin sollten die Organisationsregelungen definieren, wer wem welche Nutzungsrechte für bestimmte Merkmale vergeben darf (z. B. Amtsberechtigung, Telefonpause) und wie die Vergabe der Rechte protokolliert wird. Ebenso sollte festgelegt werden, ob bestimmte Merkmale grundsätzlich nicht zugelassen werden sollen (z. B. Anklopfen, Aufschalten). Auch Möglichkeiten der Unterdrückung der Rufnummernanzeigesind zu nennen.

Selbstverständlich sollte sein, daß die Dienstvereinbarung zur Nutzung der Telekommunikationsanlage, in der alle notwendigen Hinweise jederzeit nachlesbar für die zukünftigen Nutzer enthalten sind, im Einvernehmen mit dem Personalrat und dem behördlichen Datenschutzbeauftragten abgeschlossen wird. Vor allem beim Einsatz von behördenübergreifenden Anlagen halte ich es für sinnvoll, den Landesdatenschutzbeauftragten in die Planungsarbeiten mit einzubeziehen. Nur auf diese Art und Weise lassen sich sinnvolle Empfehlungen rechtzeitig und mit minimalemKostenaufwand realisieren.
In § 27 DSG MV wird die Pflicht zur Unterstützung des Landesdatenschutzbeauftragten bei seiner Aufgabenerfüllung durch öffentliche Stellen angesprochen. Zu dieser Unterstützung zählt aus den o. g. Gründen auch die rechtzeitige und umfassende Information über die Planung und Entwicklung neuer technischer Verfahren, bei denen personenbezogene Daten automatisiert verarbeitet werden. Im § 29 Abs. 5 DSG MV wird darauf besonders hingewiesen. Diese Informationspflicht wird oft nicht hinreichend beachtet, in einem Fall auch von unserem Innenministerium nicht, unter dessen Federführung im Laufe des Jahres 1993 die Telekommunikationsanlageder Landesregierung in Betrieb genommen wurde.

2.18.2 Postleitzahlen in Adreßlisten - sensible personenbezogene Daten?

Seit dem 1. Juli 1993 gelten die neuen Postleitzahlen. In vielen öffentlichen Stellen war ein erheblicher Aufwand zur Umstellung der Adreßlisten auf die neuen Postleitzahlen notwendig. Daß dabei nicht immer so vorgegangen wurde, wie der Datenschutz es erfordert, zeigte eine Routinekontrolle in einem Amt zur Regelung offener Vermögensfragen.
Während der Kontrolle stand auf dem Arbeitstisch eines Mitarbeiters ein Personalcomputer, der im Geräteverzeichnis nicht aufgeführt war. Es stellte sich heraus, daß es sich um das Leihgerät einer Computerfirma handelte, auf dem die automatisierte Postleitzahlenumstellung in Adreßlisten der Beteiligten an Restitutionsverfahren durchgeführt wurde. Über die allgemeine Verschwiegenheitspflicht hinaus existierten keine schriftlichen Vereinbarungen mit dem Auftragnehmer, was mit den Daten auf dem firmeneigenen Personalcomputer nach Abschluß der Umstellung geschehen soll.

Aber gerade in diesem Fall sind die Adressen der Betroffenen besonders schützenswert. Denn allein schon die Kenntnis der Adresse eines Antragstellers in einem Restitutionsverfahren kann weitreichende Mißbrauchsmöglichkeiten eröffnen.

Mit diesem Beispiel möchte ich verdeutlichen, wie wichtig der Begriff der Angemessenheit im Zusammenhang mit technisch-organisatorischen Maßnahmen ist. In jedem Telefonbuch sind Adressen zu finden, die nicht besonders schützenswert sind. Hingegen ist die Sammlung der Adressen bestimmter Behörden durchaus in den Bereich der sehr sensiblen Daten einzuordnen und deshalb ein hohes Maß an technisch-organisatorischen Maßnahmen angemessen und erforderlich.

2.18.3 Telefax

Telefaxgeräte erfreuen sich einer immer größeren Beliebtheit. Auch in den öffentlichen Stellen meines Zuständigkeitsbereiches werden zunehmend Telefaxgeräte eingesetzt. Bei vielen meiner Kontroll- und Beratungsbesuche mußte ich jedoch feststellen, daß Fragen des Datenschutzes beim Einsatz von Telefaxgeräten noch zu wenig Aufmerksamkeit geschenkt wird. In einem Informationsblatt (s.a. Abschnitt 3.) habe ich bereits einige konkrete Hinweise zum Datenschutz beim Einsatz von Telefaxgeräten gegeben. Auf zwei der dort genannten Aspekte möchte ich besonders eingehen.

Was passiert, wenn der Besitzer eines Telefaxgerätes umzieht und eine neue Telefaxnummer bekommt? Er teilt möglicherweise allen Personen, die seine alte Telefaxnummer kennen, rechtzeitig vor dem Umzug die neue Nummer mit. Aber weiß er wirklich, welcher Personenkreis seine alte Nummer kennt? Sicher nicht! Die alte Nummer wird einem neuen Nutzer zugeteilt, da die Telekom einmal vergebene Telefonnummern nicht für eine Neuvergabe sperrt. Zufällig schließt der neue Nutzer auch wieder ein Telefaxgerät dort an. Nach dem Umzug schickt nun doch jemand ein Fax an die alte Nummer und merkt nicht, daß der Empfänger nicht derjenige ist, für den er ihn hält. Auf diese Art und Weise können personenbezogene Daten sehr schnell in falsche Hände kommen.

Auch der Aufstellungsort des Telefaxgerätes spielt aus datenschutzrechtlicher Sicht eine wichtige Rolle. In öffentlichen Stellen haben größere Organisationseinheiten oft nur ein gemeinsames Telefaxgerät. Um die Benutzung für alle Mitarbeiter zu ermöglichen, steht das Gerät z. B. auf dem Flur. Es ist also kaum kontrollierbar, wer die empfangenen Telefaxtexte liest, bevor der Empfänger die für ihn bestimmte Mitteilung aus dem Gerät nimmt.

Jeder, der ein Telefaxgerät benutzt, muß wissen, daß das Versenden eines Schreibens per Telefax ohne die Nutzung von Sicherungsverfahren dem Schreiben einer Postkarte gleicht. Sensible personenbezogene Daten sollten deshalb nur in Ausnahmefällen per Fax gesendet werden. Auf jeden Fall sollten dann zusätzliche Sicherungsmerkmale benutzt werden, die viele Telefaxgeräte besitzen. Genannt seien hier z. B. Abrufverfahren und die Nutzung von Paßwortmechanismen. Auch die vorherige telefonische Ankündigung einer Telefaxsendung kann verhindern, daß Unbefugte Kenntnis von den so übertragenen Daten erlangen können.

2.19 Baulicher Datenschutz

2.19.1 Schallschutz, Zutrittskontrolle, Datenträgerkontrolle

Daß auch bautechnische Probleme für datenschutzrechtliche Fragen von Bedeutung sind, zeigte eine Petition, in der mangelnder Schallschutz im Gebäude eines Landratsamtes beklagt wurde. Mir wurde mitgeteilt, daß vertrauliche Gespräche, die in einem in zentraler Lage liegenden Besprechungsraum geführt werden, auf dem Flur mitgehört werden können.
Daraufhin habe ich eine Kontrolle in dem besagten Landratsamt durchgeführt und stellte fest, daß dem baulichen Datenschutz in diesem Fall jedoch ausreichend Aufmerksamkeit geschenkt worden war. Sowohl die Türen als auch die neu eingezogenen Wände gewährleisteten einen ausreichenden Schallschutz.

Das Beispiel soll verdeutlichen, daß der Datenschutz schon bei der Planung von Baumaßnahmen berücksichtigt werden muß. Von besonderer Bedeutung ist das in meinem Zuständigkeitsbereich deshalb, weil zur Zeit umfangreiche Renovierungs- und Rekonstruktionsmaßnahmen in Gebäuden öffentlicher Stellen durchgeführt werden, bei denen auch Maßnahmen in Bezug auf den Datenschutz besonders kostengünstig realisiert werden können. Als bautechnische Maßnahmen zur Gewährleistung der Zugangskontrolle sollen hier einbruchhemmende Türen, vergitterte Fenster und Bewegungsmelder erwähnt werden. Ein bautechnisches Mittel zur Gewährleistung der Datenträgerkontrolle ist die Installation von Brandwarnanlagen.

2.19.2 Verkabelung - Datenstraßen der Rechnernetze

Welche Unsicherheiten auf datenschutzrechtlichem Gebiet hinsichtlich der Verkabelung bestehen, wenn Rechnernetze installiert werden, zeigte sich durch die vielen Fragen, die ich zu diesem Thema zu beantworten hatte.
Nur ein Beispiel: Ein Mitarbeiter der Bauabteilung des Finanzministeriums fragte bei mir an, ob es denn wirklich nötig sei, Verteilerschränke von Rechnernetzen abzuschließen oder in einem verschlossenen Raum aufzustellen.
Ich möchte hier nur einige grundsätzliche Hinweise geben, die bei der Realisierung von Netzen zu beachten sind. Bei jeder Netzinstallation sind immer auch die jeweiligen gebäude- und behördenspezifischen Besonderheiten zu berücksichtigen. Allgemeine Hinweise ersetzen nie das Datenschutz- und Datensicherheitskonzept, das vor der Realisierung jedes Netzes vorliegen sollte. Netze müssen entsprechend der Struktur der Behörde dadurch gegliedert sein, daß funktionale Subnetze gebildet werden, die den Aufgaben einzelner Verwaltungseinheiten entsprechen. Jedes einzelne Subnetz sollte sternförmig aufgebaut werden, wobei ich den Einsatz filternder aktiver Komponenten empfehle. Diese Komponenten gewährleisten, daß Daten nur an das Endgerät gelangen, für das sie tatsächlich bestimmt sind.

In letzter Zeit werden zunehmend Verfahren auf dem Markt angeboten, die eine behördeninterne drahtlose Datenübermittlung ermöglichen. Um das Risiko des unberechtigten Abhörens so gering wie möglich zu halten, empfehle ich, auf die Nutzung dieser Verfahren zur Übertragung personenbezogener Daten zu verzichten. Vielmehr sollten für den Primärbereich (zwischen Gebäuden) und den Sekundärbereich (zwischen Etagen) LWL-Kabel, für die Verkabelung im Tertiärbereich (innerhalb der Etagen) UTP- oder STP-Kabel nach 10BaseT-Standard verwendet werden. Verteiler in allen Ebenen sind so anzuordnen, daß ein unberechtigter Zugriff ausgeschlossen werden kann (verschließbar, nicht allgemeinzugänglicher Aufstellort).
Im IT-Strukturrahmen für die Landesverwaltung Mecklenburg-Vorpommern werden im Abschnitt "Interne Vernetzung" Verkabelungssysteme beschrieben. Die Einhaltung aller Forderungen, die dort hinsichtlich strukturierter Universalverkabelung erhoben werden, ist Voraussetzung für die datenschutzgerechte Realisierung einer inhouse-Vemetzung.

2.20 Registerführung

2.20.1 Dateibeschreibung und Geräteverzeichnis

§ 16 DSG MV schreibt vor, daß jede speichernde Stelle verpflichtet ist, in einer Beschreibung jeder automatisierten Datei folgendes festzulegen:

- die Bezeichnung der Datei,
- die Art der gespeicherten Daten,
- die Art und den Umfang der Nutzung der Daten,
- den Kreis der Betroffenen,
- die Art der regelmäßig übermittelten Daten und deren Empfänger,
- die Art der regelmäßig empfangenen Daten und deren Herkunft,
- die bestehenden Fristen für die Sperrung oder Löschung der Daten,
- die technisch-organisatorischen Maßnahmen nach § 17 DSG MV,
- bei automatisierten Verfahren die Betriebsart des Verfahrens, die Art der Geräte sowie das Verfahren zur Übermittlung, Sperrung, Löschung und Auskunftserteilung.

Ebenso ist die speichernde Stelle verpflichtet, in einem Verzeichnis der Geräte, mit denen personenbezogene Daten automatisiert verarbeitet werden, neben der o. g. Dateibeschreibung festzulegen:

- den Standort, den Typ und die Art der Geräte,
- den Hersteller,
- das verwendete Betriebssystem,
- die verwendeten Programme.

Um die Führung dieser Verzeichnisse so weit wie möglich zu vereinfachen und zu vereinheitlichen, habe ich im Amtsblatt Mecklenburg-Vorpommern Nr. 21 vom 24.05.1993 Musterformulare und ausführliche Hinweise zur Führung von Dateibeschreibung und Geräteverzeichnis veröffentlicht. Ich empfehle, diese Vorlagen zur Erstellung der eigenen Unterlagen zu nutzen. Dadurch wird gewährleistet, daß die vom Gesetz verlangten Angaben vorhanden sind. Darüber hinaus wird mir eine effektive Vorbereitung hinsichtlich meiner Beratungs- und Kontrolltätigkeit ermöglicht, weil ich vor jedem Besuch einer öffentlichen Stelle Angaben über automatisiert geführte Dateien mit personenbezogenen Daten in eben dieser Form anfordere.
Ich mußte jedoch häufig feststellen, daß vor allem Dateibeschreibungen nicht entsprechend den Forderungen des § 16 DSG MV geführt wurden. In einigen Fällen gab es bei den speichernden Stellen geringe Kenntnisse über Inhalt und Struktur der bei ihnen geführten Dateien, daß nur die Firma, die für die Programmierung und Pflege der Software verantwortlich war, zum Anfertigen der Dateibeschreibung in der Lage war.

Die Angabe der Rechtsgrundlage zur Verarbeitung der personenbezogenen Daten wird für die Dateibeschreibung im Gesetz zwar nicht ausdrücklich verlangt, ich habe jedoch empfohlen, die Rechtsgrundlage in die Dateibeschreibung mit aufzunehmen. Ebenfalls viel zu selten wurden ausreichende Angaben zu den bestehenden Fristen für die Sperrung oder Löschung von Daten gemacht. Um Unzulänglichkeiten dieser Art abbauen zu können, werde ich in meiner künftigen Beratungs- und Kontrolltätigkeit verstärkt auf die Führung von Dateibeschreibung und Geräteverzeichnis eingehen.

2.20.2 Vereinheitlichung (Koordinierung mit anderen Verzeichnissen)

Mehrfach wurde Kritik hinsichtlich der Praktikabilität der von mir empfohlenen Form von Dateibeschreibung und Geräteverzeichnis geübt. Diese Kritik ist insofern berechtigt, als daß jede speichernde Stelle Verzeichnisse ähnlichen Inhalts (z.B. Geräteverzeichnis) in mehreren verschiedenen Formen führen muß. Es sei hier nur an die Forderungen der Landeshaushaltsordnung und der IT-Ressortplanung erinnert. Um den verwaltungstechnischen Aufwand auf das notwendige Minimum zu reduzieren habe ich im IMA-IT (Interministerieller Ausschuß für Informations- und Telekommunikationstechnik - s.a. Abschnitt 2.22.) den Vorschlag gemacht, die zur Zeit unterschiedlichen Formen zu vereinheitlichen, so daß die speichernde Stelle nur noch jeweils ein Verzeichnis führen muß, das für alle in Frage kommenden Adressaten die geforderten Angaben enthält. In diesem Zusammenhang wäre es meiner Meinung nach sehr sinnvoll, rechentechnische Unterstützungsmöglichkeiten zu nutzen. Ich könnte mir eine Lösung bezüglich der Geräteverzeichnisse dergestalt vorstellen, daß in einer Datenbankanwendung (Paradox als Landesstandard wäre dafür sehr geeignet) alle notwendigen Angaben erfaßt werden und durch Nutzung von vorhandenen Reportfunktionen Ausdrucke mit den Angaben erfolgen, die von der jeweiligen kontrollierenden Stelle verlangt werden. Dadurch könnte der Erfassungsaufwand minimiert und die im Gesetz geforderte Aktualität sichergestellt werden.
Ich empfehle dem IMA-IT als zuständigem Koordinierungsgremium, nach Lösungsmöglichkeiten zu suchen und habe hierfür meine Unterstützung zugesagt.

2.21 AK Technik

2.21.1 Zur Rolle des LfD MV im AK Technik

Auf der 45. Sitzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Februar 1993 wurde beschlossen, mir den Vorsitz des Arbeitskreises "Technische und organisatorische Datenschutzfragen" (AK Technik) zu übertragen. Die Übernahme des Vorsitzes dieses Arbeitskreises wurde damit begründet, daß auf diese Art und Weise eine sinnvolle Einbeziehung der neuen Bundesländer in die gemeinsame Arbeit der Datenschutzbeauftragten des Bundes und der Länder gefördert wird. Ausdrücklich wurde durch die Konferenz betont, daß der Arbeitskreis durch den bisherigen Vorsitzenden, den Bayrischen Landesdatenschutzbeauftragten, sowohl fachlichals auch organisatorisch sehr gut geleitet wurde.
Im Berichtszeitraum habe ich zwei Sitzungen des Arbeitskreises vorbereitet und in Schwerin durchgeführt. Neben den fachlichen Zuarbeiten meiner Dienststelle war die Koordination der Aktivitäten der Kollegen aus dem technischen Bereich eine wichtige Aufgabe. Im folgenden stelle ich einige Themen aus der Arbeit des Arbeitskreises näher dar, die auch für Mecklenburg-Vorpommern von besonderer Bedeutung sind oder in absehbarer Zeit von Bedeutung sein werden.

2.21.2 Die Chipkarte

Die ständig fortschreitende Miniaturisierung in der Elektronik ermöglichte die stetige Weiterentwicklung der Chipkarte. Dadurch kann sie immer universeller in den verschiedensten Bereichen eingesetzt werden. Besondere Bedeutung bekommt sie für den Bürger dadurch, daß ihr Einsatz, z. B. als Krankenversichertenkarte (s.a. Punkt 2.11.6.), schon jetzt feststeht und in einigen Bundesländern bereits getestet wird. Aber auch die Verwendung der Chipkarte als mögliches Zahlungsmittelim öffentlichenNahverkehr verdient eine nähere Betrachtung.

Der Arbeitskreis konnte sich auf umfangreiche Vorarbeiten und Recherchen des Hamburgischen Datenschutzbeauftragten und des Bundesbeauftragten für den Datenschutz stützen. Ein datenschutzrechtlich grundsätzliches Problem bei der Verwendung der Chipkarte resultiert daraus, daß nur ein Bruchteil ihrer Leistungsfähigkeit für die geplanten Anwendungen benötigt wird. Man muß sich nur einmal klarmachen, daß die Chipkarte, die die Größe einer Telefonkarte hat, ein kompletter kleiner Computer ist. Nur zu verständlich ist daher das Bedürfnis der Anwender, auch einen Großteil der Leistungsfähigkeit zu nutzen und möglichst viele Informationen auf ihr zu speichern. Aus der Sicht des Datenschutzes ergeben sich dadurch unabsehbare Risiken. Deshalb wurde z.B. bei der Anwendung der Chipkarte als Krankenversichertenkarte festgelegt, daß nur 256 Bytes zur Speicherung von Informationen gemäß § 291 Abs. 2 SGB V verwendet werden dürfen. Selbst bei Chipkarten mit höherer Kapazität dürfen nur diese 256 Byte freigegeben und mit genau definierten Informationen in einem unveränderlichen Format belegt werden. Doch schon hier gibt es Abweichungen zu den getroffenen Festlegungen dahingehend, daß zur Zeit zwei Byte freigelassen werden, deren Verwendungsmöglichkeit nicht definiert ist. Alle Teilnehmer der Sitzung des Arbeitskreises waren sich darin einig, daß so eine Mißbrauchsmöglichkeitgeschaffen wird, die nicht toleriert werden kann.

Um einen ausreichenden technischen Sicherheitsstandard zu gewährleisten, wurde vom Bundesbeauftragten für den Datenschutz empfohlen, die kryptografische Versiegelung anzuwenden. Dieser Empfehlung folgten Krankenkassen und Kassenärztliche Bundesvereinigungen jedoch aus Kostengründen nicht. Um dennoch ein Minimum an Sicherheit zu gewährleisten wurde unter anderem festgelegt, daß nur zertifizierte Hard- und Software eingesetzt werden darf, daß jeder Versicherte den Inhalt seiner Karte lesen können muß und daß der nicht benutzte Speicherplatz mit definierten Zeichen zu belegen ist.

Die Verwendung von Chipkarten als Zahlungsmittel im öffentlichen Nahverkehr wird in anderen Bundesländern bereits getestet. Es ist schon jetzt absehbar, daß ein solches Zahlungssystem nur durch Speicherung umfangreicher personenbezogener Daten funktioniert, denn es muß genau festgehalten werden, wer wann mit welchem Verkehrsmittel welche Strecke gefahren ist, damit eine ordnungsgemäße und revisionssichere Abbuchung vom Konto des Karteninhabers erfolgen kann. Es liegen also genug Informationen vor, um detaillierte Bewegungsprofile einzelner Bürger erstellen zu können. Noch kritischer wird das Ganze, wenn Chipkarten (möglicherweise auch EC- und Kreditkarten) als Universalzahlungsmittel eingesetzt werden. Dann läßt sich möglicherweise ein ganzer Tagesablauf wie folgt rekonstruieren: um 8.35 Uhr im Supermarkt eingekauft, 47,40 DM bezahlt; dann mit der Straßenbahn von A nach B gefahren, 2,80 DM bezahlt; um 9.15 angekommen; im Cafe für einen Kaffee um 9.45 Uhr 3,50 DM bezahlt usw. Ein sicherer Schritt zum "gläsernen Menschen"!
Um vor diesen Gefahren zu warnen, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf ihrer 46. Sitzung im Oktober 1993 in Berlin eine entsprechende Entschließung verabschiedet (siehe Anlage 10).

2.21.3 Mobilfunk

Die weitere Verbreitung mobiler Sprach- und Datenübertragungsdienste im privaten - und Behördenbereich macht es notwendig, auf die damit verbundenen datenschutzrechtlichen Risiken deutlich hinzuweisen. Einerseits ist die Vertraulichkeit von Gesprächsinhalten nicht in allen Fällen sichergestellt, andererseits entsteht durch die Speicherung von zusätzlichen Verbindungsdaten, wie z. B. dem Aufenthaltsort des Teilnehmers, die Möglichkeit, Bewegungsprofile zu erstellen.
Der Arbeitskreis Technik hat besonders die datenschutzrechtlichen Fragen des BOS-Funks (Behörden und Organisationen mit Sicherheitsaufgaben) untersucht. Um die Aktualität des Themas zu verdeutlichen und die Notwendigkeit klarzumachen, daß sich der Arbeitskreis intensiv mit Sicherheitsrisiken des Mobilfunks befaßt, möchte ich einen Fall aus meiner Kontrolltätigkeit darstellen.

Bei der Kontrolle einer Polizeidirektion, die eigentlich der Überprüfung der Zugriffsmöglichkeiten auf INPOL-Datenbestände diente, erfuhr ich, daß Abfragen von Beamten im Außendienst auch mit Hilfe von BOS-Funkgeräten durchgeführt werden.
Der Beamte beauftragt über Funk die Leitstelle, eine INPOL-Abfrage per Computer zu starten. Das Ergebnis dieser Anfrage, z. B. Daten eines Kfz-Halters aus dem ZEVIS-Datenbestand, wird dem Anfragenden über Funk mitgeteilt.
Bei diesem Vorgang wurden gleich mehrere datenschutzrechtliche Grundprinzipien verletzt. Die Identifikation des Anfragenden erfolgte nur anhand der Stimme. Die Abfrage selbst wurde nicht protokolliert. Der Austausch von Informationen mit Hilfe der Funkgeräte erfolgte völlig

ungeschützt, so daß mit handelsüblichen Empfängern der gesamte Funkverkehr durch Unbefugte abgehört werden konnte.

Ein Fall von vielen anderen, aber er macht deutlich, wie wichtig es ist, schnellstmöglich Schritte zu unternehmen, den BOS-Funk sicher zu machen. Das setzt natürlich voraus, daß der Polizei die dafür erforderlichen Mittel zur Verfügung gestellt werden.

Der Arbeitskreis hat technische Möglichkeiten des Mobilfunks untersucht, um Empfehlungen geben zu können, wie gerade im Bereich des BOS-Funks, wo sehr sensible personenbezogene Daten übermittelt werden, datenschutzrechtlich unbedenklichere Lösungen eingesetzt werden können. Dabei wurde deutlich, daß alle bisher verwendeten Techniken, die das Abhören verhindern sollen, im Grunde genommen untauglich sind. Nur ein Beispiel: Es sind Geräte legal zu erwerben, die es ermöglichen, mit Hilfe von Invertern verschleierte Gespräche wieder verständlich zu machen (Invertierdecoder). Als Empfehlung kann deshalb nur gelten, auch im BOS-Bereich digitale Mobilfunktechnik einzusetzen, da nur auf dieser Basis eine wirkungsvolle Verschlüsselung der Gesprächsinhalte möglich ist. Diese Empfehlung kommt in einer Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Ausdruck, die auf der 46. Sitzung im Oktober 1993 in Berlin verabschiedet wurde (siehe Anlage 7).

2.21.4 Wartung und Fernwartung

Die ständig zunehmende Komplexität von EDV-Anlagen zur Verarbeitung personenbezogener Daten in Behörden erfordert eine immer umfassendere Wartung dieser Systeme sowohl hard- als auch softwareseitig. Die dafür notwendigen, sehr umfangreichen Kenntnisse sind bei Mitarbeitern dieser Behörden oft nicht vorhanden, so daß Wartungsaufgaben durch externe Dienstleister wahrgenommen werden. Da nicht immer vermieden werden kann, daß diese Dienstleister Kenntnis über personenbezogene Daten erhalten, was im Bereich der Softwarewartung manchmal geradezu notwendig ist, stellt sich die Frage nach der Zulässigkeit der Übertragung von Wartungsaufgaben an externe Dienstleister. Besonders kritisch ist die Situation z. B. im medizinischen Sektor, wo zunehmend sehr komplexe Klinikinformationssysteme in Betrieb genommen werden, die kaum noch von klinikeigenen Technikern gewartet werden können. Wartung in diesem Bereich kann durchaus der Offenbarung von Sozialdaten gleichkommen. Dazu gibt es jedoch in §§ 67 ff SGB X abschließende Regelungen, die Wartung unter diesen Umständen durch externe Dienstleister ausschließen.

Seit einigen Jahren befaßt sich der Arbeitskreis mit diesem Thema. Um die Zulässigkeit von Wartung und Fernwartung beurteilen zu können, ist es notwendig, beide Begriffe rechtlich widerspruchsfrei in das Begriffssystem der Datenschutzgesetze einzuordnen. Dazu wurden durch die Datenschutzbeauftragten im wesentlichen zwei Standpunkte vertreten:

- Die mögliche Kenntnisnahme von personenbezogenen Daten ist eine Datenübermittlung.
- Wartung und Fernwartung fallen unter die Auftragsdatenverarbeitung (oder -nutzung).

Für beide Standpunkte lassen sich in den Datenschutzgesetzen Argumente finden, die kaum zu widerlegen sind. Das hängt damit zusammen, daß die Begriffe Datennutzung, Datenverwendung, Datenübermittlung und Auftragsdatenverarbeitung in den verschiedenen Datenschutzgesetzen unterschiedlich definiert sind. Darüber hinaus ist eine unterschiedliche Auslegung der vorhandenen Gesetze offensichtlich möglich.
Angesichts dieser Situation wurde zunächst unter Federführung des Bayrischen LfD eine Orientierungshilfe verabschiedet, in der ein Minimum an notwendigen Sicherheitsmaßnahmen bei der Durchführung von Wartungsaufgaben aus technischer Sicht definiert wurden. Weil damit aber noch immer keine befriedigende Lösung des Problems erreicht worden ist, haben sich die Mitglieder des Arbeitskreises darüber geeinigt, die Konferenz der Datenschutzbeauftragten des Bundes und der Länder darauf aufmerksam zu machen, daß hier Handlungsbedarf außerhalb des AK-Technik besteht. Der Arbeitskreis hat den erarbeiteten Sachstandsbericht gebilligt und der Konferenz als Arbeitsgrundlage zur Verfügung gestellt.
Auf der 46. Sitzung im Oktober 1993 in Berlin hat sich die Konferenz mit dem Thema befaßt und mit der weiteren Bearbeitung den LfD Nordrhein-Westfalen beauftragt.

2.21.5 Lauschangriff - technisch gesehen

Ergänzend zu Punkt 2.4.1. soll an dieser Stelle zum Lauschangriff noch einiges aus technischer Sicht gesagt werden. Eine Beurteilung hinsichtlich der Wirksamkeit des Lauschangriffs ist nur sinnvoll, wenn die technischen Möglichkeiten seiner Realisierung und die entsprechenden Gegenmaßnahmen zur Abwehr bekannt sind.

Es ist erstaunlich, welche Möglichkeiten heute bereits der interessierte Laie hat, ganz legal Technik zu erwerben, die durchaus geeignet ist, die Wirksamkeit technischer Mittel zur Ausforschung von Räumen in Frage zu stellen. So sind z. B. Funkscanner, die zum Aufspüren von Wanzen verwendet werden können, mit den verschiedensten Leistungsmerkmalen in allen Preisklassen leicht über Elektronikversandhäuser zu beschaffen. Welche Möglichkeiten im Rahmen der organisierten Kriminalität diesbezüglich bestehen, wo scheinbar unbegrenzte finanzielle Mittel zur Verfügung stehen und bestens ausgebildete Fachleute vorhanden sind, läßt sich nur erahnen. Allein aus öffentlich zugänglicher Literatur und durch Befragung von Anwendern und Vertreibern von Funktechnik konnte ich mir in kürzester Zeit einen Überblick über die technischen Möglichkeiten des Lauschangriffs und der Lauschabwehr verschaffen. Das Ergebnis der Untersuchung wurde von einem Spezialisten auf dem Gebiet der Lauschabwehr bestätigt. Ich hatte diesen Spezialisten gebeten, im Rahmen einer Sitzung des Arbeitskreises Technik über die technischen Möglichkeiten beider Seiten zu referieren. Aufgrund seiner Erfahrungen schätzte er die technischen Möglichkeiten zur Durchführung eines effektiven Lauschangriffes besser ein als die technischen Möglichkeiten zur Abwehr. Er räumte jedoch auch ein, daß sowohl der Zeitfaktor als auch die zur Verfügung stehenden finanziellen Mittel eine maßgebliche Rolle spielen, wenn der Lauschangriff einigermaßen erfolgreich sein soll, und daß letzten Endes bei jedem Lauschangriff auf Ahnungslosigkeit der Belauschten gebaut werden muß.

2.21.6 Datenschutz und Personalcomputer

Der zunehmende Einsatz von Personalcomputern in allen Bereichen der öffentlichen Verwaltung macht die Frage der Realisierung des Datenschutzes an PC sowohl für den Arbeitskreis als auch für meine Kontroll- und Beratungstätigkeit zu einem Dauerthema. Nicht nur bei Kontrollen in meinem Zuständigkeitsbereich muß ich immer wieder feststellen, daß viel zu wenig Möglichkeiten genutzt werden, um auch mit dem PC ordnungsgemäß personenbezogene Daten zu verarbeiten (s.a. Abschnitt 2.16.). Auch im Rahmen des Arbeitskreises wurde von bei Kontrollen festgestellten Mängeln berichtet.

Um kompetent beraten und Lösungen empfehlen zu können, die auf einem zufriedenstellenden datenschutzrechtlichen Niveau stehen, informieren sich die Datenschutzbeauftragten ständig über die Angebotssituation auf dem Markt. Dazu besuchen wir nicht nur Fachmessen und Weiterbildungsveranstaltungen, sondern laden auch kompetente Fachleute aus Forschung und Industrie ein, die über ihre Erfahrungen berichten. Für die 21. Sitzung des Arbeitskreises konnte ich für einen Fachvortrag den Geschäftsführer einer Firma als Gast gewinnen, die PC-Sicherheitsprodukte speziell für den Behördenbereich im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entwickelt, produziert und vertreibt. Auf diese Art und Weise ist es auch möglich, Herstellern klarzumachen, welche Forderungen die Datenschutzbeauftragten an bestimmte Produkte, z. B. aus dem Bereich der PC-Sicherheit, stellen. Während des Meinungsaustausches wurde deutlich, daß die Frage der Schutzmöglichkeit von Protokolldateien dem Systemadministrator gegenüber nach wie vor nicht zufriedenstellend gelöst ist.
Einigkeit bestand dahingehend, daß ein ausreichender Schutz nur dann gewährleistet werden kann, wenn Personalcomputer mit einer entsprechenden Kombination von Hard- und Softwarekomponenten ausgerüstet werden. Die zunehmende Bedeutung des PC auch im Rahmen von Client-Server-Konfigurationen erfordert es, daß sich die Datenschutzbeauftragten weiterhin intensiv mit der Sicherheit der Verarbeitung personenbezogener Daten mit Hilfe von PC befassen.

2.22 IMA-IT

Der Interministerielle Ausschuß für Informations- und Telekommunikationstechnik, ist für die Koordinierung des Einsatzes von Hard- und Software in den Behörden des Landes verantwortlich. Alle Ressorts entsenden ihre IT-Referenten als ständige und stimmberechtigte Mitglieder in diesen Ausschuß. Das Innenministerium wurde mit der Federführung beauftragt. Daneben werden bei Bedarf IMA-IT-Mitglieder mit beratender Stimme zu Sitzungen hinzugezogen.

Im September 1992 wurde ich darum gebeten, als Mitglied mit beratender Stimme an den Sitzungen des IMA-IT teilzunehmen. So werde ich sehr frühzeitig in die Planungs- und Einführungsphase von IT-Lösungen, die landeseinheitlich eingesetzt werden sollen, einbezogen, um meine datenschutzrechtlichen Empfehlungen einfließen zu lassen. Nachfolgend stelle ich einige wichtige Aspekte aus meiner Beratungstätigkeit im IMA-IT dar.

2.22.1 IT-Strukturrahmen

Zunächst wichtigste Aufgabe des IMA-IT war es, einen Landesstandard, den IT-Strukturrahmen (ITSR), zu erarbeiten, der für alle Landesbehörden sowohl verbindliche Festlegungen als auch Empfehlungen und Hinweise für die Planung, Beschaffung und den Betrieb informationstechnischer Systeme und Verfahren enthält. Die Festlegungen bezüglich der Systemarchitektur, fachneutraler IT-Verfahren sowie interner und externer Vernetzung bekamen verbindlichen Charakter, während alle organisatorischen Regelungen, zu denen auch der Abschnitt Datenschutz und Datensicherheit gehört, als Empfehlungen zu werten sind.
Der Abschnitt Datenschutz und Datensicherheit wurde zunächst durch die fachlich und organisatorisch begleitende Beratungsfirma erarbeitet und mir dann mit der Bitte um Stellungnahme vorgelegt. Einem Teil meiner daraufhin ausgesprochenen Empfehlungen konnte in der endgültigen Fassung des ITSR gefolgt werden. So wurden Hinweise zu Aufgaben und Befugnissen des behördlichen Datenschutzbeauftragten und zur Führung von Dateibeschreibung und Geräteverzeichnis aufgenommen. Auch die besondere Sensibilität, die bei der automatisierten Verarbeitung personenbezogener Daten notwendig ist, wurde verdeutlicht.
Nicht gefolgt wurde meinen Empfehlungen, den Abschnitt Datenschutz und Datensicherheit als verbindlichen Bestandteil des ITSR zu erklären. Ebenso wurde es durch die stimmberechtigten Mitglieder des IMA-IT abgelehnt, bei der Einführung von IT-Verfahren zur Verarbeitung personenbezogener Daten die Erstellung eines Datenschutzkonzeptes als verbindlich zu erklären. Auch deshalb werde ich in diesem Rahmen weiterhin die Einführung von landeseinheitlichen IT-Verfahren mit besonderer Aufmerksamkeit beratend begleiten, wie ich es in den nachfolgend geschilderten Fällen schon mit gutem Erfolg getan habe.

2.22.2 Personalinformationssystem

Anfang 1993 beschloß der IMA-IT auf Anforderung der Personalreferenten der Ressorts zu prüfen, welche Möglichkeiten für die Einführung eines landeseinheitlichen Personal- und Stellenbewirtschaftungssystems bestehen würden. Es wurde ein Arbeitskreis gegründet, an dessen Sitzungen ich teilnehme. Nach einer genauen Definition der Anforderungen und entsprechenden Marktrecherchen wurde deutlich, daß eine landeseinheitliche Lösung realisierbar ist. Schon bei der Definition der Datenfelder des geplanten Systems wurde meine Empfehlung berücksichtigt, keine Felder zuzulassen, aus denen erkennbar ist, ob der Betreffende ein Bürger aus den alten oder den neuen Bundesländern ist. Auch hinsichtlich der Abfrage- und Recherchemöglichkeiten wurde meinen Hinweisen, nur sehr stark eingeschränkt freie Abfragesprachen zuzulassen, in der Planung gefolgt. Die strenge Trennung von Leistungsmerkmalen Beschäftigter und Personaldaten wurde akzeptiert. Leistungsmerkmale dürfen nicht mit diesem System erfaßt werden.
Bezüglich der Form der Datenhaltung konnte ich die Forderung der Personalreferenten unterstützen, Personaldaten dezentral in jedem einzelnen Ressort zu halten.
Von besonderer Bedeutung war die Frage der Zugriffsrechte. Die von mir formulierten Forderungen, Zugriffsrechte sehr differenziert entsprechend der zu bearbeitenden Aufgabe zu vergeben, sollen berücksichtigt werden. Zur Zeit erfolgt die von mir geforderte Erstellung des Datenschutz- und Datensicherheitskonzeptes, in dem sich meine Forderungen und Empfehlungen widerspiegeln sollen.

2.22.3 Landeseinheitliches Schriftgutverwaltungssystem

Schon während der Erarbeitung des ITSR wurde der Wunsch der Organisationsreferenten der Ressorts deutlich, Möglichkeiten der IT-gestützten Schriftgutverwaltung zu untersuchen. Der IMA-IT rief den Arbeitskreis Registratur ins Leben. Ich wurde darum gebeten, an den Sitzungen dieses Arbeitskreises ebenfalls beratend teilzunehmen.

Zunächst wurden von mir Empfehlungen für die zur Zeit gültige "Vorläufige Registraturanordnung" des Innenministeriums ausgesprochen, die als Basis für die Formulierung der Anforderungen an das Schriftgutverwaltungssystem dienen soll. Dort fehlten z. B. Hinweise auf die Einhaltung des Landesdatenschutzgesetzes völlig. Auch bezüglich der Aussonderung und Vernichtung von Schriftgut habe ich Empfehlungen entsprechend der "Orientierungshilfe Schriftgutvernichtung" gegeben (siehe Anlage 12). Noch nicht eindeutig geklärt werden konnte, wie die Abgabe von Schriftgut an das Landeshauptarchiv Mecklenburg-Vorpommern erfolgen soll, da noch immer kein Landesarchivgesetz existiert, das hierzu verbindliche Regelungen enthalten wird. Aus gleichem Grund problematisch war die Definition von Aufbewahrungsfristen, da ohne eine gesetzliche Regelung lediglich Fristen entsprechend der sogenannten verwaltungspraktischen Bedeutung durch die Leiter der jeweiligen Organisationseinheiten festgesetzt werden. Eindeutig wurde von mir für die Realisierung des Schriftgutverwaltungssystems gefordert, daß die Personalregistratur vollkommen getrennt geführt werden muß. Da die Planungs- und Projektierungsphase noch nicht abgeschlossen ist, werde ich hier weiterhin beratend tätig sein, damit sichergestellt ist, daß ein zukünftiges landeseinheitliches Schriftgutverwaltungssystem nur unter ausreichender Berücksichtigung datenschutzrechtlicher Aspekte in Betrieb genommen wird.

3. Öffentlichkeitsarbeit und Beratungstätigkeit

3.1 Beratungs- und Kontrollbesuche

Bei meinen Besuchen mußte ich häufig feststellen, daß von Behördenmitarbeitern nicht erkannt wird, daß bei vielen Fragestellungen, beispielsweise aus dem Bereich Melderecht oder Personalaktenrecht, auch datenschutzrechtliche Aspekte zu berücksichtigen sind. Um dieses Defizit auszugleichen, lag der Schwerpunkt meiner Beratungstätigkeit in den Behörden in diesem ersten Jahr mehr auf der Informationsvermittlungund Beratung als auf der Kontrolle.

3.2 Vorträge

Trotz der recht dünnen Personaldecke meiner Behörde bin ich dem Wunsch nach Vorträgen zum Thema Datenschutz nachgekommen. Im Rahmen einer in der Hansestadt Rostock laufenden Vortragsreihe: "Der Präsident der Bürgerschaft lädt ein" referierte ich u. a. über "Aktuelle Themen des Datenschutzes in MV". Auf Einladung des Fachbereiches Informatik der Universität Rostock haben zwei Mitarbeiter meiner Behörde Vorträge zu allgemeinen Fragen des Datenschutzes und zu technisch-organisatorischen Maßnahmen gehalten. Auf Einladung der Gesellschaft für Datenschutz und Datensicherheit (GDD) berichtete einer meiner Mitarbeiter über die Informations- und Kontrolltätigkeit meiner Behörde. Des weiteren führte ich ein Seminar im Rahmen der Fortbildung der Nachwuchsjuristen des Innenministeriums des Landes zum Thema "Datenschutz in der öffentlichen Verwaltung" in Güstrow durch.

3.3 Info-Blätter

Zur Verbreitung des Datenschutzgedankens wurde von mir ein Informationsfaltblatt herausgegeben, in welchem ich in allgemeiner Form die Aufgaben des Landesbeauftragten für den Datenschutz dargestellt habe. Außerdem bringe ich in Abständen "Informationen zum Datenschutz" heraus, welche sich jeweils mit aktuellen Themen beschäftigen. Bisher sind Informationsblätter zu folgenden Themen erschienen: Großer Lauschangriff, Datenschutz und Personalcomputer, Chipkarte, Patientenakten, Datenschutz und Verfassungsschutz, Datenschutz und Personen-Identifikation, Datenschutz und Telefax, Schutz persönlicher Daten, Adreßbücher und Datenmißbrauch. Informationen zu weiteren aktuellen Schwerpunkten sind in Arbeit.

3.4 Der behördliche (interne) Datenschutzbeauftragte

Häufig erhielt ich Anfragen zu den Befugnissen und Aufgaben eines internen Datenschutzbeauftragten. Deshalb habe ich bereits im November 1992 im Amtsblatt (AmtsBl. MV 1992 S. 1523 ff) entsprechende Hinweise veröffentlicht.

3.5 Beratung der internen Datenschutzbeauftragten der obersten Landesbehörden mit meiner Behörde

Aus den zahlreichen Kontakten mit den Ministerien habe ich festgestellt, wie wichtig der Erfahrungsaustausch der internen Datenschutzbeauftragten der obersten Landesbehörden mit meiner Behörde ist. Bei einer stattgefundenen ersten Beratung hat sich herausgestellt, daß doch in vielen Behörden gleiche oder ähnlich gelagerte datenschutzrechtliche Fragestellungen auftreten. Ich beabsichtige, die Beratungen in einem halbjährlichen Abstand durchzuführen. Darüber hinaus ist für 1994 eine ähnliche Veranstaltung für die internen Datenschutzbeauftragten der Kreise und kreisfreien Städte geplant.

4. Novellierungsvorschläge zum DSG MV

Die Erfahrung, die ich innerhalb dieses einen Jahres mit der Anwendung des Landesdatenschutzgesetzes gemacht habe, sind überwiegend positiv. Trotzdem sollen schon an dieser Stelle einige Vorschläge festgehalten werden, die im Rahmen einer künftigen Novellierung Berücksichtigung finden sollten.

Dateibeschreibung

Die Art und Weise der Verarbeitung personenbezogener Daten verändert sich genau so schnell, wie sich die technischen Möglichkeiten entwickeln. Immer komplexere DV-Systeme werden eingesetzt und schon kleinste Einheiten, wie z. B. ein Einzelplatz-PC, werden so leistungsfähig, daß große Datenbestände problemlos verwaltet werden können. Das spiegelt sich natürlich in der Form der Datenhaltung für einzelne Anwendungen wider.
Deshalb sind auch bei den öffentlichen Stellen immer häufiger DV-Systeme anzutreffen, die in zahlreichen Tabellen einer einzigen Datenbankanwendung die gemeinsame Datenbasis für mehrere Fachanwendungen enthalten. Als Beispiel dafür sei ein Personalinformationssystem genannt, bei dem Daten für die Stellenverwaltung und Daten für die Besoldung und Vergütung gemeinsam in einer Datenbank gehalten werden, Mitarbeiter verschiedener Organisationseinheiten aber nur auf den für sie relevanten Datenbestand zurückgreifen können. Zugriffsmöglichkeiten zu dem Teil der Daten, der zur Erfüllung der jeweiligen Fachaufgabe benötigt wird, werden durch Vergabe entsprechender Zugriffsrechte und Bereitstellung einschränkender Menüsysteme geregelt. Es ist nicht mehr ohne weiteres möglich, in Dateibeschreibungen der jetzigen Form die o.g. Art und Weise der Datenhaltung eindeutig widerzuspiegeln. Es sollte anstelle der Datei die jeweilige Fachaufgabe als Beschreibungsbasis dienen. Für Kontroll- und Revisionszwecke ist natürlich dann ein Hinweis auf den genauen Ablageort der Daten (Dateiname) zu geben. § 16 Abs. 1 Nr. 1 DSG MV wäre dementsprechend neu zu formulieren.

Technikfolgen- Abschätzung

Die Informationstechnik führt wie kaum eine andere technische Entwicklung zu tiefgreifenden Veränderungen in allen Lebensbereichen. Diese Tatsache erfordert eine kritische Auseinandersetzung mit den Folgen des Einsatzes von Informations- und Kommunikationstechnik. Dabei müssen so unterschiedliche Aspekte wie Lebensqualität, Umweltökonomie, Wirtschaftlichkeit, Sicherheit und Datenschutz berücksichtigt werden, um das informationelle Selbstbestimmungsrecht überhaupt wahrnehmen zu können.
In § 29 Abs. 5 DSG MV wird die Beobachtung der Auswirkungen von Informations- und Kommunikationstechnik auf die Arbeitsweise der öffentlichen Stellen als eine der Aufgaben des Landesbeauftragten für den Datenschutz dargestellt. Von der Verantwortung der öffentlichen Stellen, vor dem Einsatz neuer oder der wesentlichen Veränderung schon vorhandener automatisierter Verfahren zu prüfen, mit welchen Gefahren für die Rechte der Betroffenen die Nutzung dieser Verfahren verbunden sind, ist hier nicht die Rede. Lediglich der IT-Strukturrahmen für die Landesverwaltung von Mecklenburg-Vorpommern empfiehlt die Durchführung einer Risikoanalyse als Teil der Gefährdungsanalyse, um neben den möglichen materiellen auch zu erwartende immaterielle Schäden aufzeigen zu können.

Ich empfehle daher, entsprechend der schon in Niedersachsen (Niedersächsisches Datenschutzgesetz - NDSG) und Berlin (Informationsverarbeitungsgesetz - IVG) existierenden Vorschriften auch im DSG MV eine Technikfolgen-Abschätzung verpflichtend für den Anwender einzuführen. Die Verpflichtung zur Technikfolgen - Abschätzung im DSG MV kann ein erster Schritt dahin sein, Bürgerinnen und Bürgern eine bessere Transparenz und umfangreichere Gestaltungsrechte in der sich rasant entwickelnden Informationsgesellschaft zu bieten.

Der behördliche Datenschutzbeauftragte

In unserem Datenschutzgesetz ist bisher der interne behördliche Datenschutzbeauftragte nicht obligatorisch. Das ist jedoch bereits in vielen neueren Datenschutzgesetzen anderer Bundesländer der Fall. Bisher konnte ich lediglich empfehlen, daß öffentliche Stellen, welche personenbezogene Daten automatisiert verarbeiten, ab einer Zahl von fünf Bediensteten einen behördlichen Datenschutzbeauftragten bestellen sollten. Ich halte die obligatorische Einführung auf Gesetzesebene jedoch für notwendig, da nur dadurch der Bedeutung, aber auch der Komplexität datenschutzrechtlicher Erfordernisse Rechnung getragen wird.
Durch meine Besuche bei den Behörden kann ich zwar auf Mängel beim Umgang mit Daten hinweisen, die kontinuierliche Einhaltung und Verbesserung des Datenschutzes kann jedoch nur der interne Datenschutzbeauftragte vor Ort gewährleisten. Nur dieser kann sich ständig und umfassend auch mit kleineren Mißständen befassen.

Aus den vorgenannten Gründen würde ich folgende Formulierung vorschlagen:

"Öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten und hierbei in der Regel mindestens 5 Bedienstete ständig beschäftigen, haben einen Beauftragten für den Datenschutz zu bestellen. Beauftragte müssen die erforderliche Sachkenntnis und Zuverlässigkeit besitzen. Sie unterstützen die öffentliche Stelle bei der Sicherstellung des Datenschutzes."

Übermittlung an Stellen innerhalb/außerhalb des öffentlichen Bereiches

Die in § 12 Abs. 1 DSG MV getroffene Formulierung: "Die Übermittlung personenbezogener Daten an Stellen innerhalb des öffentlichen Bereichs ist über § 10 hinaus zulässig, wenn ..." hat in der Vergangenheit zu Mißverständnissen und deswegen zu Nachfragen geführt, da § 10 die Verarbeitung, nicht jedoch die Übermittlung regelt. Ich schlage daher folgenden Gesetzeswortlaut vor: "Die Übermittlung personenbezogener Daten an Stellen innerhalb des öffentlichen Bereichs ist über die in § 10 für die Verarbeitung genannten Voraussetzungen hinaus zulässig, wenn ...".

Des weiteren sollte in § 12 DSG MV (Datenübermittlung an Stellen innerhalb des öffentlichen Bereiches) zusätzlich klargestellt werden, daß die in den Absätzen 1 und 2 aufgestellten Voraussetzungen für Datenübermittlungen auch innerhalb der Behörde zu gelten haben. Diese Regelung ist erforderlich, da das Gesetz von dem organisatorischen und nicht von dem funktionalen Behördenbegriff ausgeht. Für die Auswirkungen auf das Recht des Betroffenen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen, ist es unerheblich, ob die Daten an eine andere öffentliche Stelle oder innerhalb der öffentlichen Stelle weitergegeben werden.

Gem. § 13 DSG MV (Übermittlungen an Stellen außerhalb des öffentlichen Bereiches) wird es als ausreichend angesehen, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat. In diesem Fall unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung.

Die vorliegende Übermittlungsregelung ist im Vergleich zu den Regelungen in anderen Landesdatenschutzgesetzen relativ weitgehend. Um dem Recht auf informationelle Selbstbestimmung ausreichend Rechnung zu tragen, sollte im Gesetzestext zusätzlich formuliert werden, daß der von der Datenübermittlung Betroffene nicht lediglich unterrichtet wird, sondern zusätzlich auf die Möglichkeit des Widerspruchs aufmerksam gemacht wird.
Es wäre weiterhin klarzustellen, daß der Grundsatz der Zweckbindung auch im Verhältnis zu den privaten Datenempfängern in der Weise abgesichert wird, daß eine spezielle Absprache zwischen übermittelnder Stelle und dem Empfänger zu erfolgen hat.

Schlußwort

Zum Schluß danke ich meinen Mitarbeiterinnen und Mitarbeitern für die geleistete Arbeit und ihren engagierten Einsatz.

Für die Zukunft erwarte ich, daß sich ein Teil der operativen Einsätze, wie beispielsweise die vielen anlaßbezogenen Kontrollen und Beratungen, zugunsten geplanter Einsätze verschieben wird. Bereits abgezeichnet hat sich, daß die entwicklungsbegleitende Beratung im Datenschutz an Bedeutung gewinnen wird. Es wäre wohl auch kaum zu vertreten, wenn gute technische Lösungen oder technologische Entwicklungen allein daran scheitern sollten, daß man die Belange des Datenschutzes nicht rechtzeitig berücksichtigt hat. Aber auch künftig werden die konkreten Sorgen des einzelnen Bürgers an erster Stelle bei der Erledigung meiner Aufgaben stehen.

Alle Aspekte des Datenschutzes konnte der vorliegende Bericht freilich nicht berücksichtigen - so zum Beispiel die zur Zeit in Gang befindliche Entwicklung eines einheitlichen europäischen Datenschutzes. Aber jeder hat die Möglichkeit, sich bei mir über dieses und weitere andere Themen zu informieren. Darüber hinaus werde ich im kommenden Berichtszeitraum wieder eine Reihe themengebundener Datenschutzblätter herausgeben.

Schwerin, den 05.01.1994

Dr. Werner Kessel

Anlage 1

Beschluß der 41. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. März 1991 zu Telekommunikation und Datenschutz

I.

Die Telekommunikation hat außerordentlich stark an Bedeutung gewonnen und ersetzt häufig den Brief oder auch das persönliche Gespräch: Über die dreißig Millionen deutschen Telefone werden monatlich rund drei Milliarden Gespräche geführt. Für die Privatsphäre des Bürgers in einer freiheitlichen Gesellschaft ist es unverzichtbar, daß Telefongespräche unkontrolliert und unbeobachtet geführt werden können. Von existentieller Bedeutung wird dies, wenn der Bürger in Notlagen gerät, aus denen er sich nur mit vertraulicher Beratung und Hilfe befreien kann. Daher unterstützen sowohl die Kirchen als auch Hilfs- und Beratungsorganisationen die Forderung des Datenschutzes, das "Grundrecht auf unbeobachtete Kommunikation"zu sichern.

Dieser Forderung muß die technische Ausgestaltung der Telekommunikationsnetze und -dienste folgen, und die rechtlichen Regelungen müssen diesen sich aus der Verfassung ergebenden Auftrag erfüllen. Der Gesetzgeber hat in dem am 1. Juli 1989 in Kraft getretenen Poststrukturgesetz die Bundesregierung aufgefordert, "Rechtsverordnungen zum Schutz personenbezogenener Daten der am Fernmeldeverkehr Beteiligten" zu erlassen. Der Ausschuß für Post und Telekommunikation und der Innenausschuß des Deutschen Bundestages haben mehrfach den Schutz des Fernmeldegeheimnissesangemahnt.

Die vom Bundesminister für Post und Telekommunikation vorgelegten Entwürfe von Verordnungen über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM (TDSV) und über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (UDSV), widersprechen in wesentlichen Punkten dem Grundrecht auf unbeobachtete Kommunikation. Dabei ist besonders unverständlich, daß der Bundesminister von bereits früher gemachten Zusagen an den Deutschen Bundestag wieder abgerückt ist.

Die Entwürfe bleiben in wichtigen Punkten unter dem Datenschutzniveau, das von der EG-Kommission in ihrem Richtlinienentwurf zum Schutz personenbezogener Daten und der Privatshäre in öffentlichen digitalen Telekommunikationsnetzen für den europäischen Binnenmarkt angestrebt wird.

II.

Ein wesentlicher Mangel besteht in der beabsichtigten Vollerfassung aller Verbindungsdaten von Telefongesprächen: Für jedes Telefonat soll bis zur Versendung der Entgeltrechnung bei der Deutschen Bundespost TELEKOM festgehalten werden, wer wann wie lange und mit wem telefoniert hat, nach Wahl des Kunden achtzig Tage darüber hinaus. Eine monatliche Auflistung dieser dem Fernmeldegeheimnis unterliegenden Informationen (Einzelentgeltnachweis) sollen Kunden - auch Arbeitgeber - auf Wunsch erhalten können. Außerdem können nach § 12 Fernmeldeanlagengesetz (FAG) auch Gerichte und Staatsanwaltschaften bei strafrechtlichen Ermittlungen jeder Art, also auch bei Bagatelldelikten, ohne besondere Voraussetzungen auf diese Daten zugreifen.

Abzulehnen ist auch die vorgesehene Beschränkung des Kunden auf die Alternative, daß von einem Anschluß die Telefonnummer des Anrufers immer oder nie beim Angerufenen angezeigt wird. Dem Recht auf informationelle Selbstbestimmung entspricht es, daß der Anrufer in jedem Einzelfall entscheiden kann, ob seine Rufnummer beim Angerufenen angezeigt wird. Umgekehrt hat jeder Angerufene selbstverständlich das Recht, nur Gespräche entgegenzunehmen, bei denen die Nummer des Anrufers angezeigt wird.

III.

Die Datenschutzbeauftragten fordern:

1. Alle - durch die computergesteuerte Vermittlungstechnik entstehenden - Verbindungsdaten sind nach dem Ende der Verbindung mit folgender Maßgabe zu löschen:

   In die Entgeltdatenverarbeitung dürfen nur diejenigen Daten eingehen, die zur Berechnung der Entgelte in Summenform unerläßlich sind. Auf Antrag des Kunden darf zur Prüfung der Richtigkeit des in Rechnung gestellten Entgeltes oder zur Erstellung eines Einzelentgeltnachweises die Rufnummer des Angerufenen nur in einer zumindest um die letzten vier Ziffern verkürzten Form gespeichert werden. Die Daten sind spätestens achtzig Tage nach dem Absenden der Entgeltrechnung zu löschen.

   Die Entscheidung des Kunden über die Form der Abrechnung muß auch bei der Abrechnung zwischen verschiedenen Netzbetreibern respektiert werden.

2. Die Erstellung von "Kommunikationsprofilen", die Aussagen über das persönliche Telefonierverhalten des Bürgers und die Nutzung anderer Telekommunikationsdienste enthalten, muß ausgeschlossen sein.

3. Bei der Anzeige der Rufnummer des Anrufers beim Angerufenen müssen beide die Wahlmöglichkeiten haben, diese Anzeige entweder auf Dauer oder im Einzelfall "auf Knopfdruck" zu unterdrücken.

4. Ausnahmen von diesen Grundsätzen - zum Beispiel zur Aufklärung telefonischer Bedrohungen oder in Notfällen - müssen begründet, ausdrücklich geregelt und für den Betroffenen transparent sein.

5. Die Konferenz bekräftigt ihre Forderung (Beschluß vom 4./5. Oktober 1990), Eingriffe in das grundsätzlich geschützte Fernmeldegeheimnis (Art. 10 GG) auf das unerläßliche Maß zu beschränken und insbesondere nicht schon im Bereich der Bagatellkriminalität zuzulassen. Die Regelung des § 12 FAG hat im Zuge der technischen Entwicklung eine verfassungsrechtlich bedenkliche neue Qualität erhalten, da sie nunmehr auch die bei Einsatz neuer Kommunikationstechniken anfallenden Abrechnungs-, Verbindungs-, Nutzungs- und Inhaltsdaten umfaßt. Statt im FAG sollten die Eingriffsmöglichkeiten in das Fernmeldegeheimnis im Rahmen der Strafverfolgung - schon aus Gründen der Normenklarheit - in der Strafprozeßordnung unter engen Voraussetzungen und Beschränkungen abschließend geregelt werden.

Anlage 2

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Datenschutz bei internen Telekommunikationsanlagen

Der zunehmende Einsatz von digitalen Telekommunikationsanlagen (TK-Anlagen) in Wirtschaft und Verwaltung birgt Datenschutzrisiken in sich, denen durch eine datenschutzfreundliche Ausgestaltung der Technik und durch geeignete bereichsspezifische Regelungen entgegengewirkt werden muß. Telefongespräche stehen - auch wenn sie von einem Dienstapparat aus geführt werden - unter dem Schutz des Grundgesetzes. Dies hat das Bundesverfassungsgericht in seiner neueren Rechtsprechung hervorgehoben.

Der Schutz des Fernmeldegeheimnisses und des nicht öffentlich gesprochenen Wortes ist gerade bei Arbeitnehmern bedeutsam, da diese sich in einem besonderen Abhängigkeitsverhältnis befinden; aber auch das informationelle Selbstbestimmungsrecht Dritter, die anrufen oder angerufen werden, muß gewahrt werden.

Entsprechende bundesrechtliche Regelungen für interne TK-Anlagen sind überfällig, da in diesen Anlagen - insbesondere wenn sie digital an das öffentliche ISDN angeschlossen sind - umfangreiche Sammlungen sensibler personenbezogener Daten entstehen können, die sich auch zur Verhaltens- und Leistungskontrolle eignen und zudem Hinweise auf das Kommunikationsverhalten aller Gesprächsteilnehmer geben.

Die Regelungen sollten verbindliche Vorgaben für die technische Ausgestaltung von TK-Anlagen geben und den Umfang der zulässigen Datenverarbeitung festlegen:

- Es müssen die technischen Voraussetzungen gewährleistet sein, daß Anrufer und Angerufene die Rufnummernanzeige fallweise abschalten können.

- Die automatische Speicherung der Rufnummern von externen Anrufern nach Beendigung des Telefongesprächs ist auszuschließen, es sei denn, eine sachliche Notwendigkeit besteht hierfür (z.B. bei Feuerwehr und Rettungsdiensten).

- Die Weiterleitung eines Anrufs an einen anderen als den gewählten Anschluß sollte dem Anrufer so rechtzeitig signalisiert werden, daß dieser den Verbindungsaufbau abbrechen kann. Das Mithören und Mitsprechen weiterer Personen bei bestehenden Verbindungen sollte nur nach eindeutiger und rechtzeitiger Ankündigung möglich sein.

- Verbindungsdaten einschließlich der angerufenen Telefonnummern sollten nach Beendigung der Gespräche nur insoweit gespeichert werden, als dies für Abrechnungs- und zulässige Kontrollzwecke erforderlich ist. Die Nummern der Gesprächspartner bei Arbeitnehmervertretungen, internen Beratungseinrichtungen und sonstigen auf Vertraulichkeit angewiesenen Stellen dürfen nicht registriert werden.

- Die TK-Anlagen müssen durch geeignete technische Maßnahmen gegen unberechtigte Veränderungen der Systemkonfiguration und unberechtigte Zugriffe auf Verbindungs- und Inhaltsdaten geschützt werden.

Da TK-Anlagen geeignet sind, das Verhalten und die Leistung der Arbeitnehmer zu kontrollieren, und sie überdies häufig die Arbeitsplatzgestaltung beeinflussen, löst ihre Einführung in Betrieben und Behörden Mitbestimmungsrechte der Betriebsräte und überwiegend auch der Personalräte aus. Sie dürfen daher nur betrieben werden, wenn unter Beteiligung der Arbeitnehmervertretungen verbindlich festgelegt wurde, welche Leistungsmerkmale aktiviert und unter welchen Bedingungen sie genutzt werden, welche Daten gespeichert, wie und von wem sie ausgewertet werden. Die Nutzer der TK-Anlage sind über den Umfang der Datenverarbeitung umfassend zu unterrichten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, daß umgehend datenschutzrechtliche Regelungen für den Einsatz und die Nutzung von internen TK-Anlagen mit einer bereichsspezifischen Rechtsgrundlage für die Verarbeitung von Arbeitnehmerdaten geschaffen werden.

Anlage 3

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Entwurf eines Gesetzes zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung - Gesundheits-Strukturgesetz 1993 -

Die Bundesregierung will mit dem Gesundheits-Strukturgesetz dem Kostenanstieg in der gesetzlichen Krankenversicherung entgegenwirken. Dieses begrüßenswerte Ziel soll nach dem vorgelegten Gesetzentwurf u.a. auch durch eine verstärkte automatisierte Datenverarbeitung erreicht werden. Die damit verbundenen Eingriffe in die Persönlichkeitsrechte der Versicherten und in die sie schützende ärztliche Schweigepflicht müssen auf das unbedingt Notwendige beschränkt werden. Die Datenschutzkonferenz hält vor allem folgende Verbesserungen des Gesetzentwurfs für notwendig:

- Der Gesetzentwurf sieht vor, daß die Krankenhäuser den Krankenkassen mehr Versichertendaten zur Verfügung stellen müssen als bisher. Es sollte deshalb eingehend geprüft werden, ob die Krankenkassen tatsächlich alle geforderten Angaben benötigen; die Aufgabenteilung zwischen Krankenkassen und Medizinischem Dienst muß aufrechterhalten bleiben.

- Für das Modellvorhaben zur Überprüfung des Krankenhausaufenthalts müssen die Erhebung, Verwendung und Löschung von Versichertendaten durch den Medizinischen Dienst präziser als bisher vorgesehen geregelt werden.

- Beim Einzug der Vergütung der Krankenhausärzte für Wahlleistungen durch Krankenhäuser sollte die Einschaltung privater Abrechnungsstellen ohne Einwilligung der Patienten nicht zugelassen werden, da dabei Abrechnungsdaten an Dritte offenbart werden. Die Daten sind gegen unbefugte Offenbarung und Beschlagnahme rechtlich besser geschützt, wenn sie - auch zur Abrechnung - im Krankenhaus verbleiben. Die Krankenhäuser sind zudem selbst in der Lage, die Vergütung einzuziehen.

- Für die neu vorgesehenen Patienten-Erhebungsbögen zur Ermittlung des Bedarfs an Pflegepersonal im Krankenhaus sollte eine strikte Zweckbindung sowie eine frühestmögliche Löschungs- oder Anonymisierungspflicht festgelegt werden. Eine Überlassung der Patienten-Erhebungsbögen in der im Gesetzentwurf vorgesehenen Fassung an die Krankenkassen ist abzulehnen.

Anlage 4

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Lauschangriff

Die Datenschutzbeauftragten des Bundes und der Länder erklären (bei Gegenstimme des LfD Bayern):

Nachdem erst vor kurzem mit dem Gesetz zur Bekämpfung der organisierten Kriminalität die Befugnisse der Strafverfolgungsbehörden erheblich erweitert worden sind und obwohl über den Erfolg dieser Maßnahmen noch keine Erfahrungen gesammelt werden konnten, wird gegenwärtig parteiübergreifend vielfach die Forderung erhoben, der Polizei in bestimmten Fällen das heimliche Abhören und Herstellen von Bild- und Tonaufzeichnungen in und aus Wohnungen (sog. "Lauschangriff")zu ermöglichen.

1. Das Grundgesetz gewährt jedem einen unantastbaren Bereich privater Lebensgestaltung, der der Einwirkung der öffentlichen Gewalt entzogen ist. Dem einzelnen muß um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein "Innenraum" verbleiben, in dem er "sich selbst besitzt" und "in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt" (BVerfGE 27,1 ff.). Jedem muß ein privates Refugium, ein persönlicher Bereich bleiben, der obrigkeitlicher Ausforschung - insbesondere heimlicher - entzogen ist. Dies gilt gegenüber Maßnahmen der Strafverfolgung vor allem deshalb, weil davon auch unverdächtige oder unschuldige Bürger betroffen sind. Auch strafprozessuale Maßnahmen dürfen nicht den Wesensgehalt eines Grundrechts, insbesondere nicht das Menschenbild des Grundgesetzes verletzen.

2. Die Datenschutzbeauftragten nehmen die Gefahren, die das organisierte Verbrechen für die Opfer und auch für die Demokratie und den Rechtsstaat heraufbeschwört, sehr ernst. Sie sind allerdings der Meinung, daß eine angemessene Abwägung zwischen der Verfolgung der organisierten Kriminalität und dem Schutz der Persönlichkeitsrechte der Bürger geboten und möglich ist und es eine Wahrheitserforschung um jeden Preis auch künftig im Strafprozeßrecht nicht geben darf. Daraus folgt, daß der Lauschangriff auf Privatwohnungen für Zwecke der Strafverfolgung auch in Zukunft nicht erlaubt werden darf.

3. Eine andere Frage ist, ob und unter welchen Voraussetzungen der Gesetzgeber für Räume, die allgemein zugänglich sind oder beruflichen oder geschäftlichen Tätigkeiten dienen (z.B. Hinterzimmer von Gaststätten, Spielcasinos, Saunaclubs, Bordelle), einen Lauschangriff zulassen kann. Hierfür sind Mindestvoraussetzungen ein eng begrenzter abschließender Straftatenkatalog, die Verwendung der gewonnenen Erkenntnisse ausschließlich zur Verfolgung dieser Straftaten, ein strikter Richtervorbehalt sowie die Wahrung besonderer Amts- und Berufsgeheimnisse.

Anlage 5

Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. Februar 1993 zur Richtlinie des Rates vom 07. Juni 1990 über den freien Zugang zu Informationen über die Umwelt (30/313/EWG)

Im Interesse eines wirksamen Umweltschutzes hat der Ministerrat der Europäischen Gemeinschaft die Umweltinformationsrichtlinie erlassen, die jedem Bürger ein Recht auf Zugang zu den bei Behörden vorhandenen Informationen über die Umwelt gewährt. Da es nicht gelungen ist, die Richtlinie innerhalb der vorgegebenen Frist bis Ende 1992 in deutsches Recht umzusetzen, herrscht gegenwärtig Rechtsunsicherheit bei Bürgern und Behörden über den Zugang zu Umweltinformationen.

Die Konferenz der Datenschutzbeauftragten sieht in der Gewährleistung eines freien Zugangs zu Umweltinformationen einen wesentlichen Beitrag zu größerer Transparenz des Verwaltungshandelns. Informationsfreiheit und Datenschutz bilden dabei keinen unlösbaren Gegensatz. Die Konferenz hält es für geboten, die Arbeit am Entwurf des Umweltinformationsgesetzes (UIG) zügig zum Abschluß zu bringen. Sie begrüßt entsprechende Initiativen auf Landesebene.

In den Gesetzen sind folgende datenschutzrechtliche Grundsätze zu berücksichtigen:

Soweit Umweltinformationen auf Personen beziehbar sind, ist das Grundrecht auf informationelle Selbstbestimmung zu beachten. Deshalb sind Informationen grundsätzlich in anonymisierter oder aggregierter Form zu geben. Wenn damit das Informationsinteresse nicht erfüllt werden kann, sind Eingriffe in das Persönlichkeitsrecht nur unter klaren gesetzlichen Voraussetzungen zulässig, welche die Rechte, insbesondere die Verfahrensrechte, der Betroffenen wahren.

Anlage 6

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 zu regelmäßigen Datenübermittlungen an die öffentlich-rechtlichen Rundfunkanstalten und die Gebühreneinzugszentrale (GEZ) (gegen die Stimme Bayerns und bei Stimmenthaltung Sachsens)

Die öffentlich-rechtlichen Rundfunkanstalten drängen seit langem auf die Schaffung einer Rechtsgrundlage für die regelmäßige Übermittlung von Meldedaten aller Einwohner an die gemeinsame Gebühreneinzugszentrale (GEZ). Sie verweisen dazu auf bereits bestehende Regelungen in den Ländern Hessen und Nordrhein-Westfalen. Auf Bitten der Konferenz der Regierungschefs der Länder hat deshalb nunmehr der zuständige Arbeitskreis der Innenministerkonferenz einen Musterentwurf für eine bundesweite Lösung im Melderecht erarbeitet. Der Entwurf sieht vor, daß künftig alle Meldebehörden in der Bundesrepublik im Fall der Anmeldung, Abmeldung oder des Todes eines volljährigen Einwohners bis zu acht Kerndaten an die GEZ übermitteln dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen eine derartige Regelung insbesondere aus folgenden Gründen ab:

Die Regelung könnte im Ergebnis zu einem bundesweiten Melderegister bei Volljährigen führen. Sie könnte außerdem gegen das verfassungsrechtlich garantierte Verhältnismäßigkeitsprinzip verstoßen. Den Rundfunkanstalten stünde möglicherweise der unkontrollierte Zugriff auf Millionen personenbezogener Daten volljähriger Einwohner der Bundesrepublik zu, obwohl es für die Rundfunkanstalten nur von Interesse ist, welcher Einwohner bei ihnen gebührenpflichtig ist und bislang seine Gebührenpflicht nicht angemeldet hat. Das vorgesehene generelle Übermittlungsverfahren kennt keine Unterscheidung zwischen erforderlichen und nicht erforderlichen Daten, sondern überläßt diese Unterscheidung der GEZ. Über die Frage, ob ein Volljähriger überhaupt gebührenpflichtig ist, geben die Meldedaten keine Auskunft. Das muß nach wie vor im herkömmlichen Verfahren durch Befragung ermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder sind bereit, an geeigneten und verfassungskonformen Lösungen der Landesregierungen zur Sicherung des Gebührenaufkommens der Rundfunkanstalten mitzuwirken.

Anlage 7

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 zur Gewährleistung des Datenschutzes bei der Mobilkommunikation

Die Verbreitung mobiler Sprach- und Datenübertragungsdienste hat in jüngster Vergangenheit stark zugenommen. So gibt es bereits jetzt in Deutschland mehr als eine Million Teilnehmer der Funktelefonnetze C und D; mit der Aufnahme des Regelbetriebs von MODACOM ist seit Juni dieses Jahres auch ein öffentlicher mobiler Datenübertragungsdienst in Deutschland verfügbar. Es ist zu erwarten, daß sich die Teilnehmerzahl mobiler Kommunikationsdienste in Zukunft weiter vergrößern wird.

Die mit der Nutzung von Mobilfunkdiensten verbundenen Vorteile gehen mit Gefährdungen für den Datenschutz einher. Neben den auch bei anderen Telekommunikationsdiensten gespeicherten Angaben, wer wann mit wem in Verbindung war, wird bei der Mobilkommunikation auch erhoben, wo sich der mobile Teilnehmer jeweils aufhält. Die Speicherung dieser Daten ermöglicht die Bildung von problematischen Bewegungsprofilen.

Darüber hinaus ist vielfach auch die Vertraulichkeit der Kommunikationsinhalte gefährdet, insbesondere dann, wenn Daten unverschlüsselt per Funk übertragen werden. Dies gilt sowohl für die analogen Funktelefon-Netze B und C als auch für den von der Deutschen Bundespost Telekom betriebenen mobilen Datenübertragungsdienst MODACOM. Bei satellitengestützten Diensten ist es sogar möglich, die übertragenen Daten im gesamten, teilweise viele tausend Quadratkilometer umfassenden Abstrahlbereich des Satelliten unbemerkt abzuhören und aufzuzeichnen.

Von den Herstellern und Betreibern mobiler Kommunikationsdienste ist zu fordern, daß sie diesen Gefahren für das Fernmeldegeheimnis und für den Datenschutz durch eine entsprechende Gestaltung entgegenwirken und technische Vorkehrungen für eine sichere Kommunikation treffen.

Die Teilnehmer mobiler Kommunikationsdienste müssen von den Anbietern, Herstellern und Betreibern über die mit der Nutzung verbundenen Risiken und das erreichte Sicherheitsniveau aufgeklärt werden. Sofern bei bestimmten Diensten Sicherheitsmerkmale realisiert sind - wie z. B. in den digitalen D-Netzen -, muß die Sicherheit für die Aufsichts- und Kontrollorgane auch nachprüfbar sein. Falls durch den Dienstbetreiber nicht die erforderliche Sicherheit gewährleistet werden kann, ist eine Übertragung personenbezogener oder sonstiger sensibler Daten mit dem jeweiligen Dienst nur dann vertretbar, wenn der Benutzer zusätzliche Sicherheitsvorkehrungen trifft, also z.B. die übertragenen Daten anwendungsseitig verschlüsselt.
Zusätzlich kompliziert wird die Datenschutzproblematik bei der Mobilkommunikation dadurch, daß unter Umständen bei verschiedenen Dienst- und Netzbetreibern, aber auch bei anderen Unternehmen - den sogenannten Service-Providern, die lediglich Dienste vermarkten -, personenbezogene Daten gespeichert werden.

Hier muß im Zuge der anstehenden Überarbeitung des Telekommunikationsrechts dafür Sorge getragen werden, daß sich die Verarbeitung der Kommunikationsdaten auf das wirklich erforderliche Maß beschränkt und daß die Nutzer darüber aufgeklärt werden, bei welcher Stelle welche personenbezogenen Daten gespeichert oder sonst verarbeitet werden.

Besonders problematisch ist es, wenn bei der internationalen Mobilkommunikation auch in solchen Staaten personenbezogene Daten gespeichert werden, in denen kein ausreichendes Datenschutzniveau gewährleistet ist oder in denen das Fernmeldegeheimnis nicht sichergestellt wird. Deshalb ist es erforderlich, auf internationaler Ebene Regelungen zu treffen, die den Datenschutz bei mobilen Kommunikationsdiensten gewährleisten.

Die Konferenz unterstreicht aus diesem Grunde ihre Forderung, die Arbeiten an der EG-Richtlinie über Datenschutz im ISDN und in öffentlichen digitalen Mobilfunknetzen zu einem datenschutzrechtlich befriedigenden Abschluß zu bringen. Auch für den noch gänzlich datenschutzrechtlich ungeregelten Bereich der Satellitenkommunikation müssen endlich völkerrechtlich verbindliche Regelungen getroffen werden.

Anlage 8

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 zum Integrierten Verwaltungs- und Kontrollsystem (InVeKoS) (Verordnungen der EWG Nrn. 3508/92 und 3887/92)

Die vom Ministerrat der EG 1992 beschlossene Reform der gemeinsamen Agrarpolitik sieht die Angleichung der gemeinschaftlichen Preise für bestimmte Kulturpflanzen an den Weltmarkt vor und gewährt auf Antrag als Ausgleich für die dadurch bedingten Einkommenseinbußen flächen- und tierbezogene Zuwendungen an die Erzeuger. Zur Verhinderung einer mißbräuchlichen Verwendung von Fördermitteln hat die EG die Mitgliedsstaaten dabei zur Einführung eines "Integrierten Verwaltungs- und Kontrollsystem (InVeKoS)" verpflichtet. Diese haben danach integrierte Datenbanken mit Angaben über Flurstücke, deren kulturartige Nutzung sowie den Tierbestand einzurichten und in einem Mindestumfang entsprechende Kontrollen durchzuführen.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder hat die EG mit dem "Integrierten Verwaltungs- und Kontrollsystem" den Landwirtschaftsverwaltungen der Länder ein Überwachungssystem verordnet, das dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot, widersprechen kann. Insbesondere legt das EG-Recht für die Kontrolldichte nur ein Mindestmaß an Kontrollen, jedoch keine Obergrenze fest.

Zur Vermeidung unverhältnismäßiger Einschränkungen des informationellen Selbstbestimmungsrechts der betroffenen Landwirte fordern daher die Datenschutzbeauftragten des Bundes und der Länder,

- ortsunabhängige Überwachungsmöglichkeiten (Fernerkundung mittels Satellit oder Flugzeug) nicht für eine flächendeckende Totalüberwachung einzusetzen, sondern auf den von der EG geforderten Stichprobenumfang zu beschränken;
- bei der Nutzung des Kontrollsystems InVeKoS und der darin gespeicherten personenbezogenen Daten den Grundsatz der Verhältnismäßigkeit und insbesondere der Zweckbindung zu beachten;
- nur dezentrale Datenbanken in den einzelnen Bundesländern einzurichten (keine Euro- oder Zentraldatenbank über Landwirte!), und an zentrale Datenbanken keine personenbezogenen Daten zu übermitteln;
- zu beachten, daß die EG-Verordnungen zu InVeKoS keine Rechtsgrundlage für eine Erweiterung der Nutzungen enthalten (z. B. zu Kontrollzwecken bei anderen landwirtschaftlichen Förderungsmaßnahmen oder außerhalb des landwirtschaftlichen Bereichs, z. B. zur Besteuerung).

Anlage 9

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 zum Datenschutz bei der Privatisierung der Deutschen Bundespost Telekom und bei der europaweiten Liberalisierung des Telefonnetzes und anderer Telekommunikationsdienste

Im Zuge der sog. Postreform II soll die Deutsche Bundespost Telekom - nach der dafür notwendigen Änderung des Grundgesetzes in Form einer Aktiengesellschaft privatisiert werden. Zugleich hat der Ministerrat der Europäischen Gemeinschaften in seiner Entschließung vom 22. Juli 1993 (Amtsblatt der EG Nr. C 213 vom 6. 8. 1993) seine Entschlossenheit bekräftigt, die Monopole im öffentlichen Sprachtelefondienst (Festnetz) der Mitgliedstaaten bis zum 1. Januar 1998 zu beseitigen.

In absehbarer Zeit werden daher in Deutschland neben der "Telekom AG" auch im Telefondienst andere private Unternehmen Telekommunikationsdienstleistungen anbieten. Diese Privatisierung hat Konsequenzen für den Datenschutz, der bisher für die Deutsche Bundespost Telekom auf einem vergleichsweise hohen Niveau geregelt ist. Insbesondere das grundgesetzlich garantierte Fernmeldegeheimnis würde für private Netzbetreiber und Diensteanbieter jedenfalls nicht mehr unmittelbar gelten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für unabdingbar, daß durch die Privatisierung und Liberalisierung der Schutz der Bürger insbesondere in solchen Bereichen nicht verringert wird, die - wie der Telefondienst - der Daseinsvorsorge zuzurechnen sind. So wie bisher die konkurrierenden privaten Betreiber der Mobilfunknetze einen gleichmäßig hohen Datenschutzstandard gewährleisten müssen, hat dies auch zu gelten, wenn in Zukunft private Unternehmen im Wettbewerb miteinander stationäre Telefonnetze betreiben und entsprechende Dienste anbieten. Die Einhaltung von datenschutzrechtlichen Bestimmungen bei Telekommunikationsnetzen und -diensten muß zukünftig von einer unabhängigen Stelle nach bundesweit einheitlichen Kriterien und von Amts wegen kontrolliert werden können.

Da der Wettbewerb zwischen privaten Netzbetreibern und Diensteanbietern nicht nur national begrenzt, sondern im europäischen Binnenmarkt stattfinden wird, sind auch Rechtsvorschriften der Europäischen Gemeinschaften erforderlich, die einen möglichst hohen, einheitlichen Datenschutzstandard in der Telekommunikation gewährleisten.

Anlage 10

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 zu kartengestützten Zahlungssystemen im öffentlichen Nahverkehr

Mit der Weiterentwicklung von Chipkarten werden kartengestützte Zahlungssysteme zunehmend auch im Verkehrsbereich eingesetzt. Damit besteht die Gefahr, daß sehr detaillierte Bewegungsprofile entstehen, die den persönlichen Bereich jedes Einzelnen einschränken und z. B. auch für Strafverfolgungsbehörden, Finanzämter und für die Werbewirtschaft von Interesse sein könnten. Da sämtliche Fahrten für einen gewissen Zeitraum aufgelistet werden können, hat jeder Kontoinhaber die Möglichkeit, Fahrten sämtlicher Familienmitglieder jederzeit nachzuvollziehen.

So sind im öffentlichen Nahverkehr zahlreiche sogenannte Postpaid-Verfahren in Erprobung, bei denen dem Fahrgast am Monatsende die aufsummierten Fahrpreise vom Konto abgebucht werden. Diese Zahlungsweise erfordert die Speicherung umfangreicher personenbezogener Daten: Neben der Konto-Nr. und Bankleitzahl des Fahrgastes werden sowohl Datum und Uhrzeit des Fahrscheinkaufs bzw. des Fahrantritts als auch Automatennummer und Preisstufe der jeweiligen Fahrt erhoben.

Eine solche Vorgehensweise ist umso problematischer, als technische Alternativen existieren, die weitaus datenschutzfreundlicher sind. Im öffentlichen Nahverkehr können - wie skandinavische und auch deutsche Projekte aufzeigen - Wertkartensysteme eingesetzt werden, bei denen im voraus bezahlt wird und die daher gänzlich ohne personenbezogene Daten auskommen.

Die Datenschutzbeauftragten halten es daher für dringend erforderlich, daß mehr als bisher bei der Einführung kartengestützter Zahlungssysteme darauf geachtet wird, die "datenfreie Fahrt" zu ermöglichen. Im öffentlichen Nahverkehr sollte weiterhin auch die datenschutzfreundlichste Lösung angeboten werden: Der Kauf einer Fahrkarte am Automaten mit Bargeld.

Die Konferenz fordert weiter, daß noch vor der Pilotierung der dargestellten Technikvorhaben im Verkehrsbereich eine Untersuchung möglicher Alternativen, eine Analyse der von ihnen ausgehenden Gefahren für das informationelle Selbstbestimmungsrecht und eine Darstellung der technischen und organisatorischen Möglichkeiten zur Gewährleistung des Persönlichkeitsschutzes zu erstellen ist (Technikfolgen-Abschätzung). Nur Verfahren mit dem geringsten Eingriff in das allgemeine Persönlichkeitsrecht sollten eine Chance zur Erprobung erhalten.

Anlage 11

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 zur Gefährdung der Vertraulichkeit der Funkkommunikation von Sicherheitsbehörden und Rettungsdiensten

Durch die Aufhebung der bisher gültigen Beschränkungen der zulässigen Empfangsbereiche für Rundfunkempfänger zum 30. Juni 1992 werden zunehmend Empfangsgeräte betrieben, die das Abhören des Funkverkehrs ermöglichen. Dies stellt eine erhebliche Bedrohung des Fernmeldegeheimnissesdar.

Die Datenschutzbeauftragten des Bundes und der Länder beobachten die damit verbundene Gefährdung der Vertraulichkeit der Funkkommunikation von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) mit Sorge. Sie erkennen die Bemühungen der Polizeiverwaltungen der Länder an, durch zusätzliche technische Maßnahmen die Sicherheit des Sprechfunkverkehrs zu erhöhen. Sie stellen jedoch fest, daß die erforderliche Vertraulichkeit bisher nicht gewährleistet werden konnte. Auch Sprachverschleierungssysteme erreichen diese nicht hinreichend.

Daher begrüßt die Konferenz die im Rahmen des Schengener Abkommens getroffene grundsätzliche Entscheidung, im BOS-Bereich eine europäische Normierung zu erarbeiten, die die Digitalisierung und eine Verschlüsselung des BOS-Funkverkehrs vorsieht. Die Konferenz hält es für erforderlich, daß das Normierungsverfahren so zügig wie möglich durchgeführt wird und auch schon vor der Umsetzung dieser Norm alle Möglichkeiten für einen effektiven Schutz der Vertraulichkeit des BOS-Funkverkehrs entsprechend dem jeweiligen Stand der Technik genutzt werden.

Die Konferenz weist weiter darauf hin, daß nicht nur bei den Behörden der Polizei, sondern auch in anderen BOS-Bereichen, wie z. B. dem Rettungswesen, eine Vertraulichkeit des Funkverkehrs zu gewährleisten ist. Daher sind auch in den übrigen BOS-Bereichen frühestmöglich entsprechende Absicherungenzur Vertraulichkeit des Funkverkehrs gefordert.

Anlage 12

ORGANISATIONSHILFE ZUR VERNICHTUNG

VON

SCHRIFTGUT

(Organisationshilfe- Schriftgutvernichtung)

Über die Organisationshilfe - Schriftgutvernichtung

Nach § 17 Abs. 1 Satz 1 DSG MV hat die mit personenbezogenen Daten umgehende und in ihrem Auftrag tätige Stelle die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich und angemessen sind, um einen den Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz entsprechenden Umgang mit Daten sicherzustellen.
Insbesondere ist zu gewährleisten, daß der Betroffene sein Recht auf Auskunft bzw. Sperrung gem. §§ 20, 21 DSG MV wahrnehmen kann.

Werden personenbezogenen Daten in nicht automatisierten Dateien oder Akten verarbeitet, sind Maßnahmen zu treffen, die je nach Art der Datenverarbeitung und der zu schützenden personenbezogenen Daten erforderlich sind, um die Zugangskontrolle, die Datenträgerkontrolle, die Übermittlungskontrolle, Transport- und Organisationskontrolle zu gewährleisten (§ 17 Abs. 3 DSG MV).

Die vorliegende Organisationshilfe zur Datensicherung beim Vernichten von Schriftgut (Organisationshilfe - Schriftgutvernichtung) soll helfen zu erkennen, unter welchen Gesichtspunkten die Datensicherheit zu überprüfen ist und welche Sicherungsziele im Einzelfall bei der Vernichtung von Schriftgut durch geeignete Maßnahmen in angemessenem Umfang erreicht werden müssen. Die Organisationshilfe - Schriftgutvernichtung enthält Fragen zur Datensicherheit, die auf Sachverhalte hinweisen, zu denen angemessene Maßnahmen zu treffen sind. Im allgemeinen wird es verschiedene Möglichkeiten geben, dem Anliegen zu entsprechen.
Bei den öffentlichen Stellen des Landes Mecklenburg-Vorpommern unterliegt die Vernichtung von Schriftgut mit personenbezogenen Daten im allgemeinen dem Datenschutz (DSG MV). Insbesondere dann, wenn Schriftgut im Auftrag durch einen Dritten vernichtet wird, kann es erforderlich sein, die teilweise unterschiedlichen Regelungen des Bundesdatenschutzgesetzes (BDSG) und des Sozialgesetzbuchs (SGB) anzuwenden. Entsprechende Verweise enthält der Abschnitt D (Vernichten des Schriftguts als Datenverarbeitung im Auftrag durch einen Dritten).

A. Allgemeine Anforderungen

Bezüglich der zeitlichen Begrenzung der Verantwortung einer öffentlichen Stelle bei der Vernichtung ihres Schriftguts gilt folgender Grundsatz:

Eine öffentliche Stelle ist für die Datensicherheit von Schriftgut, das vernichtet werden soll, verantwortlich, bis deren Vernichtung abgeschlossen ist, d.h., bis die im Schriftgut enthaltenen personenbezogenen Daten als gelöscht (§ 3 Abs. 7 Nr. 6 DSG MV) gelten können.

- Die öffentliche Stelle muß daher über jedes Schriftgut mit personenbezogenen Daten bis zu deren Vernichtung die uneingeschränkte Verfügungsgewalt besitzen.

- Insbesondere darf zu venichtendes Schriftgut mit personenbezogenen Daten vor Abschuß der Vernichtung nicht in das Eigentum Dritter übergehen.

- Bis zum Ende ihrer Verantwortlichkeit, d. h. bis zum Abschluß der Vernichtung des Schriftguts, hat sich die öffentliche Stelle durch Kontrollen von der ordnungsgemäßen Durchführung der Vernichtung zu überzeugen.

1. Durch welchen technischen Vorgang oder nach welchem Verfahren wird das Schriftgut vernichtet?

   1.1 Ist der Zustand, in dem sich das Schriftgut befinden muß, um als vernichtet gelten zu können, festgelegt?

   1.2 Gibt es spezifizierte Anforderungen analog der Norm DIN 32757 (Vernichten von Informationsträgern) an den für das Vernichten des Schriftguts vorgesehenen technischen Vorgang oder an das Verfahren?

2. Ist gewährleistet, daß personenbezogene Daten ausnahmslos als gelöscht (§ 3 Abs. 7 Nr. 6 DSG MV) gelten können, sobald das Schriftgut, auf dem diese Daten aufgezeichnet sind, nach dem unter 1. genannten technischen Vorgang oder Verfahren vernichtet wurden?

3. Ist durch eine institutionalisierte Kontrolle gewährleistet, daß Abweichungen von bestehenden Vorschriften und besondere Vorkommnisse der Leitung der öffentlichen Stelle bekannt werden?

   3.1 Wurde eine Person oder Organisationseinheit mit der Kontrolle der Vernichtung von Schriftgut beauftragt?

   - Erfolgte der Auftrag schriftlich?

   - Ist allgemein bekannt, daß diese Person oder Organisationseinheit den Auftrag hat, entsprechende Kontrollen durchzuführen?

   - Berichtet die mit der Kontrolle beauftragte Person oder Organisationseinheit unmittelbar an die Leitung der öffentlichen Stelle?

   3.2 Wird der Ablauf der Vernichtung lückenlos kontrolliert?

   - Wird die Sicherheit einer eventuellen zentralen Sammelstelle für zu vernichtendes Schriftgut kontrolliert?

   - Wird die ordnungsgemäße Durchführung einer eigenen zentralen Vernichtung kontrolliert?

   - Wird bei einer Vernichtung des Schriftguts durch Dritte der Transport kontrolliert?

B. Vernichten des Schriftgutes durch den einzelnen Mitarbeiter

1. Ist schriftlich geregelt, in welchen Fällen der Mitarbeiter für die Vernichtung von Schriftgut selbst zuständig ist?

2. Ist der Mitarbeiter verpflichtet, die Schriftstücke bis zu deren Vernichtung zu sichern?

3. Ist vorgeschrieben, wie die Vernichtung zu erfolgen hat?

C. Zentrales Vernichten des Schriftguts durch die öffentliche Stelle

1. Wo wird das zentral zu vernichtende Schriftgut gesammelt?

2. Wie wird das zu vernichtende Schriftgut zu der Sammelstelle transportiert?

   2.1 Ist der Mitarbeiter selbst für den Transport zur Sammelstelle zuständig?

   - Ist die Sicherheit des zu vernichtenden Schriftguts bei dem Mitarbeiter bis zu dessen Ablieferung bei der Sammelstelle gewährleistet?

   2.2 Wird das Schriftgut durch einen zentralen Dienst eingesammelt?

   - Wie wird das Schriftgut beim Mitarbeiter bis zum Einsammeln durch den zentralen Dienst gesichert?
   - Erfolgt das Einsammeln in gesicherter Form durch Bedienstete der öffentlichen Stelle oder unter deren ständiger Aufsicht?

3. Wie ist das zu vernichtende Schriftgut bei der Sammelstelle gesichert?

4. Ist der Ablauf der Vernichtung des gesammelten Schriftguts schriftlich geregelt?

D. Vernichtung des Schriftguts im Auftrag durch einen Dritten

1. Regelungen, soweit das DSG MV anwendbar ist

   1.1 Kann der Auftragnehmer die nach § 17 DSG MV notwendigen technischen und organisatorischen Maßnahmen gewährleisten (§ 4 Abs. 1 Satz 3 DSG MV)?

   1.2 Gibt es einen schriftlichen Vertrag, der Art und Umfang des Umgangs mit personenbezogenen Daten und ergänzende Weisungen sowie Regelungen zu etwaigen Unterauftragsverhältnissen beinhaltet (§ 4 Abs. 1 Satz 4 DSG MV)?

   - Wurde ausgeschlossen, daß die Vernichtung durch den Auftragnehmer als Unterauftrag einem anderen Auftragnehmer übertragen wird?

1.3 Finden auf den Auftragnehmer die Vorschriften des Datenschutzgesetzes Mecklenburg-Vorpommern Anwendung:
Wenn nein:

- Wie wurde sichergestellt, daß der Auftragnehmer die Bestimmungen des Datenschutzgesetzes Mecklenburg-Vorpommem befolgt und sich, sofern die Datenverarbeitung im Geltungsbereich dieses Gesetzes durchgeführt wird, der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft (§ 4 Abs. 3 Satz 1 DSG MV).

2. Regelungen, soweit das BDSG anwendbar ist

2.1 Wurde der Auftragnehmer unter besonderer Berücksichtigung der erforderlichen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt (§ 11 Abs. 2 Satz 1 BDSG)?

2.2 Wurde der Auftrag schriftlich erteilt, und wurden dabei die Durchführung der Schriftgutvenichtung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festgelegt (§ 11 Abs. 2 Satz 2 BDSG)?

- Wurde ausgeschlossen, daß die Vernichtung durch den Auftragnehmer als Unterauftrag einem anderen Auftragnehmer übertragen wird?

2.3 Ist der Auftragnehmer eine öffentliche Stelle?
Wenn nein:

- Sind die bei dem Vernichten des Schriftguts beschäftigten Personen bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnissesverpflichtet worden (§ 5 Satz 2 BDSG)?

3. Regelungen, soweit das Sozialgesetzbuch (SGB) anwendbar ist

3.1 Wurde der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt (§ 80 Abs. 1 SGB X i.V.m. § 11 Abs. 2 Satz 1 BDSG)?

3.2 Genügt der Datenschutz beim Auftragnehmer den Anforderungen, die für den Auftraggeber gelten (§ 80 Abs. 2 Satz 1 SGB X)?

3.3 Wurden Weisungen zur Ergänzung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen (§ 9 BDSG) erteilt (§ 80 Abs. 2 Satz 2 SGB X)?

3.4 Sind die erforderlichen Anzeigen bei den Aufsichtsbehörden erfolgt (§ 80 Abs. 3 SGB X)?

3.5 Ist der Auftragnehmer eine nicht-öffentliche Stelle?
Wenn ja:

- Die Verarbeitung personenbezogener Daten im Auftrag durch nicht-öffentliche Stellen ist nur zulässig, wenn anders Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger besorgt werden können (§ 80 Abs. 5 SGB X). Ist diese Voraussetzung erfüllt?

- Hat sich der Auftragnehmer schriftlich damit einverstanden erklärt, daß der Auftraggeber jederzeit berechtigt ist, mit den in § 38 Abs. 3 und 4 BDSG genannten Mitteln die Einhaltung der Vorschriften über den Datenschutz und der ergänzenden Weisungen zu überwachen (§ 80 Abs. 2 Satz 3 SGB X)?

4. Wurde schriftlich vereinbart, in welchem Zustand sich das Schriftgut zu befinden hat, um als vernichtet gelten zu können (Abschluß der Vernichtung)?

5. Ist gewährleistet, daß der Auftraggeber über sein Schriftgut bis zum Abschluß der Vernichtung uneingeschränkt verfügen kann?

   5.1 Bleibt das Schriftgut bis zum Abschluß der Vernichtung Eigentum des Auftraggebers?

   5.2 Ist gewährleistet, daß das Schriftgut vor seiner Vernichtung nicht mit fremdem Schriftgut vermischt wird?

6. Wurde eine schriftliche Vereinbarung über den Ort getroffen, an dem vernichtet wird?

7. Gibt es eine Vereinbarung über Handhabung und Sicherung des Schriftguts zwischen der Übergabe und dem Abschluß der Vernichtung?

   7.1 Wurden Regelungen für den Transport getroffen?

   7.2 Wurde eine eventuell erforderliche Zwischenlagerung geregelt?

8. Gibt es eine schriftliche Vereinbarung über den zulässigen Zeitraum zwischen der Übergabe des Schriftguts und dem Abschluß der Vernichtung?

   8.1 Hat die Vernichtung unverzüglich zu erfolgen?

   8.2 Hat die Vernichtung am gleichen Tage zu erfolgen?

9. Wurde mit dem Auftragnehmer vereinbart, daß der Auftraggeber bis zum Abschluß der Vernichtung zu Kontrollen berechtigt ist?

10. Ist gewährleistet, daß andere Auftraggeber keine Kenntnis der in dem Schriftgut gespeicherten Daten erhalten können ?
    Kann die Vertraulichkeit durch Kontroll- oder Eigentumsrechte anderer Auftraggeber, die sich auf dessen zu venichtendes Schriftgut beziehen, beeinträchtigt werden?

11. Gibt es schriftliche Bestätigungen über die Durchführung jeder Vernichtungsaktion?

    11.1 Erhält der Auftraggeber eine Quittung bei der Übergabe von Schriftgut an den Auftragnehmer?

    11.2 Erhält der Auftraggeber eine schriftliche Bestätigung des Auftragnehmers nach der ordnungsgemäßen Vernichtung des Schriftguts?

Abkürzungsverzeichnis

AFIS	automatisches Fingerabdruckidentifizierungssystem
AK	Arbeitskreis
AO	Abgabenordnung
AOÄG	Gesetz zur Änderung der Abgabenordnung
AOK	AllgemeineOrtskrankenkasse
ARD	Arbeitsgemeinschaftder Rundfunkanstalten Deutschlands
AROV	Amt zur Regelung offener Vermögensfragen
ASRG	Arbeitsschutzrahmengesetz
BBG	Bundesbeamtengesetz
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Datenschutz
BGBl.	Bundesgesetzblatt
BKA	Bundeskriminalamt
BKK	Betriebskrankenkasse
BMF	Bundesministeriumfür Finanzen
BMG	Bundesministeriumfür Gesundheit
BMI	Bundesministeriumdes Innern
BMJ	Bundesministeriumfür Justiz
BML	Bundesministeriumfür Landwirtschaft
BNotO	Bundesnotarordnung
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BR-Drs.	Bundesrats-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik

BStatG	Bundesstatistikgesetz
BtG	Betreuungsgesetz
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlungdes Bundesverfassungsgerichts
DBP Telekom	Deutsche Bundespost Telekom
DSG	Datenschutzgesetze der Länder
DSG MV	Gesetz zum Schutz des Bürgers beim Umgang mit seinen Daten (Landesdatenschutzgesetz von Mecklenburg-Vorpommern)
DV	Datenverarbeitung
DVAG	Deutsche Vermögensberatungs AG
DVZ	Datenverarbeitungszentrum
EDV	elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz
GMBl.	gemeinsames Ministerialblatt
GoV	Gesellschaftzur Klärung offener Vermögensfragen mbH
GVG	Gerichtsverfassungsgesetz
HEG MV	Hochschulerneuerungsgesetz Mecklenburg-Vorpommern
HFSt	Hauptfürsorgestelle
IM	inoffizieller Mitarbeiter (der Stasi)
IMA-IT	Interministerieller Ausschuß für Informations- und Telekommunikationstechnik
INPOL	Informationssystem der Polizei
InVeKoS	Integriertes Verwaltungs- und Kontrollsystem

IT	Informations- und Telekommunikationstechnik
ITSR	Informations- und TelekommunikationstechnikStrukturrahmen
JWG	Jugendwohlfahrtsgesetz
KA	Kriminalakten-Richtlinie
KAN	Kriminalaktennachweis
KBA	Kraftfahrt-Bundesamt
Kfz	Kraftfahrzeug
KJHG	Kinder- und Jugendhilfegesetz
KPI	Kriminalpolizeiinspektion
KpS	Kriminalpolizeilichepersonenbezogene Sammlungen
KV	Kassenärztliche Vereinigung
LAROV	Landesamt zur Regelung offener Vermögensfragen
LBA MV	Landesbesoldungsamt Mecklenburg-Vorpommern
LfD	Landesbeauftragter für den Datenschutz
LKA	Landeskriminalamt
LKA MV	LandeskriminalamtMecklenburg-Vorpommern
LKHG	Landeskrankenhausgesetz
LMG MV	Meldegesetz für das Land Mecklenburg-Vorpommern (Landesmeldegesetz)
LVA MV	Landesversicherungsanstalt Mecklenburg-Vorpommern
LVerfSchG	Landesverfassungsschutzgesetz
LWL	Lichtwellenleiter
MeldDÜV MV	Meldedatenübermittlungsverordnung Mecklenburg-Vorpommern
MfS/AfNS	Ministeriumfür Staatssicherheit / Amt für Nationale Sicherheit
MPU	medizinisch-psychologischeUntersuchungsstelle

MRRG	Melderechtsrahmengesetz
NDR	Norddeutscher Rundfunk
NJW	Neue Juristische Wochenschrift
OFD	Oberfinanzdirektion
OrgKG	Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformender Organisierten Kriminalität
OVG	Oberverwaltungsgericht
OWI	Ordnungswidrigkeit
PC	Personalcomputer
PDV	Polizeidienstvorschrift
PIOS	Personen, Institutionen, Objekte, Sachen
PKZ	Personenkennzahl
PsychKG	Gesetz über Hilfen und Schutzmaßnahmen für psychisch Kranke
RegVBG	Registerverfahrenbeschleunigungsgesetz
SGB nr.	Sozialgesetzbuch, Teil
SiR MV	Richtlinien für die Sicherheitsüberprüfung von Personen im Rahmen des Geheimschutzes (Sicherheitsrichtlinien)
SOG MV	Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg - Vorpommern (Sicherheits- und Ordnungsgesetz)
SPUDOK	Spurendokumentation
Stasi	Staatssicherheitsdienst der ehemaligen DDR
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StUG	Stasi-Unterlagen-Gesetz
StVÄG	Strafverfahrenänderungsgesetz

StVZO	Straßen-Verkehrs-Zulassungsordnung
SÜG	Sicherheitsüberprüfungsgesetz
SWV	Schweriner Wohnungsverwaltung
TDSV	Telekom-Datenschutzverordnung
UDSV	Teledienstunternehmen-Datenschutzverordnung
UIG	Umweltinformationsgesetz
VermG	Vermögensgesetz
ZAST	Zentrale Aufnahmestellefür Asylbewerber
ZER	Zentrales Einwohnermelderegister
ZEVIS	Zentrales Verkehrsinformationssystem
ZPO	Zivilprozeßordnung

Stichwortverzeichnis

Publikationen

Beim Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern sind derzeit folgende Publikationen erhältlich:

Gesetz zum Schutz des Bürgers Beim Umgang mit seinen Daten
(Landesdatenschutzgesetz von Mecklenburg-Vorpommern - DSG MV -)

Bundesdatenschutzgesetz - BDSG -
(Text und Erläuterungen)

Informationsblätter

- Der Landesbeauftragte für den Datenschutz
- Datenschutz geht jeden an
- Großer Lauschangriff
- Datenschutz und Personalcomputer
- Chipkarte
- Patientenakten
- Datenschutz und Verfassungsschutz
- Datenschutz und Personen-Identifikation
- Adreßbücher
- Datenmißbrauch
- Schutz persönlicher Daten
- Datenschutz und Telefax

- Hinweise zu den Aufgaben eines internen Datenschutzbeauftragten öffentlicher Stellen

- Forderungen an Wartung und Fernwartung von DV-Anlagen

- Organisationshilfe zur Vernichtung von Schriftgut

- Hinweise zur Führung von Dateibeschreibung und Geräteverzeichnis

Handbuch des Landtages mit DSG MV