LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 2/1245**
2. Wahlperiode **09.02.96**

UNTERRICHTUNG

durch den Landesbeauftragten für den Datenschutz

Zweiter 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 02. Februar 1996 gemäß § 29 Abs. 1 des Landesdatenschutzgesetzes

VORWORT

Das Datenschutzgesetz von Mecklenburg-Vorpommern sieht vor, daß der Landesbeauftragte für den Datenschutz für jeweils zwei Kalenderjahre einen Tätigkeitsbericht vorlegt. Der Zweite Tätigkeitsbericht umfaßt den Zeitraum vom 1. Januar 1994 bis zum 31. Dezember 1995. Wie bereits in meinem ersten Bericht habe ich Vorgänge ausgewählt, die mir geeignet erscheinen, einen Gesamteindruck von der Tätigkeit meiner Behörde zu vermitteln.

Einige Beiträge schließen an Sachverhalte an, die ich im Ersten Tätigkeitsbericht dargestellt hatte. Insofern könnte es für den Interessierten nützlich sein, in dem einen oder anderen konkreten Fall vielleicht noch einmal auf diesen Bericht zurückzugreifen. Dort bin ich unter anderem auf die rechtlichen Grundlagen und die Herausbildung des Datenschutzes in Mecklenburg-Vorpommern eingegangen.

Danken möchte ich dem Bundesbeauftragten für den Datenschutz und meinen Kollegen in den anderen Bundesländern für die fachliche Unterstützung sowie die angenehme Zusammenarbeit. Ein weiterer Dank gilt meinen Mitarbeitern für ihre engagierte, zuverlässige und sachkundige Arbeit im Berichtszeitraum sowie bei der Gestaltung der einzelnen Beiträge dieses Berichtes.

Dr. Werner Kessel
Landesbeauftragter für den Datenschutz
Mecklenburg-Vorpommern

INHALTSVERZEICHNIS

Seite

1. Einleitung

Im allgemeinen neigt der moderne Mensch nicht dazu, jedermann alles über sich mitzuteilen. Wir führen vertrauliche Gespräche und versenden Briefe mit persönlichem Inhalt in geschlossenen Umschlägen. Dieses Verhalten ist Ausdruck eines elementaren Bedürfnisses des zivilisierten Menschen - des Bedürfnisses nach dem Schutz seiner Privatsphäre.

Grundlegende Rechte werden üblicherweise in der Verfassung eines modernen Staates berücksichtigt. Insofern erscheint es unverständlich, weshalb sich der Bundesbürger immer noch auf das Volkszählungsurteil von 1983 berufen muß, wenn er vom Staat geeignete Maßnahmen zur Wahrung des Grundrechts auf Schutz der personenbezogenen Daten einfordern will.

Leider hat es der Bundestag bei der Novellierung des Grundgesetzes im Oktober 1994 versäumt, dieses Recht durch Aufnahme in das Grundgesetz in eine allgemein verständliche Form zu bringen. Statt dessen beläßt er es bei der für die meisten Bürger wenig transparenten Ausdrucksform als Urteilsspruch mit Grundrechtscharakter. Freilich kommt der Fachmann auch mit der derzeitigen Situation ganz gut zurecht. Um den geht es hier aber nicht. Es wäre nicht nur eine nette Geste des Staates gegenüber dem Bürger, wenn er es ihm ersparen würde, sich seine Grundrechte aus verschiedenen Quellen zusammenzutragen. Auch die öffentlichen und nicht-öffentlichen Stellen würde die Einfügung des Grundrechts auf Datenschutz in das Grundgesetz unmißverständlich daran erinnern, daß es zunächst Sache des Betroffenen ist, über die Verwendung seiner personenbezogenen Daten selbst zu entscheiden. Es wäre sehr zu wünschen, daß bei den nächsten Diskussionen um Aufnahme dieses Rechts in das Grundgesetz der Bürger nicht wieder aus dem Blickfeld gerät.

Unserem Landesgesetzgeber ist das nicht passiert. In Mecklenburg-Vorpommern ist der Datenschutz in Art. 6 der Landesverfassung festgeschrieben. Das heißt jedoch nicht, daß es deswegen im Lande keine Sorgen bei der Umsetzung dieses Rechts gibt.

Immer noch kommt es vor, daß öffentliche Stellen die alte DDR-Personenkennzahl (PKZ) verlangen oder sie sich mit Einverständnis des Betroffenen beschaffen wollen, obwohl sie längst nicht mehr verwendet werden darf. In Fragebögen wird oft überflüssigerweise und undifferenziert nach einfachen Mitgliedschaften bzw. untergeordneten ehrenamtlichen Funktionen in Massenorganisationen und Vereinen der ehemaligen DDR gefragt. Vollständige Kopien ganzer Seiten aus Sozialversicherungsausweisen mit Angaben über Kuraufenthalte, Krankschreibungen sowie Verdienst- und Beitragsangaben werden zu unterschiedlichen Zwecken verlangt und zu den Akten genommen. Und in den bereits zu DDR-Zeiten angelegten Kriminalakten sind immer noch Daten gespeichert, die dort nach geltendem Recht schon längst nichts mehr zu suchen haben.

Als ich im Herbst 1992 das erste Mal an einer Sitzung des Arbeitskreises "Datenschutz in den neuen Bundesländern" teilnahm, hatte ich gehofft, daß sich ein solcher Arbeitskreis im Datenschutz nicht manifestieren möge. Immerhin konnte die kontinuierliche Tätigkeit des Arbeitskreises mit der letzten planmäßigen Sitzung am 17. Oktober 1995 in Berlin beendet werden. Ich sehe hierin einen wichtigen Schritt zur Normalisierung des Datenschutzes in den neuen Bundesländern.

Neue, den Datenschutz betreffende Entwicklungen gibt es nicht nur im Land, sondern auch auf Bundes- und Europaebene. So enthalten zahlreiche neue Gesetze des Bundes Vorschriften, die auch den Datenschutz in Mecklenburg-Vorpommern betreffen. In diesem Berichtszeitraum waren das beispielsweise das Pflegeversicherungsgesetz, das Verbrechensbekämpfungsgesetz und das Umweltinformationsgesetz. Einige Bundesgesetze werden Anpassungen in den Ländern nach sich ziehen, etwa das geänderte Melderechtsrahmengesetz.

Die seit Jahren andauernde Diskussion über eine Datenschutzrichtlinie der Europäischen Union (EU) hat im Berichtszeitraum ihren Abschluß gefunden. Am 24.Juli 1995 hat der Rat der Europäischen Union die "Richtlinie des Europäischen Parlamentes und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten" verabschiedet. Dadurch wird der unterschiedliche Stand des Datenschutzes in den einzelnen EU-Staaten auf ein einheitliches Niveau gebracht. Die Mitglieder werden verpflichtet, ihre Datenschutzgesetze anzupassen bzw. entsprechende Gesetze zu erlassen. Für den Datenschutz relevant waren aber auch andere Aktivitäten innerhalb der EU, wie das Inkraftsetzen des Schengener Durchführungsübereinkommens, die auf den Weg gebrachte ISDN-Richtlinie oder auch die Rechtsprechung des Europäischen Gerichtshofes (EuGH).

Ebenfalls im Wandel begriffen ist das Verhältnis der Datenschutzbeauftragten zur Informationstechnik (sofern ich hier und im weiteren von Datenschutzbeauftragten spreche, meine ich immer die der Länder und den Bundesdatenschutzbeauftragten). Während der erste Kontakt mit der elektronischen Datenverarbeitung von Skepsis bis hin zur Ablehnung geprägt war, normalisierte sich die Beziehung im Laufe der Zeit. Es folgte eine Phase der kritischen Begleitung. Heute wird der Einsatz moderner Technologien von Datenschutzbeauftragten immer häufiger empfohlen, und zwar immer dann, wenn er dem Schutz personenbezogener Daten dient. Dazu zählen unter anderem Maßnahmen zur Sicherheit von Personalcomputern und insbesondere Verschlüsselungstechniken.

Der 14. Dezember 1995 wird wohl als schwarzer Tag für den Datenschutz in der Bundesrepublik Deutschland in die Geschichte eingehen. Nachdem sich CDU und SPD schon längst prinzipiell für den Großen Lauschangriff ausgesprochen hatten, hat sich nun auch die überwiegende Mehrheit der F.D.P.-Mitglieder dafür entschieden, daß private Wohnungen zum Zwecke der Strafverfolgung mit technischen Mitteln ausgeforscht werden dürfen. Es ist nun damit zu rechnen, daß in nächster Zeit das Grundrecht auf Unverletzlichkeit des privaten Wohnbereiches durch bundesgesetzliche Regelungen eine starke Einschränkung erfährt.

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

2.1. EU-Datenschutzrichtlinie

Am 24. Juli 1995 hat der Rat der Europäischen Union die "Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten" (EU-Datenschutzrichtlinie) bei Stimmenthaltung des Vereinigten Königreiches angenommen. Damit hat eine mehrjährige, intensive Diskussion in europäischen und nationalen Gremien einen positiven Abschluß gefunden. Die Verabschiedung der EU-Datenschutzrichtlinie stellt einen entscheidenden Schritt auf dem Weg eines einheitlichen Datenschutzniveaus sowohl innerhalb der EU-Mitgliedstaaten als auch im Datentransfer zwischen der EU und Drittstaaten dar.

Adressaten der Richtlinie sind nicht die einzelnen Bürger, sondern die Mitgliedsländer. Sie ist nicht unmittelbar geltendes Recht und bedarf daher der Umsetzung in nationales Recht der EU-Staaten. Diese haben drei Jahre Zeit, um die für die Umsetzung erforderlichen Rechts- und Verwaltungsvorschriften zu erlassen. Der dafür notwendige Aufwand ist in den einzelnen Mitgliedstaaten recht unterschiedlich. Er reicht von der Schaffung neuer Gesetze in Griechenland und Italien - dort gibt es bisher keine Datenschutzgesetze - bis hin zur bloßen Änderung und Ergänzung einzelner Teilbereiche, zum Beispiel in Deutschland, wo bereits eine gut ausgearbeitete gesetzliche Grundlage für den Datenschutz existiert.

In einer Arbeitskreis-Sitzung der Datenschutzbeauftragten wurde der damalige Entwurf der EU-Datenschutzrichtlinie in der Fassung des Gemeinsamen Standpunktes des Rates diskutiert. Dabei wurde festgestellt, daß neben dem Bundes- auch die Landesgesetzgeber gefordert sind. Das genaue Ausmaß der fälligen Rechtsänderungen und -ergänzungen ist noch nicht völlig abzusehen. Änderungsbedarf wird es vor allem bei folgenden Punkten geben:

- Der Umgang mit besonders sensiblen Daten - etwa solchen, aus denen die ethnische Herkunft, politische Meinungen oder religiöse Überzeugungen hervorgehen - erfordert eine eigene Regelung.

- Das Verbot automatisierter Persönlichkeitsbewertung muß berücksichtigt werden.

- Das Widerspruchsrecht des Betroffenen gegen den Umgang mit seinen Daten ist zumindest im nicht-öffentlichen Bereich zu erweitern.
- Die Beschränkung, im nicht-öffentlichen Bereich nur dann Kontrollen durchführen zu können, wenn hinreichende Anhaltspunkte für die Verletzung datenschutzrechtlicher Vorschriften vorliegen, wird aufgehoben werden müssen.

- Die Richtlinie verlangt eine weitgehende Angleichung der Datenschutzanforderungen im öffentlichen und privaten Bereich. Nicht ausdrücklich gefordert, aber sinnvoll wäre es daher, die Aufsichts- und Kontrollstellen der beiden Bereiche zusammenzulegen.

Die Datenschutzbeauftragten sind zur Zeit um eine Anpassung des Bundesdatenschutzgesetzes an die EU-Datenschutzrichtlinie bemüht. Im Rahmen der anstehenden Novellierung des Landesdatenschutzgesetzes (siehe Abschnitt 4) werde ich mit dem federführenden Innenministerium M-V den sich aus der Richtlinie ergebenden Umsetzungsbedarf erörtern.

2.2. Rechtswesen

2.2.1. Verbrechensbekämpfungsgesetz

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

Bis zuletzt waren die hiermit zusammenhängenden Änderungen in insgesamt 16 Gesetzen datenschutzrechtlich umstritten. Dies galt insbesondere für die des Gesetzes zu Art. 10 Grundgesetz (G 10). Danach werden dem Bundesnachrichtendienst (BND) neuartige Befugnisse bei der Fernmeldeaufklärung zugewiesen. Bisher beschränkte sich der BND auf die Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung waren. Nunmehr soll der BND schwerpunktmäßig auch auf dem Gebiet der inneren Sicherheit tätig werden. Zwar hat die Bundesregierung bei den Gesetzesberatungen immer wieder darauf hingewiesen, daß es bei zusätzlichen Gefahrenbereichen wie

- unerlaubtem Außenwirtschaftsverkehr mit Waren, Datenverarbeitungsprogrammen und besonderen geschützten Technologien,

- unbefugtem Drogenhandel,

- Geldfälschungen im Ausland,

- Geldwäsche im Zusammenhang mit Kriegswaffenhandel, Verstößen gegen das Außenwirtschaftsgesetz sowie Drogenhandel und Geldfälschungen

nur um die äußere Sicherheit geht, aber bei bestimmten schweren Delikten dürfen die auf diese Weise erlangten personenbezogenen Daten ohne nennenswerte Einschränkungen an die Strafverfolgungsbehörden weitergegeben werden. Darin sehe ich einen Verstoß gegen das rechtsstaatlich verankerte Trennungsgebot zwischen BND und Polizei.

Die Datenschutzbeauftragten kritisierten weiterhin, daß sich die Fernmeldeaufklärung gerade nicht auf bestimmte Personengruppen beschränken läßt. So schafft das Gesetz die Möglichkeit, wie bei einer "Rasterfahndung" eine unvermeidlich große Anzahl Nichtbeteiligter in Abhörmaßnahmen einzubeziehen.

Zwischenzeitlich hat das Bundesverfassungsgericht jedoch auf eine Verfassungsbeschwerde hin eine einstweilige Anordnung erlassen, nach der die im Verbrechensbekämpfungsgesetz geschaffene Befugnis des BND, Erkenntnisse aus der Fernmeldeüberwachung ohne zureichenden Tatverdacht auszuwerten und weiterzugeben, vorläufig aufgehoben wurde.

Es bleibt abzuwarten, wie das Gericht im Hauptsacheverfahren entscheiden wird.

2.2.2. Strafverfahrensänderungsgesetz

Die Landesregierungen von Bayern, Hessen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland und Thüringen haben den Entwurf eines Strafverfahrensänderungsgesetzes 1994 (StVÄG 1994) in den Bundesrat eingebracht.

In einer gemeinsamen Presseerklärung (siehe Anlage 27) kritisierten die Datenschutzbeauftragten des Bundes und von 13 Ländern diesen Entwurf als unverhältnismäßige Ermächtigung für Eingriffe in das Persönlichkeitsrecht. Der Gesetzentwurf steht im Widerspruch zu den aus dem Volkszählungsurteil resultierenden Anforderungen und fällt weit hinter den Standard der allgemeinen Datenschutzgesetze und der Polizeigesetze der Länder zurück. Es sind kaum datenschutzrechtliche Neuerungen gegenüber den Vorentwürfen enthalten.

Bereits zuvor hatte ich gegenüber dem Justizminister unseres Landes auf den Regelungsbedarf und die datenschutzrechtlichen Erfordernisse in diesem Bereich hingewiesen. Nach wie vor fehlen die notwendigen bereichsspezifischen Datenschutzvorschriften. Auf diese unhaltbare Situation haben die Datenschutzbeauftragten mehrfach aufmerksam gemacht und Hinweise, zuletzt in den Entschließungen der vergangenen Konferenzen der Datenschutzbeauftragten (DSB-Konferenz), gegeben:

- "Informationsverarbeitung im Strafverfahren" (siehe Anlage 2)
- "Fehlende bereichsspezifische gesetzliche Regelungen bei der Justiz" (siehe Anlage 9)
- "Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich" (siehe Anlage 20)
- "Forderungen an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien (außerhalb der Öffentlichkeitsfahndung der Ermittlungsbehörden)" (siehe Anlage 23).

Der Entwurf des StVÄG 1994 wurde trotz der Bedenken der Datenschutzbeauftragten vom Bundesrat beschlossen und der Bundesregierung zur Stellungnahme zugeleitet. Die Bundesregierung hat hierzu ausgeführt, daß die zu schaffenden Regelungen in jeder Beziehung verfassungsrechtlichen und datenschutzrechtlichen Anforderungen genügen müssen. Von einer detaillierten Stellungnahme hat sie jedoch Abstand genommen, da die Vorlage eines eigenen Entwurfes beabsichtigt ist.

Es bleibt abzuwarten, inwieweit in diesem Gesetzentwurf die datenschutzrechtlichen Erfordernisse berücksichtigt sein werden.

2.2.3. Ermittlung von Wahlrechtsausschlüssen

Zur Vorbereitung der Wahlen im Jahr 1994 hatten sich die Datenschutzbeauftragten des Bundes und der neuen Länder unter anderem mit der Novellierung des Bundeszentralregistergesetzes (BZRG) zu befassen.

Im Vorfeld von allgemeinen Wahlen und Abstimmungen muß bekannt sein, welche Personen nicht wählen dürfen (Ausschluß vom aktiven Wahlrecht) bzw. nicht wählbar sind (Ausschluß vom passiven Wahlrecht). Zu diesem Zweck speichern die Meldebehörden entsprechende Daten, die zum Ausschluß einzelner Personen von der Wahl führen. In den Melderegistern der Gemeinden der neuen Länder waren diese Ausschlüsse jedoch nicht oder nur teilweise vermerkt. Es bestand somit die Gefahr von Wahlanfechtungen und gegebenenfalls Wahlwiederholungen. Mit Hilfe der im Bundeszentralregister eingetragenen Vorstrafen sollte deshalb eine Aktualisierung der Melderegister vorgenommen werden. Hierfür fehlte allerdings die erforderliche gesetzliche Grundlage.

Im Entwurf eines Dritten Gesetzes zur Änderung des Bundeszentralregistergesetzes (Bundestags-Drucksache 12/6380) war deshalb zunächst eine Regelung vorgesehen, wonach den Innenministerien über alle Personen, die in den neuen Bundesländern aufgrund ihres Alters am 1. Januar 1994 wahlberechtigt sind oder bis zum 31. Dezember 1994 die Wahlberechtigung erlangen, ein Führungszeugnis für Behörden ausgestellt werden sollte. In einem solchen Führungszeugnis wird mitgeteilt, welche Strafvermerke zur betreffenden Person im Bundeszentralregister eingetragen sind. Die Datenübermittlung sollte unabhängig davon erfolgen, ob die Eintragung im Führungszeugnis für den Ausschluß vom Wahlrecht von Bedeutung ist oder nicht. Sofern das Register über eine Person keine Eintragung enthält, sollte die Registerbehörde nur dieses mitteilen. Im Führungszeugnis enthaltene Eintragungen, die für den Ausschluß vom Wahlrecht von Belang sind, sollte dann das Innenministerium an die zuständige Meldebehörde mitteilen. Den Innenministerien wäre somit eine Art "Filterfunktion" zugekommen.

Ich habe gegenüber dem Innenminister unseres Landes meine Bedenken gegen dieses Verfahren geltend gemacht, weil die vorgesehene Regelung, sämtliche Führungszeugnisse aller volljährigen Personen an die Innenministerien zu übermitteln, gegen das verfassungsrechtliche Gebot der Verhältnismäßigkeit verstößt. Es wäre nach dieser Regelung zu einer kompletten Datenübermittlung vom Bundeszentralregister an die Innenressorts der Länder gekommen, in deren Folge Informationen über jeden straffällig gewordenen Bürger des Landes vorgelegen hätten. Da nur wenige, ganz bestimmte Eintragungen tatsächlich zu einem Ausschluß vom Wahlrecht führen, wäre eine Übermittlung des gesamten Datenbestandes allein aus diesem Grund als unverhältnismäßig zu erachten. Die in einem anderen Bundesland vorab erfolgte Datenübermittlung hatte gezeigt, daß lediglich bei ca. 0,025 % der Wahlberechtigten Wahlausschlußgründe festgestellt wurden und dies insoweit keinen signifikanten Einfluß auf das Wahlergebnis hat.

Ich habe mich daher gegen eine Übermittlung aller Führungszeugnisse aus dem Bundeszentralregister ausgesprochen und statt dessen empfohlen, die Auswertung, ob ein Wahlrechtsausschluß vorliegt oder nicht, im Bundeszentralregister selbst vornehmen zu lassen. Ferner sollten von den Kandidaten, die sich zur Wahl aufstellen lassen wollen, selbst Führungszeugnisse beigebracht werden, um sich gegen spätere Wahlanfechtungen abzusichern.

Der Innenminister unseres Landes hat meine Bedenken geteilt.

Im Laufe des Gesetzgebungsverfahrens wurde die Vorschrift geändert. Danach erhalten die Meldebehörden aus dem Bundeszentralregister unmittelbar und ohne Zwischenschaltung des Innenministeriums nur Auskunft über solche Eintragungen, aus denen sich ein Ausschluß der betroffenen Person vom aktiven Wahlrecht ergibt. Der Verlust des passiven Wahlrechts wird den Meldebehörden auf Antrag über die Innenministerien mitgeteilt, die die Führungszeugnisse der Wahlbewerber auswerten, da dieses im Bundeszentralregister technisch nicht möglich ist. Die Übermittlung von Daten wurde somit auf das tatsächlich erforderliche Maß reduziert. Den datenschutzrechtlichen Anforderungen wurde mit dieser Regelung Rechnung getragen.

2.2.4. Antragsformulare zum Rehabilitierungsgesetz nicht genau genug

Im Januar 1995 hatte das Bundesministerium der Justiz (BMJ) in Abstimmung mit den zuständigen Verwaltungen in den neuen Ländern sowie dem Bundesbeauftragten für den Datenschutz neue Antragsformulare nach dem Strafrechtlichen, Beruflichen und Verwaltungsrechtlichen Rehabilitierungsgesetz vorgelegt.

Ich habe diese Formulare mit denen vom Amt für Rehabilitierung und Wiedergutmachung verglichen und folgende Abweichungen festgestellt: Im Antragsteil "Allgemeine Angaben" wird unter Ziffer 3 nach detaillierten Angaben über die Arbeitsstellen in der ehemaligen DDR gefragt. Zum Beweis der Richtigkeit dieser Angaben soll jeder Antragsteller eine beglaubigte Kopie seines Ausweises für Arbeit und Sozialversicherung beifügen. Es wird jedoch in Ziffer 2 darauf hingewiesen, daß die Fragen unter Ziffer 3 nicht zu beantworten sind, wenn der Antragsteller nur Kosten oder Geldstrafen geltend machen will. Dieser Hinweis bezieht sich jedoch lediglich auf einen Teil der nach dem Strafrechtlichen Rehabilitierungsgesetz (StrRehaG) möglichen Antragstellungen. Andererseits sind die Angaben über Arbeitsstätten gemäß § 21 Ziff. 2 Berufliches Rehabilitierungsgesetz (BerRehaG) nur im Bereich der beruflichen Rehabilitierung erforderlich. Bei Anträgen nach § 10 2. SED-Unrechtsbereinigungsgesetz (SED-UnBerG) und § 7 StrRehaG sind diese Angaben nicht vorgesehen und werden auch für die Bescheidung der Anträge nicht benötigt. Es wurden daher mit dem Musterformular "Allgemeine Angaben" Daten erhoben, die nur für einen Teil der zu bescheidenden Angaben notwendig waren, ohne daß der Antragsteller hierüber aufgeklärt wird. Insofern verstoßen die Fragen unter Ziffer 3 offensichtlich gegen den Grundsatz der Erforderlichkeit der Datenerhebung.

Ich habe dem Amt für Rehabilitierung und Wiedergutmachung empfohlen, die Antragsformulare entsprechend zu ändern und die nur in bestimmten Bereichen benötigten Daten über die Arbeitsstellen in der DDR ausschließlich in den dafür vorgesehenen Anlagen zu erfassen.

Des weiteren habe ich festgestellt, daß bei Fragen nach der politischen Vergangenheit der Antragsteller unter Ziffer 4a und 5b ein Hinweis mit dem Wortlaut eingefügt worden ist: "Die folgenden Angaben zu den die Ausschließungsgründe betreffenden Fragen sind freiwillig. Sie dienen der Vereinfachung des Verfahrens bei der Rehabilitierungsbehörde. Ohne die Prüfung der Ausschließungsgründe kann die Rehabilitierungsbehörde keine Entscheidung treffen." Für den unbefangenen Leser des Fragebogens drängt sich aus der Formulierung dieses Hinweises der Eindruck auf, daß es sich bei den Fragen 1 bis 3 um allgemeine Angaben und nur bei den Fragen 4a ff. um Angaben über Ausschlußgründe handelt.

Nach längerem kontroversen Schriftwechsel wurde dem Grundantrag folgender wichtiger Hinweis zur Klarstellung vorangestellt: "Frage 3 muß in jedem Fall beantwortet werden, wenn sie eine berufliche Rehabilitierung beantragen. In den anderen Fällen ist die Beantwortung freiwillig und dient der Vereinfachung und Beschleunigung des Verfahrens bei der Rehabilitierungsbehörde. Die hier gemachten Angaben können in jedem Fall zur Überprüfung des Vorliegens von Ausschlußgründen verwendet werden."

Damit ist meines Erachtens ein tragfähiger Kompromiß erzielt worden.

2.2.5. Wie formuliert der Staatsanwalt den Einstellungsbescheid?

Eine Petentin teilte mir mit, daß sie Anzeige gegen Unbekannt wegen eines Einbruchs in ihre Gartenlaube erstattet hatte. In dem Einstellungsbescheid der Staatsanwaltschaft waren zu ihrer Verwunderung die Namen von zwei mutmaßlichen Tätern genannt, denen jedoch nichts nachgewiesen werden konnte. Sie wandte sich an mich, weil sie annahm, daß die Staatsanwaltschaft mit der Nennung der Namen gegen den Datenschutz verstoßen habe.

Nach Prüfung des Sachverhaltes stellte ich fest, daß das Verfahren datenschutzrechtlich nicht zu beanstanden war.

Derjenige, der durch eine Straftat verletzt wurde, hat das Recht, gegen die Einstellung des Verfahrens Beschwerde einzulegen und gegebenenfalls ein Klageerzwingungsverfahren durchzuführen. Im Rahmen des Erzwingungsverfahrens muß der Beschuldigte namentlich bezeichnet werden, da ansonsten der Antrag unzulässig ist. Deshalb mußte die Staatsanwaltschaft der Petentin die Namen der mutmaßlichen Täter mitteilen. Erst dadurch war es ihr möglich, die ihr zustehenden Rechte wahrzunehmen.

2.2.6. Spezielle Datenschutzvorschriften jetzt auch für Notare?

Schon im ersten Berichtszeitraum hatte sich gezeigt, daß zwischen der Notarkammer Mecklenburg-Vorpommern und meiner Behörde verschiedene Auffassungen darüber bestanden, ob die Vorschriften des Landesdatenschutzgesetzes auch für Notare gelten. Mittlerweile ist diese Frage geklärt. Es besteht Einvernehmen darüber, daß auch Notare öffentliche Stellen des Landes im Sinne von § 2 Abs. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG MV) sind und somit den Bestimmungen des Landesdatenschutzgesetzes unterliegen.

Gleichwohl halte ich es für erforderlich, für den Bereich der Notare bereichsspezifische Datenschutzvorschriften zu schaffen. Das BMJ hat den Justizressorts der Länder einen Vorentwurf zu einem Gesetzentwurf zur Änderung der Bundesnotarordnung und anderer Vorschriften zur Stellungnahme übersandt. Die darin enthaltenen datenschutzrechtlichen Regelungen sind weitgehend unbefriedigend. So fehlt beispielsweise in einer Vorschrift zur Datenübermittlung das Kriterium der Erforderlichkeit. Statt dessen wird darauf abgestellt, daß die Daten für die Maßnahme "von Bedeutung sein können". Sollen personenbezogene Daten übermittelt werden, so müssen diese für die konkrete Aufgabenerfüllung tatsächlich erforderlich sein.

Auch Notare verarbeiten personenbezogene Daten immer häufiger mit Hilfe automatisierter Verfahren. Deshalb sollte eine Erweiterung der Befugnisse der Aufsichtsbehörden auf die ordnungsgemäße automatisierte Datenverarbeitung bei den Notaren vorgenommen werden.

Das Justizministerium hat meine Anregungen in seine Stellungnahme gegenüber dem BMJ aufgenommen. Es bleibt abzuwarten, inwieweit in dem zu erwartenden Gesetzentwurf datenschutzrechtliche Bestimmungen für Notare enthalten sein werden.

2.2.7. Die unvergeßliche Personenkennzahl und der vergeßliche Ausschußvorsitzende

Im März 1995 lag mir der Entwurf eines Gesetzes zur Änderung des Abgeordnetengesetzes vor. Hierin wurden Verfahrensregelungen zur Einleitung der Überprüfung der Abgeordneten durch den Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR getroffen. Unter anderem war eine Regelung vorgesehen, wonach die Abgeordneten auch ihre Personenkennzahl (PKZ) angeben sollten.

Im Vorfeld der Beratungen habe ich im März 1995 gegenüber dem Rechtsausschuß zu dem Gesetzentwurf Stellung genommen. Datenschutzrechtliche Bedenken bestanden aus meiner Sicht gegen die vorgesehene Angabe der PKZ. Im Einigungsvertrag ist festgelegt, daß die bisher für das Meldewesen der ehemaligen DDR genutzten, vom Melderechtsrahmengesetz abweichenden Daten spätestens zum 31. Dezember 1992 zu löschen waren. Dies gilt auch für die PKZ als melderechtsfremdes Datum. Hiervon ausgenommen sind durch § 2 Abs. 2 Stasi-Unterlagen-Gesetz (StUG) lediglich die Gauck-Behörde sowie Gerichte und Strafverfolgungsbehörden, die die in Abs. 2 aufgeführten Daten aus dem Zentralen Einwohnerregister der ehemaligen DDR verwenden dürfen. Diese Regelung ist abschließend und beschränkt sich darauf, daß die PKZ aus einem vorhandenen Datenbestand heraus verwendet wird. In keinem anderen Bereich ist die öffentliche Verwaltung berechtigt, die PKZ weiter zu erheben, zu verarbeiten oder zu nutzen.

Kein Bürger der ehemaligen DDR ist mehr verpflichtet, seine PKZ zu wissen und sie an öffentliche oder nicht-öffentliche Stellen mitzuteilen. Ihre Angabe im Rahmen der Überprüfung durch die Gauck-Behörde ist freiwillig. Daher habe ich Bedenken geäußert, die Abfrage der PKZ in einem Gesetz zu regeln und empfohlen, die vorgesehene Sollvorschrift zu streichen. Darüber hinaus hatte ich angeboten, auch über weitere datenschutzrechtliche Aspekte im Zusammenhang mit der Überprüfung bei den anstehenden Besprechungen im Rechtsausschuß zu beraten.

Der Rechtsausschuß hat in seiner Sitzung am 1. Juni 1995 den Gesetzentwurf in unveränderter Fassung mit den Stimmen von SPD und CDU gebilligt. Auf meine Nachfrage hin hat mir der Ausschußvorsitzende mitgeteilt, daß er vergessen hatte, meine Stellungnahme an die Ausschußmitglieder weiterzuleiten und deshalb eine Erörterung meiner Empfehlung im Rechtsausschuß unterblieben war. In der 15. Landtagssitzung am 20. Juni 1995 fand im Rahmen der Zweiten Lesung und der Schlußabstimmung des Gesetzentwurfes eine nochmalige Aussprache statt. Auf Antrag des Vorsitzenden des Rechtsausschusses wurde die Soll-Vorschrift in eine Kann-Bestimmung geändert.

Ich halte diese Kann-Bestimmung im Gesetz für überflüssig. Für besonders glücklich halte ich sie vor allem auch deshalb nicht, weil ich den öffentlichen Stellen im Lande ständig erklären muß, daß sie die PKZ nicht mehr verwenden dürfen.

Für die Zukunft hoffe ich auf eine bessere Zusammenarbeit mit dem Ausschuß und habe das dem Landtagspräsidenten und dem Ausschußvorsitzenden so mitgeteilt.

2.3. Polizei

2.3.1. EUROPOL

In dem Vertrag über die Europäische Union vom 7. Februar 1992 haben die EU-Mitgliedstaaten die Schaffung eines Europäischen Polizeiamtes (EUROPOL) vereinbart. Ende 1993 bestimmten die Staats- und Regierungschefs der EU Den Haag als Sitz von EUROPOL. Anfang 1994 wurde dort im Rahmen der Aufbauphase die EUROPOL Drogeneinheit (EDE) eingerichtet. Sie soll die Arbeit von EUROPOL vor allem im Bereich der Rauschgiftkriminalität vorbereiten.

1993 wurde der erste Entwurf eines Übereinkommens der Mitgliedstaaten der Europäischen Union über die Errichtung eines Europäischen Polizeiamtes (EUROPOL-Konvention) vorgelegt. Mittlerweile ist die Konvention nach der Beratung im Europäischen Rat von Cannes am 26./27. Juni 1995 von den EU-Botschaftern in Brüssel am 26. Juli 1995 unterzeichnet worden. Die Ratifizierung wird sich voraussichtlich über mehrere Jahre erstrecken. Das Dokument Europol 54 vom 18. September 1995 enthält die maßgebliche Fassung des Übereinkommens.

Ziel von EUROPOL ist es, die Leistungsfähigkeit und die Zusammenarbeit der EU-Mitgliedstaaten bei der Verhütung und Bekämpfung der organisierten internationalen Kriminalität zu verbessern. Darunter fallen der Terrorismus, der illegale Drogenhandel, der illegale Handel mit nuklearen und radioaktiven Substanzen, die Schleuserkriminalität, der Menschenhandel, die Kraftfahrzeugkriminalität und die mit diesen Kriminalitätsformen verbundene Geldwäsche.

Die wichtigsten Aufgaben von EUROPOL sind:

- Erleichterung des Informationsaustauschs zwischen den Mitgliedstaaten,
- Sammlung, Zusammenstellung und Analyse von Informationen und Erkenntnissen,
- Unterrichtung der Mitgliedstaaten über die sie betreffenden Informationen,
- Unterhaltung von automatisierten Informationssammlungen,
- Unterstützung der Ermittlungen in den Mitgliedstaaten,
- Ausarbeitung von Gesamtberichten über den Stand der Arbeit.

Zur Erfüllung seiner Aufgaben werden EUROPOL unter anderem folgende Befugnisse eingeräumt:

- selbständig Daten in die Informationssammlungen einzugeben und sie zu nutzen,
- Daten, die von einem Mitgliedstaat übermittelt wurden, auch dann noch zu speichern, wenn sie in den nationalen Dateien bereits gelöscht sind,
- personenbezogene Daten von anderen Informationssystemen abzurufen, soweit EUROPOL in anderen Übereinkommen das generelle Recht zum Abruf aus diesen Systemen zugestanden wird,
- bestimmte personenbezogene Daten ohne Mitwirkung der Mitgliedstaaten an Staaten und Stellen außerhalb der EU zu übermitteln,
- über Auskunftsansprüche bzgl. bei EUROPOL gespeicherter Daten zu entscheiden,
- selbständig bei EUROPOL gespeicherte Daten zu berichtigen oder zu löschen, die von EUROPOL selbst eingegeben oder von Drittstaaten oder -stellen übermittelt wurden.

Gegen die bisherige und die noch vorgesehene Tätigkeit von EUROPOL bestehen unter anderem folgende datenschutz- und verfassungsrechtlichen Bedenken:

- Die EDE arbeitet bisher ohne ausreichende rechtliche Grundlage, da die EUROPOL-Konvention noch nicht in Kraft ist und das nationale Recht - zum Beispiel das Bundesdatenschutzgesetz - entweder nicht gilt oder keine passende Regelung vorsieht.
- Als internationale zwischenstaatliche Institution mit eigener Rechtspersönlichkeit unterliegt EUROPOL weder gerichtlicher noch parlamentarischer oder exekutiver Kontrolle der Mitgliedstaaten beziehungsweise der EU. Da auch der in Art. 28 des Übereinkommens vorgesehene Verwaltungsrat keinen Einfluß auf die konkrete Aufgabenerfüllung hat, ist es fraglich, ob EUROPOL insoweit ausreichend demokratisch legitimiert ist.
- EUROPOL ist weitgehend eigenständig bei der Entscheidung über die Löschung bzw. Nutzung der bei ihm gespeicherten Daten, die aus den Mitgliedstaaten stammen, in den dortigen Dateien mittlerweile aber gelöscht wurden, sowie über die Übermittlung von Daten an Stellen außerhalb der EU. Somit besteht die Gefahr, daß der durch nationales Recht gewährleistete Schutz personenbezogener Daten in diesem Bereich unterlaufen wird.
- Nach Art. 4 der Konvention hat jeder Mitgliedstaat eine nationale Stelle zu errichten oder zu bezeichnen, die die einzige Verbindungsstelle zwischen EUROPOL und den zuständigen Behörden des Mitgliedstaates ist. In der Bundesrepublik hat das Bundeskriminalamt (BKA) diese Funktion. Wegen der föderalen Struktur der Bundesrepublik Deutschland ergeben sich Probleme im Hinblick auf die verfassungsrechtliche Kompetenzverteilung für die Polizei. So ist zum Beispiel die Gefahrenabwehr grundsätzlich Sache der Bundesländer. Es muß gewährleistet werden, daß die materiell-rechtliche Kompetenz der Länder und die damit einhergehende Verantwortung für "ihre" Daten durch die formelle Bestimmung des BKA als nationale Stelle auch im Verhältnis zu EUROPOL nicht beschränkt wird.
- Viele Regelungen, insbesondere zur Datenübermittlung an Drittstaaten, sind ungenau und lassen verschiedene Auslegungen zu. Dies steht im Widerspruch zu dem aus dem Rechtsstaatsprinzip abgeleiteten Bestimmtheitsgrundsatz.

Die Datenschutzbeauftragten haben ihre Bedenken in verschiedenen nationalen und europäischen Gremien vorgebracht. Auf der 48. Sitzung ihrer Konferenz haben sie einen Beschluß zu den datenschutzrechtlichen Anforderungen an die EUROPOL-Konvention gefaßt (siehe Anlage 10). Am 15. November 1995 fand in Den Haag eine Sitzung der Arbeitsgruppe "Polizei" der Europäischen Datenschutzkonferenz zu EUROPOL statt. Dort erklärten die Vertreter mehrerer Mitgliedstaaten, daß die Konvention unter anderem in den Punkten Rechts- und Datenschutz vor der Ratifizierung deutlich nachgebessert werden muß.

2.3.2. INPOL-Neukonzeption - Das "Informationssystem der Zukunft für die deutsche Polizei"

Bereits in meinem Ersten Tätigkeitsbericht hatte ich mich zur INPOL-Neukonzeption (Informationssystem der Polizei) geäußert und gefordert, daß alle datenschutzrechtlichen Anforderungen auf eine gesetzliche Grundlage, das BKA-Gesetz, gestellt werden müssen.

In den inzwischen vorliegenden Gesetzentwurf (Bundesrats-Drs. 94/95) sind eine Reihe datenschutzrechtlich positiv zu wertende Vorschriften aufgenommen worden. Dies gilt insbesondere für die seit langem überfälligen bereichsspezifischen Regelungen zur bundesweiten polizeilichen Datenverarbeitung in INPOL.

Zwischenzeitlich liegt ein technisches Grobkonzept zur INPOL-Neukonzeption mit Stand vom 28. März 1995 vor. Dazu erläutere ich einige mir wichtig erscheinende Aspekte:

Infrastrukturansatz

Bereits auf der Ebene der technischen Infrastruktur sind datenschutzrechtliche Anforderungen zu formulieren und zu realisieren, da unzureichende technisch-organisatorische Maßnahmen auf der Infrastrukturebene in den einzelnen Anwendungen nicht mehr aufgefangen werden können (deshalb zum Beispiel die Forderung nach genereller Verschlüsselung von Daten bei Übertragungen im Netz). Im Hinblick auf die verstärkte europäische Zusammenarbeit (EUROPOL) wäre darauf zu achten, daß die hiesigen Vorkehrungen zur Datensicherung auch europäischen Standards entsprechen; anderenfalls bestünde wegen mangelnder Kompatibilität die Gefahr, daß auf bestimmte Sicherheitsvorkehrungen ganz verzichtet würde.

Zentrale Polizeidomäne zur Kommunikation mit externen Informationsdiensten

Die zentralen Polizeidomäne enthält im Sinne eines gesamtheitlichen "Kommunikations- und Informationszentrums" (KIZ) die zentralen Informations- und Kommunikationseinrichtungen, die für den Betrieb des Verbundsystems (INPOL-neu) erforderlich sind. Eine wesentliche Aufgabe ist die Bereitstellung von Diensten und Schnittstellen für die Kommunikation mit der "Außenwelt", das heißt mit externen Informationsdiensten. Hierbei ist aus datenschutzrechtlicher Sicht zu berücksichtigen, daß die externen Kommunikationsdienste, wie das Ausländerzentralregister (AZR), das Bundeszentralregister (BZR) oder das Zentrale Verkehrsinformationssystem (ZEVIS) keine polizeilichen Anwendungen sind, sondern bereichsspezifischen Regelungen unterliegen. Wenn die Kommunikation mit den externen Diensten über eine zentrale Stelle abgewickelt wird, darf dies nicht dazu führen, daß die zentrale Stelle auf die Kommunikationsinhalte zurückgreift und sie auswertet.

Demnach wären

1. die bereichsspezifischen Anforderungen mindestens zu erfüllen;
2. weitergehende Sicherheitsvorkehrungen im Rahmen von INPOL wünschenswert (beispielsweise individuelle Authentifikation bei ZEVIS-Abrufen zusätzlich zur Terminalkennung);
3. Maßnahmen zur Sicherung gegen unberechtigte Zugriffe auf die zentrale Domäne zu treffen.

Übergeordnete Benutzerverwaltung

Es wird der Eindruck erweckt, daß eine übergeordnete Benutzerverwaltung vorgesehen ist. Die Aussage ist jedoch so zu verstehen, daß bei dezentraler Benutzerverwaltung die überregional erforderlichen Informationen in einem elektronischen Verzeichnis zur Verfügung stehen. Eine zentrale Benutzerverwaltung wäre dagegen angesichts der großen Zahl von Benutzern unrealistisch.

Universelle Kommunikationsschnittstelle

Da der Kommunikationsschnittstelle für die gesamte INPOL-Neukonzeption entscheidende Bedeutung zukommt, wären konkretisierende Aussagen hierzu erforderlich, die bisher fehlen. Jedenfalls muß die Schnittstelle so ausgestaltet werden, daß die für INPOL-neu erforderlichen Datensicherungsvorkehrungen gewährleistet werden.

Sicherheit der Informationstechnik (IT-Sicherheit)

Zur IT-Sicherheit sind im technischen Grobkonzept einige Aussagen getroffen worden, die einer weiteren Konkretisierung und Differenzierung bedürfen. Im Kreise der Datenschutzbeauftragten (DSB) besteht Konsens, daß die Forderung nach geeigneter Verschlüsselung generell und nicht nur für Satellitenübertragung gilt. Die Empfehlungen der DSB zum Datenschutz bei elektronischen Mitteilungssystemen wären zu berücksichtigen (vgl. Anlage 15).

Darüber hinaus sollten alle standardisierten Vorkehrungen zur Datensicherung genutzt werden, die ISDN (Integrated Services Digital Network) bietet, zum Beispiel geschlossene Benutzergruppen oder Rufnummernprüfung.

Das vorgesehene INPOL-neu-Verfahren soll eine umfassende Abfragemöglichkeit im gesamten Datenbestand eröffnen. Wenn ein einzelnes Datenobjekt abgefragt wird, kann sich der Anwender in Form einer Gesamtübersicht auf einen Blick anzeigen lassen, welche Informationen zu anderen Datenobjekten wie Personen, Sachen, Objekten, Institutionen oder Fällen gespeichert sind, die mit dem abgefragten Datenobjekt in Beziehung stehen. So erhält der Benutzer eine umfassende Auskunft zu dem gesamten Datenbestand des betreffenden Datenobjektes.

Diese Abfrage in Gestalt einer Gesamtübersicht stellt eine erhebliche Erweiterung der bisherigen Nutzungsmöglichkeiten von INPOL dar. Aus datenschutzrechtlicher Sicht ergibt sich daher die Forderung, dem Abfrageberechtigten aus der Gesamtübersicht nur das Datenmaterial zur Verfügung zu stellen, das er für die Erfüllung seiner ihm übertragenen polizeilichen Aufgaben benötigt. Insbesondere sind die Pläne für einen Kriminalaktennachweis mit Fallgrunddaten und die Aussagen zum Verhältnis und den Informationsflüssen zwischen SPUDOK (Spurendokumentation) und Kerninformationen einer kritischen Würdigung zu unterziehen.

Insgesamt ist festzustellen, daß die polizeiliche Datenverarbeitung durch die INPOL-Neukonzeption eine neue Dimension erhält, die es kritisch zu begleiten gilt.

2.3.3. Sind alle polizeilichen Befugnisse tatsächlich erforderlich?

Die Datenschutzbeauftragten haben auf ihrer 48. Konferenz am 26./27. September 1994 in einer Entschließung Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen erarbeitet (siehe Anlage 8).

Anliegen der Datenschutzbeauftragten war es, die Diskussion auf besser gesicherte Erkenntnisse zu stützen. Das Bundeskriminalamt hatte Vorschläge für eine umfassende Rechtstatsachensammlung über die Anzahl besonderer Erhebungsmethoden, den Erfolg dieser Maßnahmen und Schwierigkeiten bei der Durchführung unterbreitet. Sie wurden jedoch von der Mehrzahl der Länderpolizeien bei der Vorlage ihres Schlußberichtes am 7./8. Dezember 1994 abgelehnt. Statt dessen sollte eine Bund/Länder-Fallsammlung eingerichtet werden mit der Intention, den rechtspolitischen Forderungen der Polizei argumentative Unterstützung zu geben. Laut Schlußbericht sollte die Fallsammlung so ausgelegt sein, daß durch die gesammelten Fälle "Schwachstellen", "spektakuläre Erfolgsfälle" und "zweifelsfreie Grenzen polizeilicher Möglichkeiten" dargestellt werden.

Die Datenschutzbeauftragten stellten hierzu fest, daß die Einrichtung einer Rechtstatsachensammlung als objektives Instrument zur Bewertung polizeilicher Eingriffsbefugnisse auch aus datenschutzrechtlicher Sicht zu begrüßen wäre. Diese Sammlung darf jedoch nicht einseitig den Zweck verfolgen, Forderungen der Polizei zur Erreichung zusätzlicher Befugnisse argumentativ zu unterstützen. Das Vorhaben geht in die falsche Richtung, wenn es von vornherein aufgrund des angelieferten Datenmaterials auf bestimmte Ereignisse festgelegt ist. Vielmehr soll die Rechtstatsachensammlung eine objektive Beurteilung des Einsatzes und der Erkenntnisse besonderer Erhebungsmethoden zur Datenverarbeitung ermöglichen.
Mit Schreiben vom 13. April 1995 forderten die Datenschutzbeauftragten daher den Vorsitzenden der Innenministerkonferenz auf, die Überlegungen für eine offene und aussagekräftige Rechtstatsachensammlung weiter zu verfolgen.

Ich hatte den Innenminister unseres Landes gebeten, den Standpunkt der Datenschutzbeauftragten anläßlich der nächsten Innenministerkonferenz (IMK) in die Meinungsbildung einfließen zu lassen. Dazu war er nicht bereit.

Der Innenausschuß des Deutschen Bundestages hat dieses Thema in seiner Sitzung am 28. Juni 1995 behandelt. Alle Fraktionen haben die Absicht der Bundesregierung unterstützt, durch Einrichtung einer systematischen Rechtstatsachensammlung die Erkenntnisse über die Erforderlichkeit und den Erfolg von polizeilichen Befugnissen zur Erhebung und Verarbeitung personenbezogener Daten zu verbessern. Datenschutz und innere Sicherheit müssen sich also bei gutem Willen keineswegs gegenseitig ausschließen.

2.3.4. Bereinigung der DDR-Kriminalakten - Ende in Sicht?

Im März 1994 habe ich in zwei Kriminalpolizeiinspektionen den Zustand der Kriminalakten, die bereits zu DDR-Zeiten angelegt worden waren, kontrolliert und dabei datenschutzrechtliche Mängel festgestellt.

Im wesentlichen wurden die bereits während des ersten Berichtszeitraumes bei einer Stichprobenkontrolle gemachten Erfahrungen bestätigt. In den geprüften Akten befanden sich immer noch personenbezogene Daten, die gemäß § 45 Abs. 2 Satz 1 des Gesetzes über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern (SOG MV) bereits hätten entfernt sein müssen. Diese Regelung gilt für alle personenbezogenen Daten, deren Erhebung unzulässig war oder deren weitere Speicherung unzulässig ist. Anhand der umfangreichen Daten- und Vernehmungsprotokolle sowie der in den Akten enthaltenen Ausführungen zur persönlichen und gesellschaftlichen Entwicklung des Betroffenen, zu Familienverhältnissen etc. konnten umfassende Persönlichkeitsbilder erstellt werden. In einer Kriminalakte waren neben den oben genannten Unterlagen beispielsweise auch Fotos enthalten, auf denen der Betroffene völlig nackt abgebildet war. Diese Fotos dienten dazu, die Tätowierungen am Körper des Betroffenen aufzunehmen. Eine Aufnahme des Betroffenen in komplett entblößtem Zustand war jedoch weder notwendig noch erforderlich, um den Zweck zu erreichen. Es konnte nicht mehr nachvollzogen werden, woher diese Fotos stammen. Darüber hinaus waren in einigen Akten unter anderem noch Angaben zu Straftaten gespeichert, für die keine gesetzliche Grundlage mehr existiert, etwa sogenannte Asozialität.

Weiterhin stellte ich fest, daß in einer Reihe von Akten die Meldungen zum Ausgang des Strafermittlungsverfahrens fehlten. Gemäß § 37 Abs. 2 SOG MV darf in diesen Fällen eine Speicherung dieser Daten zunächst nur für zwei Jahre erfolgen. Liegen bis zu diesem Zeitpunkt noch keine Erkenntnisse zum Ausgang des Verfahrens vor, so hat die Polizei die entsprechenden Erkundigungen einzuholen und zu prüfen, ob eine weitere Speicherung zulässig ist. Entfällt der zugrunde liegende Verdacht, so sind die Daten umgehend zu löschen. In einigen Fällen war diese Zweijahresfrist bereits überschritten, ohne daß eine Rückmeldung seitens der Staatsanwaltschaft erfolgt war. Ich habe empfohlen, sich in diesen Fällen umgehend an die zuständigen Staatsanwaltschaften zu wenden und den Ausgang des Verfahrens zu erfragen.

Die Mängel in den kontrollierten Akten wurden durch die Mitarbeiter der Kriminalpolizeiinspektionen nach der Kontrolle sofort beseitigt.

Darüber hinaus waren bei vielen Akten die Aufbewahrungsfristen abgelaufen. Diese Unterlagen wurden weiterhin vorgehalten, ohne daß eine erneute Prüfung hinsichtlich der Zulässigkeit einer weiteren Aufbewahrung erfolgt ist. Akten mit personenbezogenen Daten, die nicht unter die Regelung des § 45 Abs. 2 Satz 1 SOG MV fallen, sind auszusondern, wenn die gesamte Akte nicht mehr zur Aufgabenerfüllung erforderlich ist. Ziffer 5 der am 1. Januar 1993 in Kraft getretenen Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen in Mecklenburg-Vorpommern (RKpS MV) sieht für die Aufbewahrung der Unterlagen unter Beachtung des Verhältnismäßigkeitsgrundsatzes differenzierte Aufbewahrungsfristen vor. Da für die Altakten überwiegend keine Fristen bestimmt wurden und darüber hinaus auch keine Überwachung der nur zum Teil festgelegten Fristen vorgesehen war, wurden die Akten unabhängig vom Ablauf der Speicherfristen weiterhin aufbewahrt, bis bei einem erneuten Zugriff festgestellt wurde, daß eine Aussonderung zu erfolgen hat. Durch die geplante Übernahme der Kriminalakten in ein automatisiertes Verzeichnis (Kriminalaktennachweis) ist eine Überwachung der Aussonderungsprüffristen möglich, so daß dann eine Speicherung entsprechend den gesetzlichen Bestimmungen erfolgen kann und die Problematik in diesem Bereich gelöst wird.

Die Kriminalpolizeiinspektion ist meinen Empfehlungen gefolgt, bis zur Inbetriebnahme des Kriminalaktennachweises die Aufbewahrungsfristen mit Hilfe eines PC zu überwachen.

Gemäß Ziffer 11 der Dienstanweisung für die Führung von Kriminalakten (KA-Richtlinien) vom 19. März 1993 sind DDR-Aktenbestände nach Vorgabe dieser Richtlinien zu bereinigen. Diese enthalten jedoch nur allgemeine Aussagen zur Führung von Kriminalakten. Zum Verfahren der Bereinigung, insbesondere welche Unterlagen den Kriminalakten zu entnehmen und wie diese auch im Hinblick auf ein mögliches schutzwürdiges Interesse der Betroffenen weiter zu behandeln sind, werden keine Hinweise gegeben. Wie eine Umfrage unter den Kriminalpolizeiinspektionen des Landes ergab, erfolgte die Bereinigung der Akten nicht kontinuierlich, sondern nur dann, wenn erneut auf diese zugegriffen wurde. Lediglich in der Kriminalpolizeiinspektion Rostock hatte man anhand eigens dafür aufgestellter Kriterien mit der kontinuierlichen Bereinigung dieser Akten begonnen.

Bei der Prüfung bereits als bereinigt geltender Kriminalakten wurde darüber hinaus deutlich, daß ganz erhebliche Unklarheiten bestanden, welche Unterlagen auszusondern bzw. welche personenbezogenen Daten zu löschen sind. Ich habe daher aufgrund der landesweiten Problematik im Mai 1994 gegenüber dem Innenminister angeregt, umgehend eine Richtlinie zur Bereinigung dieses Altaktenbestandes zu erarbeiten und in Kraft zu setzen, um so den mit dieser Aufgabe betrauten Personen eine Hilfestellung zu geben, damit die Bereinigung der Akten entsprechend den geltenden Bestimmungen erfolgen kann.

Die seit Juni 1995 vorliegende Richtlinie zur Bereinigung der DDR-Kriminalakten trägt diesen Anforderungen Rechnung. Von besonderer Bedeutung ist in diesem Zusammenhang, daß nunmehr eine kontinuierliche Bereinigung der Altakten vorgesehen ist. In den anderen neuen Bundesländern ist dieses Problem zwischenzeitlich längst gelöst worden. Die Bereinigung der Kriminalaltaktenbestände in Mecklenburg-Vorpommern soll laut Aussage des Innenministers nunmehr endgültig bis Mitte 1996 abgeschlossen sein.

2.3.5. Kontrolle des KfZ-Scheins durch privaten Sicherheitsdienst

Ein Student einer Fachhochschule (FH) beklagte sich bei mir darüber, daß er jedesmal, wenn er das Gelände der FH mit seinem Pkw verlassen wollte, den Mitarbeitern des privaten Sicherheitsdienstes, die das Gelände überwachen, den Fahrzeugschein vorlegen muß. Die Papiere wurden verlangt, obwohl das Personal sich bereits beim Auffahren auf das Gelände den Studenten- bzw. Parkausweis vorzeigen ließ. Begründet wurde dieses Vorgehen mit der Prävention von KfZ-Diebstählen.

Die Kontrolle von Fahrzeug- und anderen Ausweispapieren obliegt grundsätzlich der Polizei bzw. den Ordnungsbehörden. Die Angestellten eines Wachdienstes haben insoweit nicht mehr Befugnisse, als jede andere Privatperson. Ihnen stehen zwar Selbsthilferechte (z. B. § 229 Bürgerliches Gesetzbuch) sowie das allgemeine Festnahmerecht (§ 127 Strafprozeßordnung - StPO) zu, aber beide Befugnisse waren in diesem Fall nicht einschlägig.

Das öffentlich-rechtliche Hausrecht der Fachhochschule kann keine wirksame Rechtsgrundlage für derartige Kontrollen beim Verlassen des Geländes sein. Es rechtfertigt allenfalls die Überprüfung einer Zugangsberechtigung auf das Grundstück. Dies ist gestattet, da es sich um ein eingegrenztes Grundstück handelt, auf dem sich nur Mitarbeiter und Studierende aufhalten sollen.

Somit waren die Kontrollen rechtswidrig. Die Pflicht zur Vorlage des Fahrzeugscheins stellt einen ungerechtfertigten Eingriff in das Persönlichkeitsrecht der Betroffenen dar. Dies habe ich dem Direktor der Fachhochschule mitgeteilt. Er hat sich meiner Rechtsauffassung angeschlossen. Zukünftig wird es nur noch eine Kontrolle der Parkberechtigung bzw. eines Haus- oder Studentenausweises bei der Auffahrt auf das Gelände geben. Die Kontrollen bei der Ausfahrt wurden eingestellt.

2.3.6. Forschungsprojekt "Jugendkriminalität in Mecklenburg-Vorpommern"

Im Vergleich zu anderen Bundesländern ist in Mecklenburg-Vorpommern die Zahl der 14- bis 21jährigen, die einer kriminellen Tat verdächtigt sind, besonders hoch. Um effektive Präventionskonzepte erarbeiten zu können, sind unter anderem Kenntnisse über soziale und individuelle Bedingungen, Ursachen, Verlauf und Muster krimineller Entwicklung von jungen Menschen notwendig.

Vor diesem Hintergrund beabsichtigen das Landeskriminalamt Mecklenburg-Vorpommern (LKA) und der Lehrstuhl für Kriminologie an einer Universität Daten tatverdächtiger Jugendlicher und Heranwachsender zu analysieren sowie Befragungen und Interviews durchzuführen. Der Innenminister hatte mir das Forschungsprojekt zur datenschutzrechtlichen Prüfung vorgelegt.

Vorgesehen war unter anderem, personenbezogene Daten von Jugendlichen und Heranwachsenden, die ab 1993 in die polizeiliche Kriminalstatistik Mecklenburg-Vorpommern eingegangen waren, ohne deren Einwilligung an den Lehrstuhl für Kriminologie zu übermitteln und dort auszuwerten. Gleichzeitig sollten Jugendsachbearbeiter die bei den Polizeidienststellen registrierten jugendlichen und heranwachsenden Tatverdächtigen (TV) im Anschluß an ihre Ver-

nehmung anhand eines umfangreichen Fragebogens zur Persönlichkeit, zu Straftaten und zu ihrem Umfeld befragen.

Gegen diese Verfahrensweise habe ich folgende Bedenken vorgebracht:

1. Methodische Probleme der Untersuchung

Im Hinblick auf die Wissenschaftlichkeit des Vorhabens halte ich die Befragung von Jugendlichen durch Polizeibeamte in diesem Rahmen generell für problematisch. Denn eine strikte Trennung der Vernehmungssituation einerseits und der Befragungssituation andererseits ist so aus meiner Sicht kaum realisierbar.

2. Fragebogen Polizeibeamte

Polizeibeamte sollten ihre Einschätzung über den Tatverdächtigen abgeben. Bedenklich war meines Erachtens, daß Polizeibeamte eine Einschätzung von Charaktereigenschaften vornehmen sollen, die sie aufgrund der besonderen Situation - Befragung im Anschluß an die Vernehmung - unter Umständen gar nicht abgeben können. Zwangsläufig würde diese Einschätzung sehr subjektiv und damit möglicherweise stark fehlerbehaftet sein. Denn allemal entstünde sie vor dem Hintergrund der stattgefundenen Vernehmung und wäre damit von ihr nicht unabhängig. Verlief diese beispielsweise bereits "spannungsgeladen" oder "kooperativ" oder "mauerte der Verdächtige während der Vernehmung" - was sein gutes Recht ist, da sich niemand selbst belasten muß -, liegt die Vermutung nahe, daß der Polizeibeamte seinen Ersteindruck "Sperrung, nicht kommunikativ" in die Bewertung einfließen läßt, obwohl der Verdächtige diese Charaktereigenschaft unter Umständen gar nicht besitzt.

3. Fragebogen Jugendlicher/Heranwachsender (TV-Befragung)

Die von den Jugendlichen zu beantwortenden Fragen würden in einem besonderen Maße in die Persönlichkeitssphäre und damit in das informationelle Selbstbestimmungsrecht eingreifen. Der Betroffene bezichtigt sich möglicherweise im Gespräch mit dem Polizeibeamten selbst, wenn er die Fragen - wenn auch nicht im Rahmen der Vernehmung - wahrheitsgemäß beantwortet. Fraglich wäre dann, ob nicht der Polizeibeamte unter Umständen als Ausfluß des Legalitätsprinzips sogar von Amts wegen ermitteln müßte. Beantwortet der Jugendliche die Frage jedoch nicht wahrheitsgemäß, hätte die Beantwortung ohnehin keinen Aussagewert.

4. Einwilligungserklärung

Das Formular für die Einwilligungserklärung entsprach nicht den in § 7 DSG MV genannten Voraussetzungen. Dem Betroffenen muß zunächst der Inhalt des Fragebogens bekannt sein, damit er weiß, worin er einwilligt. Konkret bedeutet das, daß ihm die Fragen vorher vorgelegt werden müssen, damit er sich dann entscheiden kann, ob er an dieser Befragung teilnimmt.

Über Art und Umfang der Erhebung, Verarbeitung und Nutzung sowie den Empfänger der Daten ist der Betroffene zu unterrichten, und ihm ist die Anschrift der mit den Daten umgehenden Stelle mitzuteilen. Darüber hinaus ist er darüber aufzuklären, daß er die Einwilligung verweigern und jederzeit für die Zukunft widerrufen kann. Der Betroffene ist ebenfalls auf die Möglichkeit hinzuweisen, einzelne Fragen nicht zu beantworten. In der vorformulierten Einwilligungserklärung ist außerdem auf die Mehrstufigkeit des Forschungsvorhabens aufmerksam zu machen.

Aufgrund meiner Bedenken hat der Leiter des Forschungsprojektes sein Konzept in den wesentlichen Punkten kurzfristig geändert.

Nunmehr wird eine Struktur- und Verlaufsanalyse nach spezifischen Kriterien und Merkmalen vorgenommen. Dazu hat das LKA regional aggregierte Grundauszählungen in Form von Maschinentabellen zur Verfügung gestellt. Durch dieses Verfahren wird die Anonymität des Tatverdächtigen sichergestellt und trotzdem der vorgesehene Zweck der Untersuchung erreicht. Die Befragung wird nicht mehr durch Polizeibeamte, sondern durch Jugendgerichtshelfer vorgenommen. Diese sind aufgrund ihrer Ausbildung und der ihnen vom Gesetz zugewiesenen Aufgaben sicher auch besser geeignet, die Jugendlichen zu interviewen. Die Einwilligungserklärung wurde entsprechend meinen Empfehlungen formuliert.

2.3.7. Mitteilung über die Beschlagnahme eines Führerscheines

Durch einen meiner Kollegen wurde ich angeregt, das Verfahren der Datenübermittlung über die Beschlagnahme von Führerscheinen von der Polizei an die Führerscheinstellen in unserem Land zu prüfen.

Beschlagnahmt die Polizei einen Führerschein, so zeigt sie dieses innerhalb von drei Tagen einem Richter an und übergibt ihm den Führerschein. Nach Abschluß des Gerichtsverfahrens wird der Beschluß zusammen mit dem Führerschein an die zuständige Führerscheinstelle übersandt. Bis zur rechtskräftigen Verurteilung des Fahrzeugführers vergehen derzeit ungefähr 3 bis 4 Monate. Erst dann kann die gerichtliche Entscheidung im Zentralen Fahrerlaubnisregister beim Kraftfahrt-Bundesamt erfaßt werden.

Sofern die Polizei einen Führerschein beschlagnahmt, informiert sie hierüber auch umgehend die zuständige Führerscheinstelle. Die Meldung erfolgt regelmäßig durch die Übersendung einer Durchschrift des Beschlagnahmeprotokolls. Nach § 40 Abs. 1 SOG MV ist eine Datenübermittlung an die Ordnungsbehörde zulässig, soweit dies zur Erfüllung polizeilicher oder ordnungsbehördlicher Aufgaben erforderlich ist. Durch die frühzeitige Benachrichtigung der Führerscheinstellen soll verhindert werden, daß Personen, deren Führerschein beschlagnahmt wurde, einen Ersatzführerschein unter dem Vorwand beantragen, sie hätten ihren Führerschein verloren. Wird eine Beschlagnahme gerichtlich nicht bestätigt und der Führerschein dem Betroffenen zurückgegeben, wurde die Führerscheinstelle bisher nicht informiert, so daß die Daten des Betroffenen dort weiterhin gespeichert wurden.

Gegen dieses Verfahren habe ich Bedenken geäußert. Denn danach wird jeder Person, deren Führerschein beschlagnahmt wurde, stillschweigend unterstellt, daß sie einen Ersatzführerschein beantragen wird. Meine Kontrollen in Führerscheinstellen haben allerdings ergeben, daß solche Anträge nur vereinzelt gestellt werden. Die regelmäßige Unterrichtung der Führerscheinstellen führt zu einer Datensammlung auf Vorrat. Innen- und Wirtschaftsministerium wiesen darauf hin, daß den Führerscheinstellen diese Daten ohnehin nach Abschluß des Gerichtsverfahrens zur Kenntnis gelangen. Ich habe angeregt, daß den Führerscheinstellen frühzeitig nur die Tatsache mitgeteilt wird, daß eine Beschlagnahme erfolgt ist, jedoch keine Gründe angegeben werden.

Darüber hinaus habe ich den Umfang der Beschlagnahmeprotokolle geprüft und im Ergebnis darauf hingewiesen, daß lediglich Name, Vorname, Geburtstag und -ort, Anschrift, Führerscheinnummer sowie Tag der Ausstellung übermittelt werden dürfen. Weitere Informationen, wie z. B. Beruf, Halter des Fahrzeuges, Grund der Beschlagnahme, sind für die Führerscheinstellen zu diesem Zeitpunkt nicht relevant. Des weiteren habe ich gefordert, daß, sofern keine gerichtliche Bestätigung der Beschlagnahme erfolgt und der Führerschein dem Betroffenen zurückgegeben wird, die Führerscheinstellen hiervon zu unterrichten und die Unterlagen zu vernichten sind.

Im Einvernehmen mit den beteiligten Ministerien wird nunmehr so verfahren.

2.3.8. Großer Lauschangriff

Nachdem sich CDU und SPD schon längst prinzipiell für den Großen Lauschangriff ausgesprochen haben, hat sich nunmehr auch die Mehrheit der F.D.P.-Mitglieder dafür entschieden. Sollte es in absehbarer Zeit tatsächlich dazu kommen, daß in privaten Wohnungen heimlich Bild- und Tonaufzeichnungen gemacht werden können, um Straftaten aufzuklären, dann bleibt uns allen nur zu hoffen, daß dieses Mittel auch wirklich den versprochenen Erfolg bringt. Aber gerade daran habe ich die stärksten Zweifel.

Für bedenklich halte ich auch die inzwischen in der Bevölkerung eingetretene Informationsschieflage. So können viele Bürger zwar mit dem Terminus "Großer Lauschangriff" etwas anfangen und verbinden mit ihm die Hoffnung auf eine erfolgreichere Arbeit der Polizei, aber kaum jemand weiß, daß es sich hierbei

- nur um die Aufklärung bereits begangener schwerer Straftaten der organisierten Kriminalität handelt, und daß das Abhören von Wohnungen bereits heute erlaubt ist, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person unerläßlich ist,

- nicht um die Wohnungen von Schwerverbrechern handelt, sondern zunächst einmal um die Wohnungen von Verdächtigen,

- um eine Maßnahme handelt, die einer aufwendigen technischen und organisatorischen Vorbereitung bedarf und deren Durchführung Tage, Wochen oder gar Monate dauern kann, bis die entscheidende Information geliefert oder auch nicht geliefert wird, und daß in dieser Zeit Gespräche Unbeteiligter, wie Familienmitglieder, Freunde, Bekannte und Besucher, aufgezeichnet werden, die erst viel später ausgewertet werden können,

- ausschließlich um die Elite der organisierten Kriminalität handelt, die sich heute leicht geeigneter technischer Mittel und wirksamer organisatorischer Maßnahmen bedienen kann, um einen Lauschangriff völlig ins Leere laufen zu lassen.

In Anbetracht dieser Tatsachen scheint mir für die vorgesehene gravierende Beeinträchtigung des Grundrechts, das den einzigen privaten Lebensraum des Bürgers schützt, nach wie vor eine überzeugende Begründung zu fehlen.

Das Bundesverfassungsgericht hat in mehreren Entscheidungen anerkannt, daß ein letzter unantastbarer Bereich privater Lebensgestaltung existiert, der der staatlichen Ausforschung entzogen bleiben muß und bei dem selbst schwerwiegende Allgemeininteressen einen Eingriff nicht rechtfertigen können. Das geltende Recht setzt voraus, auch in Krisensituationen die Grundrechte nicht in ihrem Wesensgehalt anzutasten. Aber gerade diese Entschlossenheit, die unseren Rechtsstaat ausmacht, wird meines Erachtens durch die Diskussion um den Großen Lauschangriff in Frage gestellt.

2.4. Verkehr

2.4.1. Speicherung von Wiederholungsfällen bei Verstößen im ruhenden Verkehr

Aufgrund einer Anfrage eines Kollegen habe ich mich beim auch für das Verkehrsrecht zuständigen Wirtschaftsminister darüber informiert, ob die Ordnungsbehörden unseres Landes die im Rahmen von Verwarnungs- und Bußgeldverfahren erhobenen und gespeicherten Daten auch für die Feststellung von Mehrfachverstößen nutzen.

Die Recherchen ergaben, daß eine Reihe von Behörden automatisierte Verfahren zur Abwicklung der Verwarnungs- und Bußgeldverfahren einsetzen. Sobald die gebührenpflichtige Verwarnung wirksam geworden ist, löschen einige Behörden die Daten. Andere speichern die Daten auch über diesen Zeitpunkt hinaus. Eine Ermittlung von Mehrfachtätern wäre in diesem Zusammenhang softwareseitig prinzipiell leicht möglich. Hiervon haben die Ordnungsbehörden unseres Landes bisher jedoch keinen Gebrauch gemacht. Als Rechtsgrundlage für die Speicherung der Daten wurde auf die Vorschriften des Landesdatenschutzgesetzes verwiesen.

Ich habe dem Minister mitgeteilt, daß eine Speicherung dieser Daten durch die Ordnungsbehörden auf der Grundlage der allgemeinen datenschutzrechtlichen Bestimmungen nicht zulässig ist. Das Landesdatenschutzgesetz als Auffanggesetz kann nur dann als Rechtsgrundlage herangezogen werden, wenn bereichsspezifische Vorschriften eine vom Gesetzgeber nicht beabsichtigte Regelungslücke enthalten. Die Speicherung von Angaben über Maßnahmen auf dem Gebiet des Verkehrsrechts ist aber bereichsspezifisch und abschließend in den Vorschriften des Straßenverkehrsgesetzes über das Verkehrszentralregister geregelt. Neben dieser zentralen Registrierung der gerichtlichen und verwaltungsbehördlichen Entscheidungen ist eine Erfassung von Wiederholungsfällen in örtlichen Karteien bzw. Dateien unzulässig. Insofern kommt eine Speicherung dieser Daten auf der Grundlage des Landesdatenschutzgesetzes nicht in Betracht.

Der Minister teilt meine Rechtsauffassung und hat sie den Kreisordnungsbehörden mit der Bitte um künftige Beachtung zur Kenntnis gegeben.

2.4.2. Muß mein Briefträger wissen, daß ich eine Ordnungswidrigkeit begangen habe?

Einige Bürger beschwerten sich bei mir, daß sie von Städten und Landkreisen Briefe bekamen, bei denen als Absender auf dem Umschlag der Zusatz "Ordnungsamt Bußgeldstelle" vermerkt war. Dieser Text fand sich auch in der Empfänger-Zeile der Überweisungsträger wieder. In einem Fall überreichte der Postbote einem Betroffenen einen Brief der "Abteilung für Bußgeld und Verwarnungsgeld für Verkehrsordnungswidrigkeiten" mit den Worten, daß er wohl zu schnell gefahren sei und nun eine Geldbuße zu zahlen hätte.

Solche Angaben als Absender auf Briefumschlägen oder als Empfänger von Überweisungen lassen darauf schließen, daß der Adressat bzw. Aussteller mit großer Wahrscheinlichkeit eine Ordnungswidrigkeit begangen hat. Sie sind mit dem Namen des Betroffenen verknüpft und stellen daher personenbezogene Daten dar. Alle Personen, durch deren Hände der Brief oder die Überweisung läuft, erhalten davon Kenntnis. Neben den Postbediensteten können dies unter anderem Bankangestellte, Familienangehörige, Partner nichtehelicher Lebensgemeinschaften oder Mitbewohner einer Wohngemeinschaft sein. Auch wenn für einen Teil dieser Personen bzw. Personengruppen eine Schweigepflicht besteht, ändert dies nichts daran, daß die Bekanntgabe der Daten nicht erforderlich und somit datenschutzrechtlich unzulässig ist.

Ich habe mich an die zuständigen Städte bzw. Landkreise gewandt und sie gebeten, die in ihrer Verwaltung verwendeten Umschläge und Überweisungsträger datenschutzgerecht zu gestalten. Die Städte und Landkreise sind meiner Empfehlung gefolgt und werden Zusätze wie "Bußgeldstelle" o. ä. als Absender bzw. Empfänger künftig nicht mehr verwenden.

2.4.3. Geschwindigkeitskontrolle des fließenden Verkehrs durch Private?

Der Minister für Wirtschaft und Angelegenheiten der Europäischen Union hat bei mir angefragt, inwieweit Private aus datenschutzrechtlicher Sicht in die Geschwindigkeitsüberwachung einbezogen werden dürfen.

Die Rechtslage ist folgende:

Abweichend von der allgemeinen gesetzlichen Zuständigkeitsregelung nach § 36 Ordnungswidrigkeitengesetz hat die Landesregierung den Landräten und Oberbürgermeistern (Bürgermeistern) der kreisfreien Städte die Aufgaben der Verkehrsüberwachung, unbeschadet der Zuständigkeit der Polizei, übertragen.

Grundsätzlich obliegt es daher den Kommunen, Ordnungswidrigkeiten zu verfolgen und zu ahnden. Derartige hoheitliche Tätigkeiten dürfen nicht auf Private übertragen werden.

Hiervon zu unterscheiden ist jedoch die Beauftragung Privater mit nicht-hoheitlichen Hilfstätigkeiten. Oft ist es schwierig abzugrenzen, welche Tätigkeit hoheitlicher Natur ist und welche sich als schlichte Hilfstätigkeit darstellt. Der Wirtschaftsminister will durch einen Erlaß das notwendige regeln. In diesem Zusammenhang habe ich auf die Einhaltung folgender datenschutzrechtlicher Aspekte hingewiesen:

- Die Ordnungsbehörde muß grundsätzlich Herr des Verfahrens bleiben. Wird beispielsweise eine private Firma mit der Entwicklung von Filmen beauftragt, so handelt es sich hierbei um Datenverarbeitung im Auftrag, für die es im Rahmen eines Ordnungswidrigkeitenverfahrens keine bereichsspezifische Norm gibt und folglich unser Landesdatenschutzgesetz Anwendung findet. Es müssen insbesondere die in den §§ 4 und 17 DSG MV genannten Voraussetzungen beachtet werden. Danach ist sicherzustellen, daß die auftraggebende Behörde für die Einhaltung datenschutzrechtlicher Bestimmungen sorgt. Dazu gehört insbesondere auch Sorgfalt bei der Auswahl des Beauftragten und dessen Mitarbeitern sowie die Einhaltung der technisch-organisatorischen Maßnahmen zum Schutz der Daten.

- In dem Erlaß sollte nicht nur die Art der Datenträger und deren Aufbewahrung benannt, sondern explizit auf die technisch-organisatorischen Maßnahmen unter Verwendung der Begriffe aus § 17 DSG MV hingewiesen werden. Da es sich im Ordnungswidrigkeitenverfahren um sensible personenbezogene Daten handelt, empfiehlt es sich, die einzelnen Maßnahmen konkret zu benennen, etwa Vergabe von Paßwörtern, Protokoll über Datenzugriff, keine Bildschirmeinsicht für Dritte etc.

- Unterauftragsverhältnisse sind zwar gemäß § 4 DSG MV zulässig, sollten aber bei derart sensiblen Daten ausgeschlossen werden.

- Es ist präzise zu formulieren, daß die privaten Anbieter lediglich Filme entwickeln. Eine Auswertung dieser Daten dürfen ausschließlich die Behörden vornehmen.

Der Wirtschaftsminister will meine Vorschläge berücksichtigen. Der betreffende Erlaß steht noch aus.

2.4.4. Versendung eines Fotos als Beweismittel

Ein Mitarbeiter eines Straßenverkehrs- und Ordnungsamtes hat mich zum Versand von Beweisfotos um Rat gebeten.

Im Rahmen von Bußgeldverfahren wegen Geschwindigkeitsüberschreitungen wird dem Fahrzeughalter in einigen Fällen nicht nur der Anhörungsbogen, sondern auf Wunsch auch ein sogenanntes "Frontfoto" übersandt. Soweit auf diesem Foto nur der Fahrer zu identifizieren ist, bestehen gegen dieses Verfahren keine Einwände. In einigen Fällen sind jedoch weitere Personen zu erkennen. Dann stellt die Übermittlung des Fotos einen unzulässigen Eingriff in das Recht auf informationelle Selbstbestimmung des an der Ordnungswidrigkeit nicht beteiligten Beifahrers dar.

Ich habe das so mitgeteilt und den Innen- sowie den Wirtschaftsminister gebeten, alle zuständigen Behörden über die Rechtslage zu informieren, und empfohlen, andere abgebildete Personen auf den Fotos zu schwärzen oder nur einen entsprechenden Bildausschnitt zu versenden.

Die Minister sind dieser Empfehlung nachgekommen.

2.5. Verfassungsschutz

2.5.1. Kontrolle der Sicherheitsüberprüfungsakten bei der Verfassungsschutzbehörde

Am 22. Februar 1994 hatte ich dem Innenminister mitgeteilt, daß ich beabsichtige, die Sicherheitsüberprüfungsakten beim Verfassungsschutz zu kontrollieren. Daraufhin informierte er mich einen Monat später, daß es bisher versäumt wurde, die von einer Sicherheitsüberprüfung Betroffenen auf ihr Widerspruchsrecht gemäß § 24 Abs. 2 S. 4 in Verbindung mit Abs. 6 Bundesdatenschutzgesetz (BDSG) hinzuweisen. Wir verständigten uns darauf, daß er die überfällige Unterrichtung unverzüglich nachholt. Vier Wochen später habe ich als Termin der Kontrolle den 31. Mai 1994 mitgeteilt und sie an diesem Tage auch durchgeführt. Der Innenminister beklagte sich ein gutes halbes Jahr später, in der Landtagssitzung vom 28. September 1994, darüber, daß ich meine Kontrolle "überraschenderweise" angekündigt hätte. Angesichts der oben genannten Zeiträume halte ich diesen Vorwurf für unberechtigt.

1. Die Kontrolle

Im wesentlichen hat die Kontrolle von 50 Sicherheitsüberprüfungsakten folgendes ergeben:

- Insgesamt waren zu viele personenbezogene Daten von Betroffenen und Dritten erhoben und in den Akten gespeichert, also auch solche Daten, die der Verfassungsschutz zur Erledigung seiner Aufgaben nicht benötigt.

- Bei Ü1- und Ü2-Überprüfungen wurden Bürger der ehemaligen DDR im Gegensatz zu Bürgern aus den alten Ländern ohne ersichtliche sachliche und rechtliche Gründe grundsätzlich einer strengeren Überprüfung unterzogen, was meines Erachtens einen Verstoß gegen den Gleichheitsgrundsatz darstellt.

- Es fanden sich Aussagen von Referenz- bzw. Auskunftspersonen in den Akten wieder, die in keinem Zusammenhang zum Zweck der Überprüfung standen.

- Hinsichtlich der Auskunfts- und Referenzpersonen findet eine sog. "Abklärung" in dem von den Verfassungsschutzbehörden des Bundes und der Länder betriebenen Verbundsystem NADIS (Nachrichtendienstliches Informationssystem) statt, obwohl dies von den geltenden Sicherheitsrichtlinien nicht gedeckt ist.

Aufgrund der festgestellten Verstöße gegen datenschutzrechtliche Bestimmungen habe ich dem Innenminister eine förmliche Beanstandung ausgesprochen. Aus dem daraufhin geführten Schriftwechsel erscheint mir hier folgendes berichtenswert:

Grundsätzlich besteht Übereinstimmung darin, daß die kontrollierten Sicherheitsüberprüfungsakten eine Reihe personenbezogener Daten enthalten bzw. zum Zeitpunkt meiner Kontrolle enthielten, die der Verfassungsschutz zur Erfüllung der ihm gesetzlich vorgeschriebenen Aufgaben nicht benötigt. Es handelt sich hierbei insbesondere um Angaben zu Auskunfts- und Referenzpersonen, Listen weiterer zu Überprüfender, die sich in verschiedenen Akten von Betroffenen befanden, vollständige Ablichtungen ganzer Seiten aus Sozialversicherungsausweisen und Aussagen befragter Personen, die in keinem Zusammenhang mit dem Ziel der Überprüfung standen.

Der Innenminister hat zugesichert, die unzulässigerweise gespeicherten Daten zu löschen und dafür Sorge zu tragen, daß künftig nur noch solche Daten erhoben, verarbeitet und genutzt werden, die für die Sicherheitsüberprüfung der jeweiligen Stufe erforderlich sind.

Hinsichtlich der sogenannten "NADIS-Abfrage" hat der Innenminister zugesagt, derartige Abfragen zu Auskunfts- und Referenzpersonen ab sofort nicht mehr generell, sondern nur noch im Bedarfsfall vornehmen zu lassen, das heißt nur dann, wenn dieser Personenkreis auch tatsächlich befragt werden soll. Diese Vorgehensweise begrüße ich als Verbesserung gegenüber der bisherigen Praxis.

Keine Übereinstimmung gab es hinsichtlich der Interpretation der festgestellten Tatsachen zur Gleichbehandlung der Überprüften aus den alten und den neuen Bundesländern. Diese Problematik erledigt sich jedoch von selbst, wenn die Verfassungsschutzbehörde künftig nur noch solche Daten erhebt, die sie für ihre Mitwirkung bei der Sicherheitsüberprüfung nach Maßgabe der geltenden Sicherheitsüberprüfungsrichtlinien unbedingt benötigt. Da der Innenminister dieses zugesichert hat, sah ich hier keinen weiteren Handlungsbedarf meinerseits und habe das so mitgeteilt.

2. Zum Widerspruchsrecht des Betroffenen gemäß § 24 Abs. 2 Satz 4 Bundesdatenschutzgesetz

Die Kontrolltätigkeit **zum Schutz der Rechte des Bürgers** ist eine der wesentlichen Aufgaben des Landesbeauftragten für den Datenschutz. Sinn und Zweck solcher Kontrollmaßnahmen ist es, dazu beizutragen, daß der einzelne beim Umgang mit seinen personenbezogenen Daten nicht in seinem Persönlichkeitsrecht beeinträchtigt wird. So hat der Landesdatenschutzbeauftragte zum Beispiel allein im Interesse des Bürgers darauf zu achten, daß nur das für die Aufgabenerfüllung einer Behörde erforderliche Minimum an Daten erhoben und gespeichert wird.

Selbstverständlich respektiere ich es, wenn sich jemand - aus welchen Gründen auch immer - gegen die Kontrolle seiner Sicherheitsüberprüfungsakte ausspricht.

Den Innenminister habe ich informiert, wie eine Belehrung über das Widerspruchsrecht in Anlehnung an einen mit dem Bundesbeauftragten für den Datenschutz (BfD) abgestimmten Vordruck gestaltet sein könnte. Darüber hinaus habe ich darauf hingewiesen, daß das in seinen Verantwortungsbereich fallende Unterlassen einer Belehrung nicht dazu führen kann, daß ich bis zum Rücklauf möglicher Widersprüche keine Akten kontrollieren kann. Durch Gesetz ist dem Landesbeauftragten für den Datenschutz ausdrücklich die Aufgabe übertragen worden, **jederzeit** Kontrollen durchzuführen. Es verbietet sich also a priori für die öffentliche Stelle, mit der Unterrichtung so lange zu warten, bis eine Kontrolle ins Haus steht.

Hinsichtlich des gemäß § 24 Abs. 2 Satz 4 BDSG zu belehrenden Personenkreises entwickelte sich zwischen dem Innenminister und mir eine recht langwierige Korrespondenz. Da die Interpretation des Begriffes für die Rechtsposition der Betroffenen und auch der Umfang der mir vom Gesetz übertragenen Kontrolltätigkeit von besonderer Bedeutung sind, stelle ich die Standpunkte hier noch einmal gegenüber.

Der Innenminister vertritt die Rechtsauffassung, daß jeder, über den personenbezogene Daten in Sicherheitsüberprüfungsakten gespeichert sind (überprüfte Personen, Auskunfts- und Referenzpersonen, Ehegatten, ...), der Akteneinsicht durch den Landesbeauftragten für den Datenschutz widersprechen kann. Er geht dabei von der Begriffsbestimmung des § 3 BDSG aus. Dort heißt es in Abs. 1 wörtlich: "Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)." Er ist des weiteren der Auffassung, daß der Wortlaut des Gesetzes eindeutig ist und somit für eine systematische und teleologische Auslegung des Begriffes des Betroffenen, gerade auch im Hinblick auf die Erwähnung in bereichsspezifischen Gesetzen, zum Beispiel § 22 Landesverfassungsschutzgesetz (LVerfSchG) in Verbindung mit den Richtlinien für die Sicherheitsüberprüfung von Personen im Rahmen des Geheimnisschutzes (SiR MV) und § 6 des Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (SÜG), kein Raum sei.

So entsteht zunächst der Eindruck, als bestehe große Sorge um das informationelle Selbstbestimmungsrecht des einzelnen. Folgt man dieser Auffassung jedoch konsequent, so könnte bereits **eine** Auskunftsperson die Akteneinsicht seitens des Datenschutzbeauftragten "blockieren". Es reicht dabei aus, daß über diese beispielsweise lediglich Name und Anschrift in der Akte des von der Sicherheitsüberprüfung Betroffenen gespeichert sind. Sie muß noch nicht einmal im Rahmen der Sicherheitsüberprüfung befragt worden sein. Obwohl er von seinem Widerspruchsrecht keinen Gebrauch macht, hätte der Überprüfte dann selbst keine Möglichkeit mehr zu erfahren, ob seine Akte den datenschutzrechtlichen Vorschriften genügt. Dies gilt erst recht angesichts der Tatsache, daß es durchaus keine Seltenheit ist, die Daten mehrerer Auskunftspersonen zu **einer** zu überprüfenden Person zu speichern, aber nicht alle zu befragen - so jedenfalls die Praxis der Verfassungsschutzbehörde des Landes Mecklenburg-Vorpommern bis zu meiner Kontrolle.

Ich bin der Auffassung, daß allein die von der Sicherheitsüberprüfung betroffene Person der Akteneinsicht seitens des Landesbeauftragten für den Datenschutz widersprechen kann. Im Sinne des § 24 Abs. 2 Nr. 2 BDSG ist allein sie Betroffener. Dies ergibt sich meines Erachtens bereits aus der Systematik des § 24 BDSG innerhalb des BDSG, denn in diesem Abschnitt sind ausschließlich die Rechte des Datenschutzbeauftragten und nicht die des Betroffenen geregelt. Geht man vom Sinn und Zweck der Vorschrift aus, so schränkt diese die Rechte des Datenschutzbeauftragten ein. Grund für die Einschränkung ist, daß gerade anläßlich von Sicherheitsüberprüfungen eine Vielzahl von äußerst sensiblen Einzelangaben über den Betroffenen gesammelt werden und so über diesen ein vollständiges Persönlichkeitsprofil angefertigt werden kann. Daher kann meines Erachtens ein Widerspruch gegen eine Akteneinsicht nur von der Person erfolgen, über die das Persönlichkeitsprofil erstellt wird; das aber ist nur die sicherheitsüberprüfte Person selbst.

In der Begründung zur Neufassung des Bundesdatenschutzgesetzes ist die oben genannte Problematik nicht ausdrücklich diskutiert worden. Ich schließe jedoch aus den Darlegungen zu § 22 Abs. 2 BDSG (BT-Drucksache 11/4306 vom 06.04.1989, S. 48), auf welche Art und Weise der Hinweis auf das Widerspruchsrecht erfolgen kann, nämlich "in den Hausnachrichten einer Behörde oder durch eine entsprechende Formularrubrik in den Unterlagen für die Einstellung oder für die Sicherheitsüberprüfung", daß allein die sicherheitsüberprüfte Person selbst die Möglichkeit des Widerspruchs gegen die Akteneinsicht durch den Datenschutzbeauftragten haben soll. Denn Auskunfts- und Referenzpersonen sowie Ehepartnern und Lebensgefährten sind die Hausnachrichten der betreffenden Behörde im allgemeinen nicht ohne weiteres zugänglich.

Aufgrund der Tatsache, daß an keiner weiteren Stelle in der Gesetzesbegründung die Definition des Betroffenen näher erläutert wird, ist davon auszugehen, daß der Bundesgesetzgeber eindeutig nur die sicherheitsüberprüfte Person als die Betroffenen angesehen hat.

Ich habe den Innenminister darüber informiert, daß sowohl der Bundesbeauftragte für den Datenschutz als auch meine Kollegen in den Ländern diese Rechtsauffassung teilen.

Um im Interesse der von einer Sicherheitsüberprüfung betroffenen Bürger eine Klärung herbeizuführen, habe ich mich an die Parlamentarische Kontrollkommission und den Innenausschuß des Landtages gewandt und darüber hinaus den Bundesminister des Innern um Stellungnahme gebeten. Der Innenausschuß des Landtages hat über diese Thematik nicht beraten. Der Bundesminister des Innern hat mitgeteilt, daß er ebenfalls meine Auffassung vertritt und in diesem Zusammenhang auf die seinerzeit erarbeiteten Gesetzesmaterialien sowie die mit dem BfD getroffene Abstimmung verwiesen. Daraufhin war unser Innenminister bereit, ebenfalls nach der in den anderen Ländern und im Bund üblichen Praxis zu verfahren. Allerdings hat er mir jüngst mitgeteilt, daß er auch in Zukunft Ehegatten weiter ebenso wie Betroffene belehren wird. Bedauerlicherweise kann daher unter diese seit über einem Jahr andauernde Korrespondenz immer noch kein Schlußstrich gezogen werden.

3. Zum Umfang meiner Kontrollbefugnis

Bei meinem Kontrollbesuch am 31. Mai 1994 wurde mir die Einsichtnahme in Ü3-Sicherheitsüberprüfungsakten durch den Leiter der Verfassungsschutzabteilung unzulässigerweise verwehrt. Erst bei einem zweiten Besuch am 28. November 1994 erhielt ich auch uneingeschränkten Einblick in Ü3-Akten.

Später vertrat der Innenminister die Auffassung, daß wegen der besonderen Sensibilität des Inhalts dieser Akten generell nur eine Einsichtnahme durch mich persönlich in Betracht kommen sollte.

Gemäß § 27 Abs. 1 DSG MV sind alle Stellen, soweit sie der Kontrolle des Landesbeauftragten für den Datenschutz unterliegen, verpflichtet, dem LfD und seinen Mitarbeitern Auskunft zu Fragen zu geben, jederzeit Zutritt zu allen Diensträumen sowie Einsicht in alle Unterlagen zu gewähren, die für den Umgang mit personenbezogenen Daten relevant sind. Eine Reduzierung dieser Kontrollkompetenz auf die Person des LfD und eine damit verbundene Einschränkung der Tätigkeit meiner Behörde ist nur unter den in § 27 Abs. 2 DSG MV genannten Voraussetzungen möglich. Eine Ausübung der in § 27 Abs. 1 DSG MV genannten Rechte durch den Landesbeauftragten für den Datenschutz persönlich ist nur insofern vorgesehen, als die zuständige oberste Landesbehörde **im Einzelfall** feststellt, daß Sicherheitsbelange des Bundes oder der Länder dies gebieten.

Die Reduzierung der Kontrollbefugnis auf die Person des LfD MV stellt eine Beeinträchtigung für die Aufgabenerfüllung meiner Behörde dar. Daher hat der Gesetzgeber hieran sehr hohe Anforderungen geknüpft. Die Einschränkung muß im Einzelfall erforderlich sein. Nicht ausreichend ist die bloße allgemeine Feststellung, sondern vielmehr muß eine Einzelfallprüfung erfolgen. Dabei ist der unbestimmte Rechtsbegriff der Sicherheitsgefährdung eng auszulegen. Eine allgemeine Versagung zu bestimmten Bereichen oder Unterlagen wird durch die Regelung in § 27 Abs. 2 DSG MV nicht gedeckt (Hartmann/Seemann, Datenschutz in Mecklenburg-Vorpommern, 1994, Erl. zu § 27 Abs. 2 DSG MV).

2.5.2. Referentenentwurf zum Sicherheitsüberprüfungsgesetz Mecklenburg-Vorpommern

Zum Referentenentwurf des Sicherheitsüberprüfungsgesetzes Mecklenburg-Vorpommern habe ich am 26.September 1995 Stellung genommen. Einige wesentliche Aspekte stelle ich im folgenden auszugsweise vor.

Kritisiert habe ich, daß in dem Entwurf neben "Erkenntnissen" auch "Sachverhalte" als sicherheitserheblich angesehen werden können. Nach allgemeinem Sprachgebrauch beinhalten Erkenntnisse schon eine gewisse Verdichtung von Umständen, die auf etwas schließen lassen; der Begriff Sachverhalt ist jedoch so umfassend, daß darunter die Verwertung einer Vielzahl von Daten gemeint sein kann. Nach meiner Auffassung wird damit unzulässigerweise in das Recht auf informationelle Selbstbestimmung eingegriffen.

Unüberschaubar ist für den Betroffenen ebenfalls der erwähnte Kreis sogenannter "anderer geeigneter Personen oder Stellen", die anläßlich der Sicherheitsüberprüfung befragt werden können. Dieses ist mit den im Volkszählungsurteil aufgestellten Grundsätzen nicht vereinbar. Danach muß der Bürger wissen, "wer was wann bei welcher Gelegenheit über ihn weiß" (vgl. Entscheidung des Bundesverfassungsgerichtes Band 65, S. 1 ff.). Dies hat auch Auswirkungen auf die von dem Betroffenen abzugebende Einwilligung. Die Wirksamkeit einer Einwilligungserklärung hängt bekanntlich davon ab, ob der Betroffene unter anderem über Art und Umfang der Erhebung von Daten ausreichend aufgeklärt ist.

Des weiteren habe ich die im Referentenentwurf beschriebene Maßnahme "Sicherheitsmäßige Bewertung der Angaben in der Sicherheitserklärung unter Berücksichtigung der Kenntnisse der Verfassungsschutzbehörde des Bundes und der Länder" kritisiert. Dahinter verbirgt sich unter anderem die Ermächtigung der Abteilung für Verfassungsschutz, bei dem von den Verfassungsschutzbehörden betriebenen Verbundsystem NADIS anzufragen, ob Erkenntnisse über den Betroffenen, dessen Ehegatten, Lebensgefährten, Auskunfts- oder Referenzpersonen vorliegen. Diese Verfahrensweise ist insbesondere im Hinblick auf die Abfrage der genannten Personen (mit Ausnahme des Betroffenen) nicht mit dem Recht auf informationelle Selbstbestimmung vereinbar. Einschränkungen dieses Rechts bedürfen grundsätzlich "einer (verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und damit dem rechtsstaatlichen Gebot der Normenklarheit entsprechen" (vgl. Entscheidung des Bundesverfassungsgerichtes Band 65, S. 1 ff). Aufgrund der hier gewählten Formulierung ist jedoch beispielsweise einer Auskunftsperson völlig unklar, daß die Verfassungsschutzbehörde auch sie verfassungsschutzmäßig in NADIS "abklärt".

Ebenfalls ergibt sich aus dem Gesetzestext nicht, daß der Grundsatz der Verhältnismäßigkeit beachtet wird. Darauf wird zwar in der Gesetzesbegründung mit den Worten "im Bedarfsfall" verwiesen. Die Erwähnung in der Gesetzesbegründung reicht jedoch aus meiner Sicht keinesfalls aus. Ich habe daher aus Gründen der Transparenz des Verfahrens empfohlen, NADIS-Abfragen hinsichtlich des Ehegattens, Lebenspartners, der volljährigen Personen, Eltern, Auskunfts- und Referenzpersonen etc. von deren Einwilligung abhängig zu machen und den Gesetzestext entsprechend präzise zu formulieren.

Des weiteren habe ich die Formulierung in der Sicherheitserklärung, wonach der Betroffene die Funktion in einer Partei oder Massenorganisation der ehemaligen DDR anzugeben hat, kritisiert. Aus datenschutzrechtlicher Sicht ist die undifferenzierte Frage nach "Funktionen" und "Massenorganisationen" bedenklich. Der Betroffene weiß nicht, ob eine haupt- oder ehrenamtliche Funktion gemeint ist; er weiß ebenfalls nicht, welche Massenorganisationen er anzugeben hat. Festzustellen ist, daß es eine Reihe von Massenorganisationen (und Funktionen in diesen) gab, die für die Sicherheitsüberprüfung einer Person nicht relevant sind. Ich habe daher empfohlen, bei den Funktionen zwischen haupt- und ehrenamtlichen zu differenzieren und Massenorganisationen abschließend aufzuzählen.

Von Betroffenen zu benennende Referenzpersonen geben zumeist sehr detailliert zu dessen Persönlichkeit und Lebenswandel Auskunft. Deshalb sollte er zu einem frühestmöglichen Zeitpunkt in die Befragung einwilligen. So könnte er gleichzeitig mit dem Fragebogen zur Sicherheitserklärung entsprechende Einwilligungsvordrucke erhalten.

In dem Gesetzentwurf war des weiteren vorgesehen, daß die zuständige Stelle (also die Stelle, bei der der Bedienstete beschäftigt ist) Informationen über die persönlichen, dienstlichen und arbeitsrechtlichen Verhältnisse der eine sicherheitsempfindliche Tätigkeit ausübenden Person zur Sicherheitsakte zu nehmen hat. Dazu zählen insbesondere auch "geistige oder seelische Störungen sowie Alkohol-, Drogen- oder Tablettenmißbrauch". Die generelle Speicherung derartiger Informationen halte ich für bedenklich, da grundsätzlich nur der Arzt feststellen kann und darf, ob eine geistige oder seelische Störung bzw. ein Mißbrauch von Alkohol, Drogen oder Tabletten vorliegt. Soweit ein solcher Mißbrauch nicht von medizinischer Seite diagnostiziert wurde, bewegt sich eine derartige Feststellung im Bereich der laienhaften Vermutun-

gen, die für den Betroffenen freilich von einschneidender Bedeutung sein könnte. Ich habe empfohlen, diese Regelung ersatzlos zu streichen.

Besonders wichtig für den Betroffenen ist die Ausgestaltung des Auskunfts- bzw. Akteneinsichtsrechts. Laut Gesetzentwurf soll der Sicherheitsüberprüfte lediglich das Recht erhalten, in die Sicherheitsakte, die im wesentlichen nur den von ihm selbst ausgefüllten Fragebogen enthält, aber nicht in die Sicherheitsüberprüfungsakte, die bei der Abteilung für Verfassungsschutz geführt wird, einzusehen. Und selbst in die Sicherheitsakte soll er nur einsehen können, "soweit eine Auskunft für die Wahrnehmung der rechtlichen Interessen nicht ausreicht". Eine derart restriktive Handhabung des Auskunfts- und Akteneinsichtsrechts ist mit dem Recht auf informationelle Selbstbestimmung nicht zu vereinbaren. Die Akteneinsicht ist eine wesentliche Voraussetzung für die Ausübung dieses Rechtes. Sie sollte daher unter den gleichen Voraussetzungen gewährt werden wie die Auskunft. Ich habe daher empfohlen, das Akteneinsichtsrecht analog den Voraussetzungen für die Auskunft zu gewähren.

Ein überarbeiteter Gesetzentwurf steht noch aus.

2.5.3. Auskunftserteilung durch den Verfassungsschutz

Ein Bürger, der von der Verfassungsschutzbehörde im Rahmen einer Sicherheitsüberprüfung als Referenzperson befragt worden war, wollte wissen, welche Daten zu seiner Person gespeichert worden sind. Er bat um die Übersendung einer Kopie bzw. um Einsichtnahme in die ihn betreffenden Unterlagen. Der Befragte begründete seine Bitte damit, daß ihm nicht bekannt gewesen sei, daß ein schriftlicher Befragungsvermerk angefertigt wird und er nicht wisse, ob die von ihm getroffenen Aussagen korrekt wiedergegeben worden seien.

Unser Innenminister hatte dem Betroffenen mitgeteilt, daß er seinem Schreiben ein über das allgemeine Auskunftsinteresse hinausgehendes **besonderes Interesse** nicht entnehmen könne und eine Einsichtnahme daher nicht in Frage käme. Ferner seien in dem Befragungsvermerk "keine negativen Angaben über Sie [ihn]" enthalten.

Der Petent hat sich daraufhin an mich gewandt und um Unterstützung gebeten. Ich habe den Sachverhalt geprüft und bin zu dem Ergebnis gekommen, daß dem Petenten ein Anspruch auf Auskunftserteilung gemäß § 22 LVerfSchG zusteht. Er hat einen schriftlichen Antrag gestellt und auf einen konkreten Sachverhalt, nämlich die Befragung im Rahmen der Sicherheitsüberprüfung, hingewiesen. Einer näheren Prüfung bedurfte allein die Darlegung des "besonderen Interesses". Fraglich war demnach also, ob die Begründung ausreicht, daß in dem schriftlich angelegten Befragungsvermerk Aussagen enthalten sein könnten, die er so nicht gemacht hatte, oder daß dort Daten enthalten sein könnten, die so nicht zutreffend sind.

Im Gegensatz zu anderen Gesetzen, wonach ein "berechtigtes" oder "rechtliches" Interesse oder auch gar kein Interesse dargelegt werden muß, ist beim Verfassungsschutz ein "besonderes Interesse" erforderlich. Dies wird zum Teil damit begründet, daß der Verfassungsschutz in weiten Bereichen notwendigerweise darauf angelegt ist, im Geheimen zu arbeiten und daher nicht jedem ohne weiteres Auskunft geben kann. Im vorliegenden Fall ist jedoch zu berücksichtigen, daß die anfragende Person nicht etwa im Verdacht steht, sich im extremistischen Bereich zu betätigen, sondern es geht darum, von einer dritten Person Auskünfte zu einem öffentlich Bediensteten zu erhalten, der mit einer sicherheitsempfindlichen Tätigkeit betraut werden soll.

Die Mitwirkung von Auskunfts- und Referenzpersonen im Rahmen von Sicherheitsüberprüfungen erfolgt auf freiwilliger und von gegenseitigem Vertrauen geprägter Basis. Es sind somit auf gesetzlicher Ebene besondere Anforderungen an die Einwilligung sowie an die Aufklärung der jeweiligen Person über Art und Umfang des Umgangs mit ihren Daten aufzustellen. Hat jemand seine personenbezogenen Daten freiwillig preisgegeben, so ist ihm meines Erachtens allein schon aus dieser Tatsache ein "besonderes Interesse" an der Auskunft zuzuerkennen.

Der Bundestag (BT) hat sich anläßlich der Beratung der Tätigkeitsberichte des Bundesbeauftragten für den Datenschutz unter anderem auch zur Frage der Auskunftserteilung des Bundesamtes für Verfassungsschutz (BfV) geäußert und auf Empfehlung des Innenausschusses folgenden Entschluß gefaßt (BT-Drs. 12/4094): "Der Deutsche Bundestag empfiehlt der Bundesregierung, bei der Anwendung des § 15 Bundesverfassungsschutzgesetz (BVerfSchG) ... an die Darlegung eines konkreten Sachverhaltes und eines besonderen Interesses an der Auskunft keine zu strengen Anforderungen zu stellen." (Anmerkung: Die Auskunftserteilung an die anfragende Person gemäß § 22 LVerfSchG ist entsprechend § 15 BVerfSchG geregelt.)

Den Hinweis an den Petenten, daß keine negativen Angaben über ihn bzw. die sicherheitsüberprüfte Person in den Akten gespeichert seien, halte ich in keiner Weise für geeignet, die Befürchtungen des Betroffenen auszuräumen. Denn es kommt nicht darauf an, daß aus der Sicht der Behörde, die zu einer Person Daten gespeichert hat, Daten als "negativ" eingestuft werden. Entscheidend ist aus datenschutzrechtlicher Sicht vielmehr, daß

1. die Behörde die Daten zur rechtmäßigen Erfüllung einer ihr obliegenden Aufgabe benötigt,
2. sie in dem vorhandenen Umfang zur Aufgabenerfüllung erforderlich sind und
3. die Daten vollständig und richtig sind.

Und gerade im Hinblick auf die Richtigkeit der Daten hatte der Petent Zweifel geäußert.

Ich habe den Innenminister auch auf die Praxis des BfV verwiesen, wonach ein "besonderes Interesse" an einer Auskunft bereits dann gegeben ist, wenn der Betroffene glaubhaft Umstände vorträgt, aus denen sich ein über das grundsätzlich jedem Auskunftsbegehren zu unterstellende allgemeine Interesse an einer Auskunft hinausgehendes Interesse ergibt. Aus alledem folgt, daß die von der anfragenden Person dargelegten Gründe für die Auskunft bzw. Akteneinsicht den Anforderungen, die an das "besondere Interesse" zu stellen sind, genügen.

Der Innenminister ist zwar meinen rechtlichen Erwägungen nicht gefolgt. Im Ergebnis hat er jedoch in der Sache dem Petenten - ohne Anerkennung der Rechtspflicht - den Inhalt des Befragungsvermerkes zur Kenntnis gegeben.

2.6. Stasi-Unterlagen - Outen ehemaliger Kreistagsmitglieder

Ein Kreistagsmitglied hat mich gebeten, den Umgang des Kreistages mit den Ergebnissen der Anfrage beim Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (Bundesbeauftragter) zu prüfen.

Der Präsident des Kreistages hatte als Vorsitzender eines gewählten Ausschusses, der die Bescheide des Bundesbeauftragten auswerten sollte, im nichtöffentlichen Teil einer Kreistagssitzung aus diesen vorbehaltlos zitiert. Dabei wurden unter anderem auch Namen und Untersuchungsergebnisse von ehemaligen Kreistagsmitgliedern bekanntgegeben.

Im Stasi-Unterlagen-Gesetz ist festgelegt, unter welchen Voraussetzungen öffentliche Stellen Überprüfungen durch den Bundesbeauftragten vornehmen lassen können. In welcher Form jedoch eine Auswertung dieser Unterlagen und der Prüfungsergebnisse durch die öffentlichen Stellen erfolgen darf, ist dort nicht bestimmt. Gleichwohl sind auch hier die allgemeinen Grundsätze der Zweckbindung und der Verhältnismäßigkeit zu beachten. Insbesondere ist bei jedem Verfahren eine Abwägung zwischen dem öffentlichen Interesse an der Aufarbeitung der Vergangenheit des Staatssicherheitsdienstes der ehemaligen DDR einerseits und den schutzwürdigen Belangen der jeweiligen Person andererseits erforderlich. Dies setzt eine umfassende Einzelfallprüfung unter Beteiligung des überprüften Kreistagsmitgliedes voraus. Eine generelle Bekanntgabe der Prüfungsergebnisse ohne Berücksichtigung dieser Grundsätze erachte ich als unzulässig. Darauf habe ich bereits in meinem Ersten Tätigkeitsbericht hingewiesen. Ich habe daher empfohlen, bereits vor Antragstellung beim Bundesbeauftragten diesbezügliche Verfahrensregelungen zu treffen.

Diese und ähnliche Sachverhalte habe ich zum Anlaß genommen, um "Hinweise für den Umgang mit Gauck-Bescheiden von Mitgliedern kommunaler Vertretungskörperschaften" (Amtsblatt M-V 1994, S. 260) zu geben.

Im vorliegenden Fall war zwar zu berücksichtigen, daß die Überprüfungsergebnisse in nichtöffentlicher Sitzung genannt wurden und die Mitglieder des Kreistages der Verschwiegenheitspflicht unterliegen. Jedoch war es nicht erforderlich, die Überprüfungsergebnisse von ehemaligen Kreistagsmitgliedern mitzuteilen und aus den Bescheiden des Bundesbeauftragten zu zitieren. Die betroffenen Personen waren aus ihrer Tätigkeit als Kreistagsmitglieder bereits ausgeschieden. Es bestand somit keinesfalls ein öffentliches Interesse, das ein solches Verfahren rechtfertigte. Das Überprüfungsverfahren hätte mit dem Ausscheiden dieser Personen aus dem Kreistag eingestellt werden müssen. Insoweit lag ein unzulässiger Eingriff in das Recht auf informationelle Selbstbestimmung dieser Personen vor.

Ich habe den Kreistagspräsidenten über die Rechtslage informiert und empfohlen, künftig entsprechend den Hinweisen des Landesbeauftragten für Mecklenburg-Vorpommern für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR und meiner Behörde zu verfahren.

2.7. Einwohnerwesen

2.7.1. Novellierung des Landesmeldegesetzes

Im Rahmen der Novellierung des Landesmeldegesetzes (LMG) habe ich gegenüber dem Innenministerium zum Referentenentwurf Stellung genommen. Im wesentlichen beinhaltet der Entwurf die nach der Änderung des Melderechtsrahmengesetzes erforderlichen Anpassungen.

Ich habe darauf hingewiesen, daß in § 24 Abs. 6 Satz 2 Wehrpflichtgesetz (WPflG) für Wehrpflichtige, die nach der Vollendung des 32. Lebensjahres noch der Wehrüberwachung unterliegen, nunmehr eine eigenständige Meldepflicht gegenüber dem Kreiswehrersatzamt festgelegt wurde. Die Aufgabe der Meldebehörden, diese Daten zu speichern sowie an die zuständigen Kreiswehrersatzämter zu übermitteln, ist somit entfallen.

§ 3 Abs. 2 Nr. 4 LMG ist daher zu streichen. Folglich haben die Meldebehörden dieses Merkmal zu löschen.

Wer in Beherbergungsstätten des Landes übernachtet, hat einen besonderen Meldeschein auszufüllen. Für die Nutzung dieser Meldescheine durch bestimmte Behörden sind in § 29 LMG Beschränkungen festgelegt worden. Im Entwurf ist vorgesehen, die Aufgaben, für die diese Daten genutzt werden dürfen, genau festzulegen. Diese Konkretisierung ist zu begrüßen. Darüber hinaus ist jedoch zu berücksichtigen, daß im Rahmen der Aufgabenerfüllung durch die Behörde auch der Grundsatz der Verhältnismäßigkeit zu beachten ist. Die Daten dürfen hiernach für die Aufgabenerfüllung nicht nur dienlich, sondern müssen im konkreten Fall erforderlich sein. Ich habe daher empfohlen, eine Ergänzung des Entwurfs um die Regelung "soweit dies im Einzelfall erforderlich ist" vorzunehmen.

Die Landesregierung hat inzwischen den Entwurf eines Ersten Gesetzes zur Änderung des Landesmeldegesetzes (LT-Drucksache 2/1038) in den Landtag eingebracht.

2.7.2. Darf die GEZ die Daten aller Einwohner bekommen?

Bereits im ersten Berichtszeitraum hatte ich mich mit der Frage zu befassen, ob regelmäßig Meldedaten aller Einwohner an die gemeinsame Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten (GEZ) übermittelt werden dürfen, um "Schwarzseher" und "-hörer" festzustellen. Am 17. Februar 1995 fand dazu eine Beratung beim Norddeutschen Rundfunk (NDR) statt, an der Vertreter des NDR, der GEZ, der Regierungen der NDR-Staatsvertragsländer Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein sowie die zuständigen Landesdatenschutzbeauftragten teilnahmen. Im Ergebnis dieser Sitzung wird der NDR die auf der derzeitigen Rechtslage bestehenden Möglichkeiten zur Ermittlung der "Schwarzseher" und "-hörer" ausschöpfen und die Erfahrungen in einem Bericht niederlegen. Sobald dieser vorliegt, soll eine weitere Beratung stattfinden.

Bei einer generellen Datenübermittlung wäre eine Unterscheidung zwischen Daten, die zur Feststellung von "Schwarzsehern" und "-hörern" benötigt werden, und solchen, die dafür nicht erforderlich sind, nicht möglich. Dies würde gegen den verfassungsrechtlich garantierten Verhältnismäßigkeitsgrundsatz verstoßen.

Das Ausmaß der zu erwartenden Mehreinnahmen bei einer regelmäßigen Datenübermittlung ist stark umstritten. Deshalb habe ich in dieser Sitzung darauf aufmerksam gemacht, daß es wichtig ist darzulegen, welche Einnahmen durch diese zusätzliche Maßnahme tatsächlich erzielt werden. Als Beispiel verwies ich auf die Diskrepanz zwischen der Prognose des Jarass-Gutachtens von 1992, das für das Jahr 1994 mit Mehreinnahmen des Westdeutschen Rundfunks (WDR) durch regelmäßige Datenübermittlung von 69,5 Millionen DM rechnet, zu den tatsächlich von WDR und Hessischen Rundfunk (HR) erzielten 23 Millionen DM. Daher stellt sich die Frage, ob die nach Aussage des NDR zu erwartenden Mehreinnahmen in Höhe von 10 Millionen DM für den NDR unter Umständen nach unten korrigiert werden müssen, was bei der Verhältnismäßigkeit einer erweiterten Datenübermittlung zu berücksichtigen wäre.

Darüber hinaus ist zu bedenken, daß nach Angaben des Niedersächsischen Landesbeauftragten für den Datenschutz selbst der WDR durch die dort zulässige regelmäßige Datenübermittlung die Anmeldequote von bisher 90 % um maximal 2 % erhöhen konnte.

Auch müßte zunächst einmal sichergestellt sein, daß der NDR tatsächlich die verschiedenen Möglichkeiten der Datenerhebung und der Pflege seines Datenbestandes nutzt.

Sollte sich trotz Ausschöpfung aller verfügbaren Mittel ein nicht mehr vertretbarer Einnahmeausfall des NDR ergeben, so sind bei der Suche nach Lösungsansätzen vor allem folgende Aspekte zu berücksichtigen:

- Es muß sowohl durch Rechtsvorschriften als auch durch die Gestaltung des Verfahrens gewährleistet sein, daß unbeteiligte Bürger so wenig wie möglich betroffen werden. Dabei ist sicherzustellen, daß Unbeteiligte möglichst schon bei der Datenerhebung, spätestens aber bei der Datenverarbeitung zuverlässig ausgeschieden werden können. Unbeteiligt sind nicht nur diejenigen, die kein Radio- und/oder Fernsehgerät zum Empfang bereithalten, sondern auch Ehegatten und nichteheliche Partner von angemeldeten Rundfunkteilnehmern sowie volljährige Kinder ohne eigenes Einkommen. Mir ist beispielsweise nicht ersichtlich, wie gewährleistet werden kann, daß nicht-gebührenpflichtige Lebenspartner bei einem regelmäßigen Datenabgleich erkannt und nicht von der GEZ angeschrieben werden.

- Das zu entwickelnde Verfahren muß wirksame Maßnahmen vorsehen, um fehlerhafte Zuordnungen der Daten beim Abgleich zu minimieren.

- Der Zweck einer erweiterten Datenerhebung muß präzise festgelegt werden. Dabei sind zwei Bereiche zu unterscheiden: einmal die Pflege des Datenbestandes der GEZ, um Fehler bei melderechtlichen Vorgängen zu korrigieren und jederzeit über einen aktuellen Datenbestand zu verfügen, zum anderen die Möglichkeit, bisherige "Schwarzseher" und -"hörer" zur Kasse zu bitten. Dementsprechend sollte auch der zu erwartende Mehrbetrag durch die einzelnen Maßnahmen differenziert werden.

  Ich werde weiterhin an Beratungen zu diesem Thema teilnehmen und mich für die Berücksichtigung der datenschutzrechtlichen Belange einsetzen.

2.7.3. Auskunft trotz Auskunftssperre?

Von einem Einwohnermeldeamt erhielt ich verschiedene Anfragen zu den Rechtsfolgen einer melderechtlichen Auskunftssperre. So wollte die Behörde unter anderem wissen, unter welchen Umständen sie gesetzlichen Krankenkassen oder Rechtsanwälten Auskunft über die Adresse einer Person erteilen darf, für die eine Auskunftssperre in das Melderegister eingetragen ist, und in welcher Form eine Auskunft bei Bestehen einer Auskunftssperre abgelehnt werden sollte.

Grundsätzlich kann jedem Auskunftsersuchenden der Name und die Anschrift jeder Person mitgeteilt werden. Eine Melderegisterauskunft ist jedoch unzulässig, "wenn der Betroffene der Meldebehörde das Vorliegen von Tatsachen glaubhaft gemacht hat, die die Annahme rechtfertigen, daß ihm oder einer anderen Person hieraus eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann" (§ 34 Abs. 5 LMG). Diese Auskunftssperre gilt gegenüber jedermann, unabhängig davon, welche Stellung er zu dem Betroffenen hat. Mit "jedermann" ist jede Privatperson und jede nicht-öffentliche Stelle gemeint. Einer öffentlichen Stelle darf die Meldebehörde Daten über eine Person übermitteln, für die eine Auskunftssperre im Melderegister eingetragen ist, sofern dies zur Erfüllung von Aufgaben der Meldebehörde oder der öffentlichen Stelle erforderlich ist.

Gesetzliche Krankenkassen sind öffentlich-rechtliche Körperschaften des Bundes oder eines Landes und somit öffentliche Stellen. Ihnen dürfen daher die zu ihrer Aufgabenerfüllung erforderlichen Meldedaten, unabhängig vom Bestehen einer Auskunftssperre, übermittelt werden.

Rechtsanwälte sind zwar Organe der Rechtspflege, haben aber dennoch nicht den Status einer öffentlichen Stelle, auch wenn sie in ihrer Funktion als Anwalt die Meldeauskunft im Interesse eines Mandanten begehren. Eine Auskunftssperre gilt daher auch gegenüber Rechtsanwälten. Folglich ist auch die gerichtliche Geltendmachung zivilrechtlicher Forderungen nicht möglich, da im Zivilprozeß der Kläger die ladungsfähige Anschrift des Beklagten beizubringen hat. Sollte die Meldebehörde Anhaltspunkte dafür haben, daß der Betroffene die für ihn eingetragene Auskunftssperre mißbräuchlich nutzt, um sich dem berechtigten Zugriff bestimmter Personen, etwa Gläubigern, zu entziehen, so hat sie erneut zu prüfen, ob die Voraussetzungen für die Auskunftssperre noch vorliegen, und gegebenenfalls hierüber neu zu entscheiden. Bei dieser Prüfung hat sie einen strengen Maßstab anzulegen. Lediglich im Strafverfahren ermittelt das Gericht oder die Staatsanwaltschaft von Amts wegen die Anschrift und erhält von der Meldebehörde trotz Auskunftssperre die erforderlichen Daten.

Eine weitere Frage war, in welcher Form die Einwohnermeldeämter Auskunftsersuchen ablehnen sollen, wenn eine Auskunftssperre, insbesondere wegen Gefahr für Leben und Gesundheit, vorliegt.

Lehnt die Meldebehörde die Auskunft mit der Begründung ab, daß eine Auskunftssperre besteht, so offenbart sie dem Auskunftsersuchenden, daß der Betroffene bei ihr registriert ist. Dies kann insbesondere in kleineren Gemeinden dazu führen, daß der Betroffene vom Anfragenden leicht ermittelt werden kann. Um dies zu verhindern, sollte das Einwohnermeldeamt in seiner Antwort offen lassen, ob der Betroffene bei ihm registriert ist und eine Auskunftssperre besteht oder ob er überhaupt nicht bei ihm gemeldet ist.

Die Beantragung einer Auskunftssperre ist ein Schutzrecht. Seine Geltendmachung darf daher nicht - wie in einem anderen Bundesland geschehen - von einer Gebühr abhängig gemacht werden. Die einschlägige Gebührenordnung von Mecklenburg-Vorpommern sieht deshalb auch keine Gebühr für die Eintragung einer Auskunftssperre in das Melderegister vor.

2.7.4. Asylcard

Für Asylbewerber ist vorgesehen, eine multifunktionale Chipkarte, die sogenannte Asylcard, einzuführen. Sie soll nicht nur Daten aus allen Lebensbereichen des Asylbewerbers, sondern auch Fingerabdrücke und Lichtbild enthalten. Als Einsatzbereiche sind Identitäts- sowie Zugangs- und Aufenthaltskontrollen, Speicherung von Verfahrensdaten, der Empfang von Sach- und Unterstützungsleistungen geplant, wobei diese Aufzählung nicht abschließend ist.

Damit die Asylcard ihre Funktion erfüllen kann, müssen die gespeicherten Daten auf dem aktuellen Stand gehalten werden. Dies führt dazu, daß der Asylbewerber in einem ständigen "check up" seine jeweilige Lebenssituation preisgeben muß. Das gesamte Verfahren ist von der Vermutung geprägt, der Asylbewerber wolle grundsätzlich betrügen, und dem sei vorzubeugen.

Informationsrechte für den Betroffenen sind bei der Einführung der Asylcard überhaupt nicht geplant. Aber auch der Asylbewerber muß eine Möglichkeit haben zu erfahren, welche Daten über ihn gespeichert sind.

Die Zusammenführung von verschiedenartigen Daten aus dem Arbeitsbereich mehrerer Behörden auf einer Chipkarte ermöglicht es, vollständige Persönlichkeitsprofile zu erstellen. Dies stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung dar, das auch Ausländern zusteht. Einschränkungen dieses Rechtes dürfen nur im überwiegenden Interesse der Allgemeinheit erfolgen und sind an bestimmte Voraussetzungen gebunden. Hier ist insbesondere die Zweckbindung zu nennen. Sie besagt, daß die Rechtsgrundlage für den Umgang mit den Daten eine präzise Angabe des Verwendungszwecks enthalten muß. Mit der Einführung der Asylcard wird jedoch eine Vielzahl unterschiedlicher Zwecke verfolgt. Multifunktionale Datenverwendung muß auf ein gesetzlich definiertes Mindestmaß beschränkt sein, denn bei jedem Grundrechtseingriff ist der Grundsatz der Verhältnismäßigkeit zu beachten. Das bedeutet, daß jede staatliche Maßnahme geeignet, erforderlich und für den Betroffenen zumutbar sein muß. Der Einsatz der Asylcard mag zwar geeignet sein, um Asylmißbrauch zu verhindern, jedoch bestehen Zweifel an der Erforderlichkeit und Zumutbarkeit. Das rechtsstaatliche Gebot der Erforderlichkeit ist verletzt, wenn das Ziel der staatlichen Maßnahme auch durch ein anderes - gleich wirksames Mittel - erreicht werden kann, das das betreffende Grundrecht weniger einschränkt. Deshalb wäre zunächst einmal zu untersuchen, ob sich die Verhütung des Asylmißbrauchs nicht schon durch Beseitigung von Defiziten im bereits bestehenden Verfahren erreichen ließe.

Aus Gründen der Datensicherung müßten die auf der Asylcard gespeicherten Daten in ein Datenverarbeitungssystem eingespeichert werden. Dies würde faktisch dazu führen, daß neben dem AZR und der Asyl Online Datei des Bundesamtes für die Anerkennung ausländischer Flüchtlinge (ASYLON) eine weitere Datenbank entstehen würde, die alle relevanten Daten über diesen Personenkreis enthält. Es entstehen also alle Risiken einer zentralen Vollerfassung von personenbezogenen Daten, wie etwa gesteigerte Mißbrauchsmöglichkeiten.

Auch das Argument, mit der Asylcard ließen sich die Kosten des Asylverfahrens reduzieren, halte ich nicht für schlüssig. Die Einführung würde eine bundesweite Errichtung von personeller und technischer Infrastruktur erfordern. Einige Landesbeauftragte für den Datenschutz haben schon auf die hohen Einführungskosten und die technischen Schwierigkeiten (z. B. Verschlüsselung der Daten, Bereitstellung der notwendigen Hardware) hingewiesen.

Der Innenminister unseres Landes erwägt, sich an einer "Machbarkeitsstudie" zu beteiligen, in der der Einsatz der Asylcard in einigen Bundesländern getestet werden soll. Ich habe meine Bedenken mitgeteilt und empfohlen, unter diesen Voraussetzungen auf die Teilnahme zu verzichten.

2.7.5. Bürgerkriegsflüchtlinge - Objekt staatlicher Ausforschung

Auf der Konferenz der Innenminister im Mai 1994 wurde unter dem Stichwort "Mißbrauchsverhütung" darüber diskutiert, ob Verfahrens- und Leistungsregelungen, die im Asylverfahren gelten, auch auf Bürgerkriegsflüchtlinge angewendet werden sollen. Dazu würde dann auch die volle erkennungsdienstliche Behandlung (ED-Behandlung) dieses Personenkreises gehören. Es wurde beschlossen, die Bundesregierung aufzufordern, eine entsprechende Änderung des Ausländergesetzes auf den Weg zu bringen und die bis zu diesem Zeitpunkt bestehenden Regelungen voll auszuschöpfen. Nur das Land Hessen hielt die geplante generelle ED-Behandlung von Bürgerkriegsflüchtlingen für bedenklich. Die gleichen Zweifel hatte bereits die Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. Februar 1992.

Ich halte die angestrebte Vorgehensweise für nicht vereinbar mit dem in der Verfassung garantierten Grundsatz der Verhältnismäßigkeit. Der Staat hat selbstverständlich das Recht zu wissen, mit wem er es zu tun hat und ob staatliche Leistungen mißbraucht werden. Daher muß sich jeder - ob Ausländer oder Deutscher - durch Dokumente ausweisen können. Nur wenn Zweifel an der Identität einer Person bestehen, dürfen ED-Maßnahmen durchgeführt, das heißt Fingerabdrücke und Lichtbilder angefertigt werden. Dieser Grundsatz muß auch für Bürgerkriegsflüchtlinge gelten. Für Asylbewerber wurde dieser rechtsstaatliche Grundsatz bereits durch das Asylverfahrensgesetz eingeschränkt. Diese müssen sich, sofern sie älter als 14 Jahre sind, stets erkennungsdienstlich behandeln lassen, sobald sie ihren Asylantrag stellen.

Selbst bei umfangreichen Überwachungsmaßnahmen kann ein Mißbrauch von staatlichen Zuwendungen nicht vollständig ausgeschlossen werden. Nach einer Antwort unserer Landesregierung auf eine Kleine Anfrage (LT-Drucksache 2/1060) haben 14, 1 % der Asylbewerber in Mecklenburg-Vorpommern gegen das Ausländer - oder Asylverfahrensgesetz verstoßen. Trotzdem wird das komplette erkennungsdienstliche Verfahren auf alle Asylbewerber angewandt und es soll auf die Bürgerkriegsflüchtlinge erweitert werden.

Ich habe deshalb unseren Innenminister gebeten, sich dafür einzusetzen, daß bei Bürgerkriegsflüchtlingen erst bei Anzeichen von Leistungsmißbrauch ED-Maßnahmen durchgeführt werden. Ferner habe ich bezweifelt, daß Abdrücke von allen zehn Fingern erforderlich sind, da ein einzelner Fingerabdruck zur Identifizierung ausreicht. Der Betroffene würde, auch wenn er kein Gesetz verletzt hat, genauso behandelt werden wie ein Straftäter.

Die Antwort des Innenministers macht deutlich, daß das gesamte Verfahren von latentem Mißtrauen gegenüber Asylbewerbern und Bürgerkriegsflüchtlingen geprägt ist.

Zunächst wird festgestellt, daß Dokumente für diese Personengruppe zur Identitätsfeststellung nicht ausreichten, weil sie gefälscht sein könnten. Ferner würden den Antragstellern nach Ablehnung ihres Antrages sehr häufig die Ausweispapiere "abhandenkommen", so daß nur Fingerabdrücke und Fotografien die Identität beweisen könnten. Die ED-Behandlung diene der Aufklärung und der Prävention des Leistungsmißbrauchs. Ein Identitätswechsel, verbunden mit einem "regen Wanderleben", um Sozialhilfe zu erlangen, sei anders nicht zu unterbinden. Auch die Erfassung aller zehn Fingerabdrücke sei notwendig. Würde nur ein Fingerabdruck genommen, sei es für die Antragsteller leichter, den Finger zu beschädigen, um einer Identifizierung zu entgehen. Dann sei ein "Zugriff auf nichtbeschädigte Finger" nicht mehr möglich. Das Abnehmen aller Fingerabdrücke sei aufgrund des nur unerheblichen Zeitaufwandes durchaus zuzumuten. Im übrigen unterlägen Asylbewerber und Bürgerkriegsflüchtlinge zahlreichen anderen Zwangsmaßnahmen und würden deshalb dieser Erfassung nur eine untergeordnete Bedeutung beimessen. Aus diesen Gründen sei meine Kritik übertrieben und unangemessen.

Das Argument, man könne ohne ED-Behandlung nicht feststellen, ob Ausweispapiere gefälscht sind, gilt für jede Ausweiskontrolle, auch bei deutschen Staatsbürgern. Da nur ein geringer Anteil der Antragsteller staatliche Leistungen mißbraucht bzw. sich unberechtigt in der Bundesrepublik aufhält, ist ein solch massiver Einsatz des Erkennungsdienstes nicht notwendig. Gerade die ED-Maßnahmen stellen einen tiefen Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen dar, der nur in Ausnahmefällen vorgenommen werden darf. Die Tatsache, daß die Flüchtlinge nach ihrer Antragstellung "schwerwiegendere Sorgen haben, als die Abnahme von Fingerabdrücken", ist keine Rechtfertigung für die ED-Maßnahmen. Die Feststellung, daß Antragsteller sich ihre Fingerkuppen verstümmeln würden, um nicht erkannt zu werden oder um staatliche Leistungen zu mißbrauchen, ist schon sehr bedenklich.

Ich empfehle allen am Verfahren Beteiligten, die bereits bestehende ED-Behandlung von Asylbewerbern zu überdenken und diese Praxis keinesfalls auf Bürgerkriegsflüchtlinge auszuweiten.

2.7.6. Zurück nach Vietnam

Aus Pressemitteilungen im Juli 1995 habe ich vom Rückübernahmeabkommen zwischen der Bundesrepublik Deutschland und der Sozialistischen Republik Vietnam erfahren. Daraufhin habe ich den Innenminister unseres Landes gebeten, mich über die datenschutzrechtlichen Aspekte dieses Abkommens zu informieren.

Das Rückübernahmeabkommen enthält Verfahrensregelungen zur Rückführung von vietnamesischen Staatsbürgern, die nicht im Besitz einer gültigen Aufenthaltserlaubnis sind. Zu diesem Zweck werden Daten der betroffenen Personen an die vietnamesischen Behörden übermittelt, aus denen sich einwandfrei deren Identität ergibt. Die Behörden prüfen, ob es sich bei den aufgeführten Personen tatsächlich um vietnamesische Staatsbürger handelt und somit eine Einreise erfolgen darf. Auf Initiative des vietnamesischen Staates wurde zu diesem Zweck ein Selbstangabebogen zum Durchführungsprotokoll aufgenommen, der den Betroffenen von den Ausländerbehörden der Bundesrepublik Deutschland zum Ausfüllen vorgelegt werden soll.

Mit diesem Vordruck sollen personenbezogene Daten erhoben werden, die meines Erachtens weit über das erforderliche Maß hinausgehen. So wird beispielsweise nach Religion, Bildungsstand, Reiserouten nach der Ausreise aus Vietnam, ausgeübten Tätigkeiten, Einreise in die Bundesrepublik Deutschland sowie Familienangehörigen im Ausland gefragt. Für besonders bedenklich halte ich, wenn der Betroffene in der Bundesrepublik Deutschland einen Asylantrag gestellt hat, dieser abgelehnt wurde und er im Vordruck gebeten wird, dieses gegenüber den vietnamesischen Behörden (Grund und Zweck der Einreise in die Bundesrepublik Deutschland) bekanntzugeben.

Das Innenministerium hat ebenso wie das Bundesministerium des Innern darauf hingewiesen, daß das Ausfüllen des Vordruckes auf freiwilliger Basis erfolgt und der Betroffene durch die Ausländerbehörde hierauf hinzuweisen ist. Dem Problem wurde jedoch in der praktischen Umsetzung nicht hinreichend Rechnung getragen.

Existiert keine Rechtsvorschrift, die den Umgang mit personenbezogenen Daten ausdrücklich vorschreibt oder zuläßt, so kann dieser nur erfolgen, sofern der Betroffene gemäß § 6 Nr. 3 DSG MV eingewilligt hat. Da der Betroffene in diesen Fällen selbst darüber entscheiden kann, in welchem Umfang und zu welchem Zweck er seine Daten preisgibt, hat der Gesetzgeber eine umfangreiche Aufklärung des Betroffenen vorgesehen. Ziel ist es, daß der Betroffene die für seine Entscheidung notwendigen Erkenntnisse erlangt und der Umgang mit seinen Daten für ihn transparent wird.

Die Anforderungen an eine rechtswirksame Einwilligung sind in § 7 DSG MV festgelegt. Der Vordruck und das gewählte Verfahren entsprechen nicht den datenschutzrechtlichen Bestimmungen. So wird beispielsweise bei der Datenerhebung mit Hilfe des Vordruckes keine schriftliche Einwilligung des Betroffenen eingeholt. Darüber hinaus erweckt der Vordruck beim Betroffenen keineswegs den Eindruck, daß es sich um eine Datenerhebung auf freiwilliger Basis handelt. Ziffer 13 enthält die Formulierung: "Zusätzlich freiwillige Angaben (z. B. Wunsch eines ständigen Aufenthalts in einem dritten Land ...)". Durch diese Darstellung könnte man zu der Auffassung gelangen, die vorstehenden Angaben wären Pflichtangaben. So ist keinesfalls die erforderliche Klarheit und Transparenz für den Betroffenen gegeben. Der Betroffene hat für die wahrheitsgemäße Beantwortung seiner Angaben zu unterschreiben; eine schriftliche Einwilligung für den Umgang mit seinen Daten fehlt jedoch.

Ich habe gegenüber dem Innenminister deutlich gemacht, daß ich es für dringend erforderlich erachte, im Rahmen der Durchführung dieses Abkommens die geltenden datenschutzrechtlichen Bestimmungen zu beachten und die hierfür erforderlichen Maßnahmen einzuleiten. Unter anderem habe ich empfohlen, ein zweisprachiges Merkblatt zu erarbeiten, daß den Anforderungen an eine umfassende Aufklärung des Betroffenen gerecht wird.

Im Durchführungsprotokoll zum Abkommen ist darüber hinaus festgelegt worden, daß der Betroffene auf Antrag Auskunft über die zu seiner Person gespeicherten Daten sowie über den Verwendungszweck erhält. Im übrigen richtet sich das Recht auf Auskunft nach dem jeweiligen nationalen Recht. In § 20 DSG MV ist der Auskunftsanspruch des Betroffenen gegenüber den Ausländerbehörden geregelt. Dieses Auskunftsrecht ist Grundlage zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung des Betroffenen. Ob es in Vietnam einen ähnlichen gesetzlichen Auskunftsanspruch gibt, ist mir nicht bekannt. Es wäre möglich, daß der Betroffene unter diesen Umständen über sein Auskunftsrecht nichts erfährt und deshalb dieses Recht nicht in Anspruch nehmen kann. Betroffene haben sehr häufig darüber keine Kenntnis. Dies gilt aus meiner Erfahrung insbesondere auch für ausländische Staatsbürger, die sich nur zeitweilig in der Bundesrepublik Deutschland aufhalten. Es besteht somit die Gefahr, daß das Auskunftsrecht leer läuft. Um eine möglichst umfassende Aufklärung des Betroffenen auch im Hinblick auf sein Auskunftsrecht zu erreichen, habe ich empfohlen, hierauf in dem Merkblatt ausdrücklich hinzuweisen.

Im Durchführungsprotokoll zum Rückübernahmeabkommens ist ferner vorgesehen, daß, soweit bei den Ausländerbehörden vorhanden, ärztliche Unterlagen im Rahmen der datenschutzrechtlichen Bestimmungen an die vietnamesischen Behörden zu übermitteln sind. Der Innenminister unseres Landes hat in seinem Durchführungserlaß zu Recht darauf hingewiesen, daß eine Übermittlung dieser Unterlagen nur mit schriftlicher Einwilligung des Betroffenen zulässig ist. Auch in diesem Fall sind die Anforderungen an eine rechtswirksame Einwilligungserklärung zu beachten.

Ich habe darauf aufmerksam gemacht, daß der weitere Umgang mit personenbezogenen Daten von vietnamesischen Staatsangehörigen unzulässig ist, soweit diese bereits ohne Beachtung der datenschutzrechtlichen Bestimmungen erhoben wurden. Personenbezogene Daten, deren Erhebung unzulässig war oder deren Speicherung unzulässig ist, sind zu löschen.

Der Innenminister beabsichtigt, meine Anregungen aufzugreifen, ein Merkblatt in deutscher und vietnamesischer Sprache zu erarbeiten und künftig rechtswirksame Einwilligungserklärungen der Betroffenen einzuholen.

2.8. Kommunalrecht

2.8.1. Veröffentlichung eines Rechnungsprüfungsberichtes durch einen Gemeindevertreter

Ein Mitglied einer Gemeindevertretung hatte einen Rechnungsprüfungsbericht an die Presse weitergegeben. Ich wurde gefragt, ob dies zulässig sei.

Die Sachverhaltsprüfung hat ergeben, daß es sich bei dem Bericht um das Ergebnis einer überörtlichen Prüfung der Gemeindeverwaltung handelte, der den zuständigen Gremien (Amtsausschuß, Rechtsaufsichtsbehörde, Rechnungsprüfungsamt) zur Auswertung vorlag. In diesem Zusammenhang wurden Funktionsträger, beispielsweise Bürgermeister und Kämmerer, genannt. Der Bericht enthielt neben der Schilderung des Prüfungsvorganges und des Ergebnisses auch zahlreiche personenbezogene Daten. So wurde beispielsweise aufgeführt, welche Personen krankgeschrieben, welche Mitarbeiter überbezahlt oder an wen zinslose Darlehen gewährt worden waren.

Eine Veröffentlichung des Berichtes wurde deshalb zu Recht abgelehnt. Erst der reduzierte Abschlußbericht sollte der Öffentlichkeit zugänglich gemacht werden. Ungeachtet dessen hatte jedoch ein Gemeinderatsmitglied den Bericht an die Presse weitergeleitet.

Der Umgang mit personenbezogenen Daten erfordert gemäß § 6 DSG MV eine Rechtsgrundlage oder die Einwilligung des Betroffenen. In diesem Fall lag beides nicht vor. Folglich war die Weitergabe des Berichtes unzulässig.

Darüber hinaus war die Weitergabe des Berichtes an die Presse nicht erlaubt, weil auch ein Verstoß gegen die Verschwiegenheitspflicht vorlag. Gemeindevertreter sind gemäß § 23 Abs. 6 Satz 1 der Kommunalverfassung für das Land Mecklenburg-Vorpommern (KV M-V) zur Verschwiegenheit verpflichtet. Ausnahmen gelten gemäß § 23 Abs. 6 Satz 2 KV M-V nur, sofern die Tatsachen offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Dies traf jedoch auf die im Bericht erwähnten personenbezogenen Daten nicht zu. Die Weiterleitung könnte somit gemäß § 172 Abs. 1 Satz 1 KV M-V mit einem Ordnungsgeld geahndet werden.

Schwieriger ist der Sachverhalt dort zu beurteilen, wo Aussagen über das Verwaltungshandeln der Gemeinde als solche getroffen werden. In diesen Fällen kommen datenschutzrechtliche Bestimmungen erst dann zur Anwendung, wenn das Rechtsverhältnis zwischen der genannten Person und dem Dienstherren berührt wird. Dies ist etwa der Fall, wenn über Personalaktendaten gesprochen oder ein fehlerhaftes Verhalten dienstrechtlich bewertet wird. Erst dann ist der Amtswalter als Privatperson berührt und es findet der Übergang in den vom Landesdatenschutzgesetz geschützten Persönlichkeitsbereich des Betroffenen statt. Da dieser Übergang fließend und oft schwierig zu beurteilen ist, habe ich empfohlen, bei künftigen Veröffentlichungen sehr genau zu prüfen, ob die Datenweitergabe ohne weiteres zulässig ist. Andernfalls sind sämtliche personenbezogene Daten zu anonymisieren oder die Namen in den Prüfberichten zu schwärzen.

2.8.2. Petitionen am schwarzen Brett

In zwei Fällen war ich aufgefordert worden, den Umgang mit personenbezogenen Daten in einem kommunalen Petitionsausschuß zu bewerten.

Im ersten Fall hatten acht Arbeitnehmerinnen den Petitionsausschuß gebeten, eine Beschwerde über den Arbeitgeber zu prüfen. Der Vorsitzende des Ausschusses übermittelte die Eingabe direkt an den Aufsichtsrat des Unternehmens, in dem die Petentinnen angestellt waren, weil er meinte, nicht zuständig zu sein.

Auf meine Nachfrage hin konnte der Vorsitzenden des Petitionsausschusses keine Rechtsgrundlage für die Übersendungen der Petition an den Arbeitgeber angeben. Er war aber der Meinung, nicht gegen datenschutzrechtliche Bestimmungen verstoßen zu haben, weil der Fall schon anderweitig - nämlich durch einen Zeitungsbeitrag einer Petentin - öffentlich bekannt gemacht worden war.

Ich habe den Vorsitzenden darauf hingewiesen, daß es sich bei der Übersendung der Petition um eine Datenübermittlung handelt. Diese ist nur erlaubt, wenn der Betroffene eingewilligt hat oder sie gemäß dem DSG MV oder eines anderen Gesetzes zulässig ist. Es ist nicht ausreichend, daß sich der Petent bereits öffentlich zu seiner Eingabe geäußert hat. Die Einwilligung muß gemäß § 7 DSG MV ausdrücklich erteilt werden und bedarf in der Regel auch der Schriftform. Da es an diesen Voraussetzungen hier fehlte, war die Übermittlung der Petition unzulässig.

Im zweiten Fall erfuhr ich, daß auf der Tagesordnung des Petitionsausschusses das Anliegen und die vollen Namen von Petenten genannt wurden. Dies war besonders bedenklich, weil der Petitionsausschuß dazu übergegangen war, öffentliche Sitzungen durchzuführen.

Ich habe darauf hingewiesen, daß die Namensnennung nicht den Bestimmungen des DSG MV entsprach und den Petitionsausschuß aufgefordert, von dieser Praxis keinen Gebrauch mehr zu machen.

Der Vorsitzende des Ausschusses hat mir zugesichert, sich in Zukunft nach dieser Empfehlung zu richten.

2.8.3. Detektiv recherchiert für Bürgermeister

Ein Petent hat mir mitgeteilt, daß der Bürgermeister einer Gemeinde eine Detektei damit beauftragt hatte, Informationen über seine Person zu beschaffen. Die Detektei erledigte ihre Arbeit prompt, lieferte einen Bericht und erhielt ihr Honorar aus der Gemeindekasse.

Ich habe den Bürgermeister der Gemeinde gebeten, zu diesem Fall Stellung zu nehmen. Er rechtfertigte sein Vorgehen damit, daß keine personenbezogenen Daten des Petenten erhoben, verarbeitet und genutzt worden seien. Die Detektei habe lediglich Aussagen des Betroffenen überprüft, die dieser gegenüber Einwohnern und Gemeindevertretern des Ortes in Angelegenheiten der Gemeinde getroffen habe. Zweck dieser Überprüfung sei es gewesen, sich Klarheit darüber zu verschaffen, mit welcher Person man es zu tun habe. Der Bürgermeister meinte, das sei seine Aufgabe. Des weiteren stellte er fest, daß es sich hierbei um einen legitimen verwaltungsinternen Vorgang handelte und daß nicht gegen datenschutzrechtliche Bestimmungen verstoßen wurde. Der Bürgermeister nahm den Bericht der Detektei zur Kenntnis und ließ ihn anschließend "entsorgen", da aus seiner Sicht für eine Aufbewahrung dieser Unterlagen keine Notwendigkeit bestand.

Ich habe den Sachverhalt bewertet und dem Bürgermeister meine Rechtsauffassung mitgeteilt.

Die für die Aufgabenerfüllung zuständigen Behörden dürfen personenbezogene Daten Betroffener erheben und diese auch prüfen, etwa durch die Vorlage von Nachweisen, soweit dies aufgrund einer Rechtsvorschrift zulässig und im Einzelfall zu diesem Zweck erforderlich ist. Aus der Darstellung des Bürgermeisters ließ sich jedoch keinesfalls ersehen, für welchen konkreten Zweck diese Daten erforderlich waren. Eine Überprüfung von Aussagen, die gegenüber Gemeindevertretern oder anderen Personen gemacht wurden, rechtfertigt nicht die Einschaltung einer Detektei.

Der Einwand des Bürgermeisters, daß keine neuen Daten erhoben, sondern nur Äußerungen des Petenten überprüft wurden, greift nicht. Das Erheben von Daten umfaßt Befragungen, Messungen, Beobachtungen, Untersuchungen etc., letztendlich Aktivitäten, die auf das Beschaffen von Informationen ausgerichtet sind. Unerheblich ist hierbei, ob es sich um neue Daten oder die Bestätigung bereits vorhandener Erkenntnisse handelt. In diesem Fall mangelte es an der für den Umgang mit den personenbezogenen Daten des Petenten erforderlichen Rechtsgrundlage.

Das Erheben von personenbezogenen Daten ist nur zulässig, soweit dies zur Aufgabenerfüllung erforderlich und der Zweck der Erhebung hinreichend bestimmt ist. Ferner sind die Daten grundsätzlich beim Betroffenen und mit seiner Kenntnis zu erheben.

Von besonderer Bedeutung war in diesem Fall, daß personenbezogene Daten nicht nur ohne Rechtsgrundlage beschafft wurden, sondern daß die Datenerhebung in verdeckter Form erfolgte. Diese Art der Datenerhebung stellt einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung des Betroffenen dar. Die verdeckte Datenerhebung kommt nur in einzelnen Bereichen, wie etwa im Rahmen der Gefahrenabwehr gemäß § 33 SOG MV oder bei der Aufgabenerfüllung der Verfassungsschutzbehörden des Landes gemäß § 9 Abs. 3 LVerfSchG, in Betracht. Jedoch gilt auch hier, daß ein derartiger Eingriff in jedem Fall einer normenklaren Rechtsgrundlage bedarf.

Aufgrund der schwerwiegenden Verstöße gegen datenschutzrechtliche Bestimmungen habe ich die Vorgehensweise des Bürgermeisters beanstandet und den Innenminister hierüber unterrichtet. Die Antwort des Bürgermeisters stand zum Ablauf des Berichtzeitraumes noch aus.

2.9. Bau-, Wohnungs- und Liegenschaftswesen

2.9.1. Einwilligung zur Übermittlung von Bauherrendaten

Der Datenschutzbeauftragte eines anderen Bundeslandes machte mich darauf aufmerksam, daß in einigen Ländern die Bauordnungsbehörden regelmäßig Daten von Bauherren an Baustelleninformationsdienste zur kostenlosen Veröffentlichung übermitteln. Die Datenübermittlung erfolgt auf der Grundlage der Einwilligung der Betroffenen. Ich habe daraufhin das Verfahren in Mecklenburg-Vorpommern überprüft.

Im Rahmen des Baugenehmigungsverfahrens reicht der zukünftige Bauherr die Anträge und die für die Entscheidung notwendigen Unterlagen bei der Bauordnungsbehörde ein. Grundlage der freiverkäuflichen Antragsformulare sind die in der Bekanntmachung des Innenministers vom 5. Mai 1994 - II 620 b - (Amtsblatt M-V 1994, S. 547 ff.) veröffentlichten Mustervordrucke für Anträge im Baugenehmigungsverfahren. In den Anträgen wird eine Einwilligungsklausel verwendet, die die Baubehörden ermächtigen soll, Daten des Bauherrn (Name, Anschrift, Lage des Baugrundstückes, Art des Vorhabens und Baukosten) an Baustelleninformationsdienste zur kostenlosen Veröffentlichung zu übermitteln.

Ist wie im vorliegenden Fall die Einwilligung des Bauherrn erforderlich, so muß sie den Anforderungen des § 7 DSG MV entsprechen. Wird die Einwilligung zusammen mit anderen Erklärungen eingeholt, so muß sie sich im äußeren Erscheinungsbild von den anderen Angaben im Vordruck deutlich abheben. Der Betroffene ist in geeigneter Weise über die Bedeutung und Tragweite seiner Einwilligung, insbesondere über Art und Umfang des Umgangs mit seinen Daten, aufzuklären. Die Datenempfänger und die Anschrift der mit den Daten umgehenden Stelle sind ihm mitzuteilen. Ferner ist er unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß er die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen kann. Diese Bestimmungen sind bereits bei der Gestaltung von Vordrucken, mit deren Hilfe personenbezogene Daten beim Betroffenen auf freiwilliger Basis erhoben werden sollen, zu berücksichtigen. Da in diesen Fällen der Umgang mit den personenbezogenen Daten des Betroffenen nicht durch Gesetz erlaubt oder vorgeschrieben ist, sondern vom Betroffenen in eigener Verantwortung entschieden wird, hat der Gesetzgeber derart hohe Anforderungen an die Einwilligungserklärung gestellt.

Die in den Bauantragsformularen verwendete Einwilligungserklärung wurde diesen Anforderungen nicht ganz gerecht. So wurde zum Beispiel nicht ausreichend auf die Freiwilligkeit, insbesondere auf die Möglichkeit des Widerrufs ohne rechtliche Nachteile, hingewiesen. Diese Forderung besteht unabhängig vom Verlangen des Betroffenen, hierüber in Kenntnis gesetzt zu werden. Ferner ist in diesen Fällen immer darauf zu achten, daß nur eine tatsächlich gegebene Einwilligung zur Übermittlung der Daten berechtigt.

Der Minister für Bau, Landesentwicklung und Umwelt hat sich meiner Rechtsauffassung angeschlossen und die unteren Bauaufsichtsbehörden darauf hingewiesen, daß die in dem Bauantragsformular verwendete Einwilligungserklärung nicht den inhaltlichen und förmlichen Anforderungen des § 7 DSG MV entspricht und somit eine Datenübermittlung auf dieser Basis unzulässig ist. Darüber hinaus beabsichtigt er, bei einer Neufassung der Musterformulare für Bauanträge die Einwilligungsklausel herauszunehmen. Im Interesse der Betroffenen ist dieses Ergebnis so zu akzeptieren.

2.9.2. Zuviel Fürsorge für Bauwillige

Ein Bürger hat mir mitgeteilt, daß er beim Liegenschaftsamt seiner Stadt einen Antrag auf Erwerb eines Grundstückes zum Bau eines Eigenheimes gestellt hatte. Zu seiner Überraschung erhielt er kurze Zeit später ein Schreiben eines Immobilienmaklers des Ortes. Ihm wurde angeboten, ein Baugrundstück einschließlich Haus zu erwerben und bei der finanziellen Abwicklung des Vorhabens behilflich zu sein. Der Petent bat mich um datenschutzrechtliche Prüfung dieser Angelegenheit.

Ich habe den Bürgermeister der Stadt aufgefordert, zum Sachverhalt Stellung zu nehmen. Die Stadt wollte in guter Absicht bauinteressierten Bürgern öffentliches Bauland zur Verfügung stellen. Um dieses Vorhaben schnellstmöglich zu realisieren, wurde unter anderem mit dem Makler ein öffentlich-rechtlicher Vertrag geschlossen. Im Vertrag war vorgesehen, die bei der Stadt bereits vorliegenden Anmeldungen von Bürgern bei der Vergabe von Bauplätzen zu berücksichtigen. Zu diesem Zweck übermittelte die Stadt die Adressen der Bürger an den Makler.

Die Voraussetzungen für eine rechtmäßige Datenübermittlung lagen in diesem Fall jedoch nicht vor. Um das Anliegen zu realisieren, war die Datenübermittlung an den Makler nicht erforderlich. Vielmehr hätte die Stadt die Bürger, die einen Antrag gestellt hatten, über die Einbeziehung des Maklers informieren können. Denkbar wäre auch ein Adreßmittlungsverfahren gewesen. Der Makler hätte dann die entsprechenden Anschreiben zur Verfügung gestellt, die die Stadt nur noch mit den jeweiligen Adressen versehen hätte. Der Makler hätte somit keine personenbezogenen Daten erhalten, ohne daß die Betroffenen dies gewollt hätten. Die Interessen der Betroffenen wären mit beiden Verfahren berücksichtigt worden.

Den Petenten habe ich darüber informiert, daß die Stadt davon ausgegangen war, in seinem Interesse zu handeln. Gleichwohl habe ich die Stadt darauf hingewiesen, daß eine Umsetzung dieses Anliegens auch ohne eine Übermittlung der Anschriften möglich gewesen wäre, und habe ihr empfohlen, künftig entsprechend meinen Hinweisen zu verfahren.

2.10. Wahlen und Statistik

2.10.1. Öffentliche Auslegung von Wählerverzeichnissen und melderechtliche Auskunftssperren

Wählerverzeichnisse enthalten Name, Vorname, Geburtsdatum und Adresse der Wahlberechtigten. Ihre Auslegung dient der Kontrolle durch die Öffentlichkeit im Vorfeld einer Wahl. Datenschutzrechtliche Probleme ergeben sich im Zusammenhang mit melderechtlichen Auskunftssperren. Diese Sperren werden unter anderem verfügt, wenn Tatsachen die Annahme rechtfertigen, daß der betreffenden Person aus der Bekanntgabe ihrer Adresse eine Gefahr für Leben, Gesundheit oder persönliche Freiheit erwachsen kann. Nach geltendem Recht werden die Auskunftssperren bei der öffentlichen Auslegung der Wählerverzeichnisse nicht berücksichtigt. Melderechtliche Vorschriften werden somit umgangen.

Unser Innenminister hält diese Situation ebenfalls für unbefriedigend, sieht zur Zeit aber keine Möglichkeit, diesen Mißstand zu beseitigen und begründet dies damit, daß auch in Zukunft verbundene Wahlen (Verknüpfungen einer Landtags-/Kommunalwahl mit der Wahl zum Bundestag und/oder zum Europaparlament) nicht ausgeschlossen sind und ohne entsprechende Änderungen der Bundes- und Europawahlordnungen landesrechtliche Vorgaben zur Berücksichtigung der Auskunftssperren leerlaufen würden.

Die bloße Möglichkeit der Durchführung verbundener Wahlen darf meines Erachtens aber nicht dazu führen, daß mit den dringend notwendigen Änderungen der einschlägigen Landesvorschriften so lange gewartet wird, bis auch die Bundes- und Europawahlordnung geändert sind.

Ich halte es für erforderlich, daß die entsprechenden Kommunalwahl- und Landeswahlvorschriften möglichst bald korrigiert werden.

Auf ihrer 49. Konferenz haben die Datenschutzbeauftragten eine Entschließung zum Datenschutz bei Wahlen verabschiedet (siehe Anlage 17). In dieser Entschließung wird auch zur öffentlichen Auslegung von Wählerverzeichnissen Stellung genommen. Die Datenschutzbeauftragten fordern darin unter anderem, daß Daten von Bürgern, für die in Melderegistern eine Auskunftssperre eingetragen ist, im Wählerverzeichnis nicht veröffentlicht werden. Hier besteht offensichtlich Handlungsbedarf beim Gesetzgeber.

2.10.2. Gebäude- und Wohnungszählung 1995

In den neuen Bundesländern und im ehemaligen Ostberlin wurde 1995 mit einer Gebäude- und Wohnungszählung begonnen. Grundlage der Zählung sind das Wohnungsstatistikgesetz sowie die zu dessen Durchführung erlassenen Landesregelungen. Die wichtigsten Merkmale dieser statistischen Erhebung sind Art, Alter, Erhaltungszustand und Eigentümer der Gebäude sowie Anzahl, Größe und Nutzungsart der Wohnungen. Die Gebäude- und Wohnungszählung ist eine Totalerhebung, das heißt, jedes Gebäude und jede Wohnung auf dem Gebiet der ehemaligen DDR werden erfaßt. Auskunftspflichtig sind Eigentümer, Verwalter, Erbbauberechtigte und die Verfügungs- oder Nutzungsberechtigten.

Bei einer derart umfassenden Befragung ist in besonderem Maße auf die Einhaltung des Datenschutzes und der Grundsätze der Statistik - Gebot der frühestmöglichen Anonymisierung, Reidentifizierungsverbot, Statistikgeheimnis - zu achten.

Anfang 1995 hatte ich eine Besprechung mit dem Statistischen Landesamt über den von ihm vorgelegten Entwurf einer "Organisationsanordnung zur Durchführung der Gebäude- und Wohnungszählung 1995". Dieser Entwurf regelt unter anderem

- die Stellung des Statistischen Landesamtes als der für die Durchführung der Zählung verantwortlichen Behörde und die Zuständigkeiten der von den Gemeinden einzurichtenden örtlichen Erhebungsstellen,

- die räumliche, örtliche und personelle Trennung der örtlichen Erhebungsstellen von anderen Dienststellen der Verwaltung,

- die von den örtlichen Erhebungsstellen zu treffenden verfahrensmäßigen Vorkehrungen, um zu verhindern, daß die Angaben in den Erhebungsvordrucken für andere Aufgaben oder Zwecke verwendet werden,

- die Auswahl der Erhebungsbeauftragten und die an sie zu stellenden Anforderungen,

- das für die örtlichen Erhebungsstellen geltende Verbot, Zusatzerhebungen oder Auswertungen der Daten vorzunehmen.

Mit diesem Entwurf war ich im wesentlichen einverstanden, habe jedoch gefordert,

- daß als Erhebungsbeauftragter nicht bestellt werden darf, wer dienstlich oder beruflich mit Wohnungsangelegenheiten betraut oder Mitarbeiter des Verfassungsschutzes ist, und daß

- von dem Verbot, Erhebungsunterlagen zu vervielfältigen, die personenbezogene Angaben enthalten, keine Ausnahmen zugelassen werden.

In der mittlerweile erlassenen Organisationsanordnung sind diese Forderungen berücksichtigt worden.

Im Zusammenhang mit der Durchführung der Gebäudezählung hat sich der Datenschutzbeauftragte einer Gemeinde bei mir erkundigt, ob Mieter nach den Adressen oder Telefonnummern der Eigentümer befragt werden dürfen. Grund der Anfrage war, daß trotz Ausschöpfung der im Wohnungsstatistikgesetz vorgesehenen Maßnahmen eine große Anzahl von Eigentümeradressen fehlen.

In § 8 Wohnungsstatistikgesetz ist geregelt, daß bestimmte öffentliche Stellen genau festgelegte Daten an die Erhebungsstellen übermitteln. Andere Möglichkeiten zur Ermittlung der Auskunftspflichtigen, wie die Erhebung von Eigentümerdaten bei den Mietern, sind darin nicht erwähnt. Wegen des abschließenden Charakters dieses Spezialgesetzes kommen die Vorschriften des Landesdatenschutzgesetzes zur Erhebung und Übermittlung von Daten nicht zur Anwendung. Die Befragung der Mieter nach den Eigentümerdaten ist danach ausgeschlossen. Dies habe ich dem Datenschutzbeauftragten mitgeteilt.

2.11. Soziales und Sozialwesen

2.11.1. Individuelle Beratung im Sozialamt

In den beiden vergangenen Jahren habe ich mehrere Kontrollen in Sozialämtern durchgeführt. Einige Sozialämter befinden sich zum Teil noch in einer Aufbau- bzw. Konsolidierungsphase und sind häufig provisorisch untergebracht. Aus dieser Tatsache resultiert, daß viele der festgestellten Mängel auf den baulichen Zustand und die Art der Unterbringung zurückzuführen waren. Zum Beispiel bleibt ein aus datenschutzrechtlicher Sicht gut administriertes Computernetz ein Sicherheitsrisiko, wenn es in einer Baracke untergebracht wird und hinsichtlich der Zugangskontrolle nicht ausreichend geschützt werden kann.

Bei den Kontrollen habe ich Hinweise zur Verbesserung des datenschutzrechtlichen Standards gegeben.

Zur Wahrung des Sozialgeheimnisses gehört es unter anderem, die Bürger bei Vorsprache in den Ämtern nicht namentlich aufzurufen. In einem Sozialamt wurde diese aus datenschutzrechtlicher Sicht angemessene Maßnahme jedoch dadurch aufgehoben, daß zwar der Aufruf nach einer von den Bürgern zu ziehenden Nummer erfolgte, anschließend aber aus Platzmangel pro Sprechzimmer zwei Klienten gleichzeitig beraten und betreut wurden. In solchen Fällen kann das Sozialgeheimnis gegenüber Dritten kaum gewahrt werden (§ 35 Sozialgesetzbuch Erstes Buch - SGB I). Auf meinen Einwand zu diesem Verfahren wurde mir entgegengehalten, daß bei einer generellen Individualberatung bedeutend längere Wartezeiten entstehen würden, was auf keinen Fall im Interesse der Sozialhilfeempfänger sei. Die Einzelberatung könnte erst nach der Verlegung des Amtes in ein neues Verwaltungsgebäude verwirklicht werden. Ich habe empfohlen, den Betroffenen zumindest die individuelle Beratung anzubieten bzw. zu entscheiden, ob wegen des vorgesehenen Gespräches einzeln beraten oder betreut werden muß.

Einigen Sozialämtern, die den Einsatz von Rechentechnik zur Vorgangsbearbeitung planen, habe ich meine Beratung angeboten und empfohlen, ein Datenschutz- und Datensicherheitskonzept auszuarbeiten (siehe Punkt 2.16.5). Das Konzept muß insbesondere klare Befugnisse der Anwender enthalten und Nutzungsbedingungen festlegen (§ 78a Sozialgesetzbuch Zehntes Buch - SGB X). Die Mitarbeiter sollten vor Inbetriebnahme des Systems geschult werden, damit von Beginn an, eine ordnungsgemäße Fallbearbeitung gewährleistet ist und Fehler vermieden werden.

In Sozialämtern mit automatisierter Sozialdatenverarbeitung habe ich festgestellt, daß die nach dem Landesdatenschutzgesetz zu führenden Dateibeschreibungen und Geräteverzeichnisse (§ 16 DSG MV) mitunter erst nach meiner Anmeldung und Aufforderung zur Übersendung erstellt wurden. Die Dateibeschreibungen sind jedoch neben der Unterstützung meiner Kontrolle für die Auskunftserteilung an die Betroffenen sowie die Schulung der Mitarbeiter von Bedeutung. Die speichernden Stellen sind verpflichtet, sie vorzuhalten und laufend zu aktualisieren.

In den Dateien sind häufig frei verfügbare Datenfelder ohne Nutzungseinschränkung vorhanden. Die Nutzung derartiger Felder ist aber nur zulässig, wenn Maßnahmen festgelegt sind, die eine willkürliche Belegung verhindern (siehe auch Erster Tätigkeitsbericht Punkt 2.14.2).

Von einigen Mitarbeitern in Sozialämtern wurde bei den Kontrollen die Meinung geäußert, daß mehr für sozial Schwache zu tun wäre. Leider behindere aber der Datenschutz diese Hilfe, weil es nicht möglich ist, die Adressen der Betroffenen zu bekommen und ihnen deshalb keine Beratung und Hilfe angeboten werden könne. In diesem Zusammenhang habe ich empfohlen, zunächst die Bürgerinnen und Bürger in allgemeiner Form zu informieren. Ein Sozialamt hat hierzu eine recht unkomplizierte Verfahrensweise angewendet, die auch aus datenschutzrechtlicher Sicht unbedenklich ist. Soziale Probleme zeichnen sich häufig ab, wenn Mieter ihren Zahlungsverpflichtungen nicht mehr nachkommen können. Das Sozialamt hat deshalb ein entsprechendes Informationsblatt herausgegeben und die städtische Wohnungsgesellschaft gebeten, es Mietschuldnern zuzuleiten, die über mehrere Monate hinweg die Miete nicht gezahlt haben. Durch dieses Verfahren können die Betroffenen direkt angesprochen werden, ohne daß Datenübermittlungen und somit ein gravierender Eingriff in das Persönlichkeitsrecht erforderlich sind. Selbstverständlich muß die städtische Wohnungsgesellschaft sorgsam mit dem Informationsblatt umgehen und sollte es erst nach einem Gespräch mit dem jeweiligen Mieter übergeben. Das Anbieten von Hilfe und die informationelle Selbstbestimmung schließen sich jedenfalls nicht gegenseitig aus, wie das Beispiel zeigt.

2.11.2. Ein- und ausgehende Post in der Sozialverwaltung

Bei einer Beratung in einem Jugendamt wurde ich gefragt, ob es zulässig sei, daß die für das Amt bestimmte Post von der Poststelle der Kreisverwaltung geöffnet wird. In der allgemeinen Geschäftsanweisung der Kreisverwaltung war geregelt, daß bestimmte Sendungen durch die zentrale Poststelle nicht zu öffnen sind, beispielsweise Sendungen an das Gesundheitsamt und die Personalvertretung. Ich habe der Verwaltung empfohlen, die Aufzählung um Sendungen zu ergänzen, deren vermutlicher Inhalt einer Geheimhaltungsvorschrift unterliegt. Sendungen an das Sozialamt und das Jugendamt sind den angegebenen Empfängern direkt zuzustellen, da sie Sozialdaten enthalten können, die unter das Sozialgeheimnis des § 35 SGB I fallen. Das Jugendamt hat die Empfehlung umgesetzt.

In ähnlichen Fällen wurde dagegen geltend gemacht, daß die Mitarbeiter der Poststelle zur Einhaltung des Datengeheimnisses verpflichtet seien und deshalb meine Forderung nach verschlossener Weiterleitung nicht verständlich sei. Hierbei spielt der Grundsatz der Erforderlichkeit die entscheidende Rolle. Aufgabe der Poststelle ist es in der Regel, die ein- und ausgehenden Sendungen zu registrieren. Zur Erfüllung dieser Aufgabe ist es nicht notwendig, den Inhalt der Sendungen zu kennen. Eingangsstempel und Eingangsvermerk können ebensogut auf dem geschlossenen Umschlag angebracht werden. Dieser Argumentation sind die Stellen gefolgt und haben daraufhin die Sendungen geschlossen weitergeleitet.

In einem anderen Fall hat sich ein Bürger bei mir beschwert, daß die an ihn gerichtete Post des Sozialamtes mit der vollständigen Absenderangabe gestempelt war. Hier ist zu entscheiden, ob die volle Absenderangabe für die Zustellung erforderlich ist oder ob nicht "Stadtverwaltung" und Nummer des Dezernats oder einer anderen größeren Verwaltungseinheit ausreichen würde. Für den Bürger ist der Absender aus dem Schreiben erkennbar und im Falle, daß die Sendung nicht zugestellt werden kann, sollte diese Angabe für die Rücksendung genügen. Das Sozialamt hat zugesichert, künftig einen neutralen Absenderstempel zu benutzen (siehe auch Punkt 2.4.2).

2.11.3. Übermittlung von Sozialdaten - immer wieder im Brennpunkt

Ein Träger der gesetzlichen Krankenversicherung hat mich um Beratung zur Übermittlung von Sozialdaten gebeten. Eine private Lebensversicherungsgesellschaft wollte Auskunft über Sozialdaten eines Verstorbenen haben und hat dies mit einer Leistungsprüfung im Versicherungsfall begründet.

Die Lebensversicherung vertrat die Auffassung, daß das Recht auf Auskunftserteilung gemäß § 305 SGB V (Sozialgesetzbuch Fünftes Buch) nach dem Tod des Betroffenen auf die Erben übergeht. Da die Erben ihre schriftliche Einwilligung zur Auskunftserteilung gegeben hätten und die Leistungsprüfung in ihrem Interesse liege, müsse die Auskunft gegeben werden. In der weiteren Begründung weist die Lebensversicherungsgesellschaft auf ein Urteil des Bundesgerichtshofes (BGH) zur Einsichtnahme in Krankenunterlagen hin.

§ 305 SGB V regelt in der bis zum 31. Dezember 1995 geltenden Fassung die Auskunftserteilung der Krankenkassen bzw. der Kassenärztlichen Vereinigungen an den Versicherten über die in einem bestimmten Zeitraum in Anspruch genommenen Leistungen und deren Kosten. Zweck der Vorschrift ist es, die Leistungserbringung und -abrechnung für den Versicherten transparent zu gestalten. Dazu kann über die Leistungsposition mit den entsprechenden Kosten oder die Aufenthaltsdauer im Krankenhaus und das Entgelt Auskunft gegeben werden. Es besteht aber kein Anspruch auf Mitteilung der Diagnose. Die Rechtsvorschrift richtet sich an den Versicherten, und sie kann nur auf die Erben übergehen, wenn ein Rechtsstreit im Zusammenhang mit der Leistungserbringung und -abrechnung besteht. Es war aus dem Antrag der Lebensversicherungsgesellschaft nicht ersichtlich, daß sie die Daten zur Klärung eines derartigen Rechtsstreites benötigte. Im übrigen ist der Sachverhalt nicht über die Auskunftserteilung nach SGB V, sondern nach den Übermittlungsvorschriften des SGB X zu beurteilen (§§ 67d ff. SGB X). Da sich das Begehren auf Krankenunterlagen erstreckt, ist die Übermittlung nur unter der Voraussetzung zulässig, nach der eine in § 203 Abs. 1 und 3 des Strafgesetzbuches (StGB) genannte Person, zum Beispiel ein Arzt, zur Übermittlung befugt wäre (§ 76 Abs. 1 SGB X).

Ich habe dem Träger der gesetzlichen Krankenversicherung mitgeteilt, daß keine der im SGB X genannten Übermittlungsvorschriften hier anwendbar und auch eine Auskunftserteilung nicht zulässig ist.

2.11.4. Wohngeldakte auf der Straße

Ein aufmerksamer Bürger hatte auf der Straße eine komplette Wohngeldakte gefunden, sie an mich gesandt und gebeten, die Angelegenheit zu bearbeiten.

Auf meine Frage, wie die Akte auf die Straße gelangt sei, teilte mir der zuständige Landrat mit, daß die Wohngeldstelle im Rahmen der Kreisgebietsreform einer anderen Amtsgemeinde zugeordnet worden ist. Die Wohngeldakte sei vermutlich beim Transport vom Lastkraftwagen gefallen. Diesen Verlust hatte die zuständige Stelle bis zu meiner Anfrage noch nicht bemerkt.

Nach der Schilderung des Landrates wurden die Akten vor dem Umzug durch die Mitarbeiter der Wohngeldstelle den neuen Ämtern zugeordnet. Anschließend sind sie in Kisten verpackt, mit Decken zugedeckt und auf einem offenen LKW an den Bestimmungsort transportiert worden. Den Mitarbeitern sei nicht erklärlich gewesen, wie die Akte dabei abhanden kommen konnte.

Ich habe dem Landrat eine Beanstandung wegen des sorglosen Umgangs mit personenbezogenen Daten ausgesprochen und ihn zu einer Stellungnahme aufgefordert. Die Beanstandung habe ich mit der Verletzung eines Privatgeheimnisses, unzureichenden technisch-organisatorischen Maßnahmen und dem Nichteinhalten von Verarbeitungsvorschriften begründet. Die Akten hätten nicht auf einem offenen LKW ohne ausreichende Sicherheitsvorkehrungen transportiert werden dürfen. Es wäre zumindest erforderlich gewesen, sie in verschlossene Behältnisse zu verstauen, am Versandort zu registrieren und am Empfangsort auf Vollständigkeit zu überprüfen.

In der Stellungnahme hat der Landrat dargelegt, daß der Vorfall mit den Mitarbeitern ausgewertet worden ist und Maßnahmen festgelegt wurden, die ähnliche Nachlässigkeiten in Zukunft ausschließen.

2.11.5. Datenerhebung für die Sozialhilfestatistik

Beantragt ein Bürger Sozialhilfe, so muß er umfangreiche Daten angeben, die es dem Sozialamt ermöglichen, eine qualifizierte Entscheidung zu treffen und angemessene Unterstützung zu gewähren. Das Bundessozialhilfegesetz (BSHG) sowie das SGB I und SGB X enthalten Vorschriften über die Leistungsgewährung, den Umgang mit Sozialdaten sowie zum Verwaltungsverfahren.

Im BSHG ist unter anderem eine Regelung enthalten, daß bestimmte Sozialdaten für statistische Zwecke zu nutzen sind. Diese Statistik ist eine Sekundärstatistik, es werden dafür nur Daten verwendet, die zur Leistungsgewährung erforderlich sind. Durch eine Neuregelung der entsprechenden Vorschrift im BSHG sollen nunmehr Daten einbezogen werden, die nicht regelmäßig für die Leistungsgewährung erforderlich sind, wie zum Beispiel höchster Schulabschluß an allgemeinbildenden Schulen, höchster Berufsbildungsabschluß oder Angaben zur besonderen sozialen Situation. Diese Daten können jedoch nur auf freiwilliger Basis erhoben und für die Statistik genutzt werden (§ 15 Landesstatistikgesetz - LStatG M-V).

Dem Sozialministerium unseres Landes und den Sozialämtern habe ich mitgeteilt, daß die Fragen nach dem Bildungsabschluß oder der besonderen sozialen Situation nur zu beantworten sind, wenn sie beispielsweise für eine Hilfe zur Arbeitsaufnahme notwendig sind. Die Mehrzahl der Sozialämter hat mitgeteilt, daß sie die Betroffenen auf die Freiwilligkeit der Erhebung hinweisen. Die Daten werden überwiegend im Gespräch, teilweise aber auch auf einem Zusatzfragebogen erhoben. Ein Sozialamt hat dargelegt, daß es "bisher keine Probleme" gegeben habe und die Betroffenen "bereitwillig die Angaben geleistet" hätten. Dies sind jedoch keine Kriterien für eine rechtmäßige Datenerhebung.

Der Sozialminister hat mich über ein Schreiben der Bundesministerin für Familie und Senioren unterrichtet, in dem beispielsweise das Erheben des Schul- und Berufsbildungsabschluß mit der Förderung der Wiedereingliederung in das Berufsleben begründet wird. Im übrigen sei dies auf die 15- bis 65jährigen Leistungsempfänger beschränkt.

Aber auch innerhalb dieser Altersgruppe ist es nicht regelmäßig erforderlich, diese Daten zu erheben. Beispielsweise dann nicht, wenn feststeht, daß für den Betroffenen eine Wiedereingliederung in das Berufsleben wegen Pflegebedürftigkeit nicht in Betracht kommt. Ebenso ist auch die Erhebung der Daten über Familienmitglieder nicht erforderlich, wenn sie keiner Hilfe des Sozialleistungsträgers bedürfen.

Es ist stets im Einzelfall zu prüfen, ob die Daten im Zusammenhang mit der Hilfegewährung stehen oder von den Betroffenen auf freiwilliger Basis für statistische Zwecke unter Beachtung der Unterrichtungsvorschrift des Landesstatistikgesetzes erhoben werden sollen (§ 15 LStatG M-V).

2.11.6. Kinder- und Jugendhilfe

Bei Beratungen im Bereich der Kinder- und Jugendhilfe wurde ich zur datenschutzgerechten Gestaltung des Hilfeplanverfahrens befragt (§ 36 Sozialgesetzbuch Achtes Buch - SGB VIII, Kinder- und Jugendhilfe). Ein freier Träger der Kinder- und Jugendhilfe berichtete, daß die Eltern die für den Hilfeplan erforderliche Datenübermittlung an das Jugendamt ablehnten. Sie befürchteten, daß ihre Sozialdaten dort einem größeren Personenkreis bekannt und möglicherweise unzulässig offenbart werden könnten. Die Aufstellung des Hilfeplans nach dem SGB VIII ist eine "Sollvorschrift", und die freien Träger und Betroffenen gingen davon aus, daß er deshalb nicht in jedem Fall zur Leistungsgewährung erforderlich ist.

Um dies datenschutzrechtlich beurteilen zu können, habe ich die Kultusministerin unseres Landes um Stellungnahme gebeten. Sie teilte mir mit, daß der Hilfeplan in der Regel zu erstellen ist. Nur in begründeten Ausnahmefällen, zum Beispiel bei besonderer Eilbedürftigkeit, kann im Einzelfall davon abgewichen und der Plan im Laufe des Verfahrens eingereicht werden.

Bei der Planung der Hilfe kommt es darauf an, daß nur Mitarbeiter des Jugendamtes beteiligt werden, die unmittelbar fachlich einbezogen sind. Sofern die Leistung durch einen freien Träger gewährt wird, ist der Personenkreis auch hier entsprechend einzuschränken. Die Hilfegewährung kann nur erfolgreich sein, wenn Daten zwischen diesem eingegrenzten Kreis von Beteiligten unter Beachtung der Zweckbindung ausgetauscht bzw. übermittelt werden. Das Ziel der Hilfe wird gefährdet, wenn der besondere Vertrauensschutz nicht gesichert ist, den diese Sozialdaten erfordern. Ich habe empfohlen, die Betroffenen umfassend über das gesamte Verfahren und insbesondere über die Verarbeitung und Nutzung ihrer Sozialdaten zu informieren, damit sie wissen, welcher Personenkreis Zugriff auf ihre Daten hat.

Das SGB VIII normiert, daß wichtige Entscheidungen bei der Leistungsgewährung in der Kinder- und Jugendhilfe im Zusammenwirken mehrerer Fachkräfte (Team- oder Erziehungskonferenz) getroffen werden sollen. Die Kultusministerin hat zur Tätigkeit und Zusammensetzung der Erziehungskonferenz empfohlen, daß unter anderem die Amts- bzw. Abteilungsleitung des Jugendamtes sowie ein Vertreter, der zur Bereitstellung der finanziellen Mittel zur Hilfegewährung befugt ist, an den Beratungen teilnehmen sollen.

Die Erziehungskonferenz hat die Aufgabe, die fachlich geeigneten Mittel für die zu gewährende Hilfe festzulegen. Zu diesem Zweck ist die Nutzung von Sozialdaten unumgänglich. Die allgemeine Vorschrift zur Wahrung des Sozialgeheimnisses (§ 35 SGB I) normiert aber, daß Sozialdaten auch innerhalb des Leistungsträgers nur Befugten zugänglich sein oder nur an diese weitergegeben werden dürfen. Die regelmäßige Teilnahme des Haushaltssachbearbeiters ist in Frage zu stellen, da er üblicherweise keine fachlich relevanten Empfehlungen geben kann und auch nicht an der fachlichen Hilfe mitwirkt. Als Entscheidungsgrundlage für die Bewilligung der finanziellen Mittel dürften anonymisierte Daten ausreichend sein. Darüber hinaus sollte die Einbeziehung des Amtsleiters auf Fälle beschränkt sein, in denen keine Einigung der Fachkräfte über die zu gewährende Hilfe zustande kommt und daher seine Entscheidung erforderlich ist.

Der Kultusministerin habe ich empfohlen, die Empfehlungen entsprechend zu überarbeiten. Inzwischen hat sie mir bestätigt, daß die Teilnahme des Haushaltssachbearbeiters an der Erziehungskonferenz nicht erforderlich ist und die Überarbeitung der Empfehlungen in Aussicht gestellt.

2.11.7. Geltendmachung von Unterhaltsansprüchen

Aufgrund einer Information meiner Kollegen habe ich das Landesjugendamt gebeten, mir mitzuteilen, wie Mütter und Väter bei Anträgen zur Feststellung des Unterhalts unterstützt werden (§ 18 Abs. 1 SGB VIII). Daraufhin wurden mir die entsprechenden Erhebungsbogen verschiedener Jugendämter zugesandt.

Es zeigte sich, daß die Datenerhebung recht umfangreich und unterschiedlich ist. So werden unter anderem Belege über das Einkommen und Vermögen von Ehepartnern und Kindern des Unterhaltspflichtigen gefordert, obwohl diese nicht auskunftspflichtig sind, oder es wird nach der Krankenkasse des zum Unterhalt Verpflichteten gefragt. Auf einigen Formularen fehlt die Rechtsgrundlage zur Erhebung der Daten, und es werden Rechtsnormen zitiert, die nicht mehr gelten. Außerdem wird nur unzureichend über das Verarbeiten und Nutzen der Daten aufgeklärt. Einige Erhebungsbogen enthalten eine pauschale Einwilligungserklärung, die zudem im

Schriftbild nicht hervorgehoben ist und deshalb weder inhaltlich noch formal den Anforderungen entspricht.

Ich habe der Kultusministerin empfohlen, im Rahmen der Fachaufsicht ein einheitliches Verfahren für die Datenerhebung in Jugendämtern zu erlassen. In einem Zwischenbescheid vom September 1995 hat sie mitgeteilt, daß die festgestellten Mängel mit den kommunalen Spitzenverbänden und dem Landesjugendamt diskutiert werden. Über das Ergebnis werde ich informiert.

2.11.8. Kindesmißhandlung - Geheimhaltung oder Offenbarung?

Im Rahmen meiner Beratungsgespräche in Jugendämtern wurde wiederholt gefragt, ob die Übermittlung von Daten bei festgestellten Kindesmißhandlungen oder sexuellem Mißbrauch zulässig sei. Bei der Beantwortung dieser Frage steht selbstverständlich der Schutz des Kindes immer im Vordergrund.

Erklärt beispielsweise ein Kind oder Jugendlicher während einer Beratung, körperlich oder sexuell mißhandelt worden zu sein, so fällt das dem Berater Anvertraute unter die berufsbedingte Schweigepflicht (§ 203 StGB) und darf nur mit Einwilligung des Kindes oder im Falle eines rechtfertigenden Notstandes (§ 34 StGB) offenbart werden. Ob Angaben an die entsprechenden Stellen zur Strafverfolgung übermittelt werden, ist immer eine persönliche, verantwortungsbewußt und im Sinne des Kindes zu treffende Entscheidung des Beraters. Wird das Privatgeheimnis mit Einwilligung des Kindes offenbart, so ist zu prüfen, ob es selbst überhaupt in der Lage ist, sein Recht auf informationelle Selbstbestimmung wahrzunehmen. Dies hängt maßgeblich von seiner Urteils- und Einsichtsfähigkeit ab. Wenn sie nicht ausreicht, ist die Einwilligung der Personensorgeberechtigten erforderlich.

Ist die Mißhandlung eines Kindes oder Jugendlichen im Rahmen der Erfüllung einer sozialen Aufgabe bekannt geworden, dürfen Sozialdaten nur übermittelt werden, soweit dies erforderlich und der Erfolg einer zu gewährenden Leistung dadurch nicht in Frage gestellt ist (§ 64 Abs. 2 SGB VIII in Verbindung mit § 69 Abs. 1 SGB X). Beispielsweise kann das Jugendamt bei Gefährdung des Kindeswohls das Gericht anrufen und Sozialdaten übermitteln, um eine Hilfeleistung zu sichern (§ 50 Abs. 3 SGB VIII).

2.11.9. Leistungen des Versorgungsamtes

Im April 1994 habe ich ein Versorgungsamt kontrolliert.

Das Versorgungsamt erhebt, verarbeitet und nutzt Sozialdaten für Leistungen nach dem Bundeserziehungsgeldgesetz (BErzGG), dem Bundesversorgungsgesetz (BVG) und dem Schwerbehindertengesetz (SchwbG). Die Antragsdaten werden im Versorgungsamt erfaßt, auf Disketten gespeichert und in der Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ) verarbeitet. Anträge und medizinische Unterlagen werden in Einzelfallakten aufbewahrt.

Im Ergebnis der Kontrolle habe ich empfohlen,

- die Dienstanweisungen zu überarbeiten und den spezifischen Bedingungen im Amt anzupassen, da sie ohne Änderung von einem anderen Bundesland übernommen worden sind,
- die Anweisungen und Formulare zu aktualisieren, da zum Teil nicht mehr geltende Rechtsgrundlagen zitiert werden und
- in Räumen mit Besucherverkehr die Akten so aufzubewahren, daß Unbefugte sie nicht einsehen oder entnehmen können.

Anläßlich des Besuches wurde ich unter anderem gefragt, ob es zulässig sei, bei der Anforderung ärztlicher Unterlagen nicht mehr die Erklärung des Betroffenen zur Entbindung von der ärztlichen Schweigepflicht beizufügen, sondern nur darauf zu verweisen, daß sie im Versorgungsamt vorliegt und zu den Akten genommen wurde. Dieses Verfahren vereinfache den Verwaltungsablauf und die Ärzte seien durch die amtliche Versicherung rechtlich abgesichert.

Mit dem dafür entwickelten Antragsformular war ich einverstanden und habe diesem Verfahren zugestimmt. Meine oben genannten Empfehlungen wurden inzwischen vom Versorgungsamt realisiert.

2.11.10. Kontrolle einer Krankenkasse

Im Dezember 1994 habe ich die Bereiche Beitrags- und Leistungswesen sowie die Datenverarbeitung einer Innungskrankenkasse (IKK) kontrolliert.

Im Bereich Beitragswesen werden die Daten der Mitglieder getrennt nach Pflichtversicherten, freiwillig Versicherten und Arbeitgebern automatisiert verarbeitet und genutzt. Die Daten sind außerdem in einem aus Rechnerausdrucken bestehenden Beitragsbuch gespeichert. Die Beitragszahlung wird automatisiert überwacht.

Im Leistungsbereich werden die in Anspruch genommenen Leistungen erfaßt und die Versicherten betreut. Bei Besuchen der Versicherten ist durch die Einzelberatung eine vertrauliche Gesprächsführung gewährleistet. Außerdem können sie sich hier im Beisein eines Sachbearbeiters den Inhalt ihrer Krankenversichertenkarte ausdrucken lassen.

Bei der Kontrolle des Beitrags- und des Leistungsbereiches habe ich festgestellt, daß teilweise identische Bildschirmmasken genutzt werden, obwohl nach Aussage der Mitarbeiter nicht alle angezeigten Daten im jeweiligen Bereich zur Aufgabenerfüllung benötigt werden.

Die IKK betreibt ein internes Rechnernetz, an das zum Zeitpunkt der Kontrolle alle Geschäftsstellen angeschlossen waren. Darüber hinaus nutzen die IKKn aus Mecklenburg-Vorpommern, Schleswig-Holstein und Hamburg ein gemeinsames Rechenzentrum in Hamburg.

Ich habe empfohlen,

- die Dienstanweisungen zum Umgang mit Sozialdaten unter Beachtung der neuen gesetzlichen Grundlagen (2. Änderungsgesetz zum Sozialgesetzbuch) zu überarbeiten,
- für den Umgang mit Sozialdaten ein Datenschutz- und IT-Sicherheitskonzept auszuarbeiten,
- die Dateibeschreibungen und Geräteverzeichnisse in der von mir im Amtsblatt für Mecklenburg-Vorpommern Nr. 21 vom 25. Mai 1993 empfohlenen Form anzulegen,
- die Zugriffsrechte nach Aufgabenbereichen weiter zu differenzieren,
- ein Lesegerät für Krankenversichertenkarten an einer gut zugänglichen Stelle zur Verfügung stellen, damit die Versicherten eigenständig den Inhalt ihrer Chipkarte lesen und ausdrucken können,
- die Aufbewahrungsfrist der Protokolle der Anmeldungen im Datenverarbeitungssystem von derzeit drei Jahren auf ein Jahr zu verkürzen und anschließend datenschutzgerecht zu vernichten (Damit könnte der Gefahr des Mißbrauchs, beispielsweise der Nutzung für unzulässige Leistungs- und Verhaltenskontrollen der Mitarbeiter, vorgebeugt werden.),
- bei der Wartung der Datenverarbeitungs-Anlage (DV-Anlage) auf Testdaten zurückzugreifen und die von den Landesbeauftragten für den Datenschutz herausgegebene Orientierungshilfe "Forderungen an Wartung und Fernwartung" zu berücksichtigen.

Der Geschäftsführer der IKK hat zugesagt, daß er diesen Empfehlungen folgen wird.

Im Vorfeld der vorgesehenen Fusion der drei Innungskrankenkassen zu einer landesweiten Kasse hatte ich empfohlen, daß es jedem Versicherten möglich sein sollte, zwischen der Betreuung durch eine oder durch mehrere Geschäftsstellen zu wählen. Würde er nur eine Stelle wählen, wäre auch nur diese zum Zugriff auf seine Beitrags- und Leistungsdaten berechtigt. Die Krankenkasse hat mir mitgeteilt, daß sich dies aus organisatorischen Gründen gegenwärtig nicht realisieren lasse, da hierzu Lösungen im Rahmen der Bundesverbände der Krankenkassen erforderlich seien. Die Datenschutzbeauftragten des Bundes und der Länder streben eine Klärung dieser Thematik mit den Bundesverbänden an.

2.11.11. Krankenkassen wollen werben

Im Mai 1994 hat mir ein Bürger mitgeteilt, daß er und auch seine Tochter von einer Ersatzkrankenkasse mehrfach zu Werbungszwecken angerufen wurden, obwohl er bereits beim ersten Anruf entsprechende Offerten abgelehnt hatte. Auf seine Frage, woher sie eigentlich den Namen, die Telefonnummer und die Anschrift der Tochter hätten, wurde ihm mitgeteilt, daß die Schulen diese Daten der Schulabgänger an die Kassen übermitteln. Es sei auch eine Aufgabe der Krankenkassen, Schulabgänger wegen des Abschlusses einer Krankenversicherung anzusprechen.

Ich habe den zuständigen Schulleiter gefragt, ob die Schule personenbezogene Daten der Schüler an Krankenkassen übermittelt. Er hat mir versichert, daß dies nicht der Fall sei. Dem Vater habe ich darauf hin mitgeteilt, daß er bzw. seine Tochter Auskunft über die gespeicherten Daten und gegebenenfalls ihre Löschung von der Krankenkasse verlangen kann. Da ich für die Kontrolle des Datenschutzes bei den bundesweiten Ersatzkassen nicht zuständig bin, habe ich den Bundesbeauftragten für den Datenschutz gebeten, die Beschwerde weiter zu bearbeiten und die Rechte der Betroffenen gegenüber der Krankenkasse geltend zu machen.

In einem anderen Fall hatte eine Ersatzkasse im August 1994 öffentliche Stellen des Landes ersucht, die Adressen neuer Mitarbeiter auf einem beigefügten Formular an sie zu übermitteln. Begründet wurde dies mit dem gesetzlichen Auftrag, über die Sozialversicherung aufzuklären und zu beraten (§§ 13 und 14 SGB I). Die Krankenkassen sind jedoch nicht berechtigt, zu diesem Zweck Sozialdaten zu erheben, zu verarbeiten und zu nutzen. Ich habe der anfragenden öffentliche Stelle mitgeteilt, daß die Datenübermittlung für Werbungszwecke nur zulässig ist, wenn der Betroffene eingewilligt hat. Darüber hinaus habe ich den öffentlichen Stellen unseres Landes meine Rechtsauffassung zur Kenntnis gegeben und um deren Beachtung gebeten.

Nach mir vorliegenden Informationen will der Bundesgesetzgeber im Rahmen der nächsten Stufe der Gesundheitsstrukturreform eine Regelung in das Sozialgesetzbuch aufnehmen, die es den gesetzlichen Krankenkassen gestattet, noch festzulegende Daten für Werbungszwecke zu erheben, zu verarbeiten und zu nutzen. In diesem Falle wäre die Nutzung von Daten für diese Zwecke gegebenenfalls neu zu beurteilen.

2.11.12. Empfehlungen für Wohnungsämter

Im Jahr 1994 habe ich eine Kontrolle in einem Wohnungsamt durchgeführt.

Das Amt ist in zwei Abteilungen gegliedert. Eine Abteilung ist zuständig für die Bearbeitung von Wohngeldanträgen und die andere für Anträge auf Ausstellung von Wohnberechtigungsscheinen sowie Anträge auf Wohnungsbauförderung. In beiden Abteilungen werden personenbezogene Daten automatisiert verarbeitet. Die Mitarbeiter des Amtes sind zur Wahrung des Sozialgeheimnisses verpflichtet und nehmen einmal jährlich an Fortbildungsveranstaltungen zum Datenschutz teil.

Die Antragsdaten für Wohngeld werden nach dem Beratungsgespräch von einem Mitarbeiter erfaßt und in einer Datei gespeichert. Alle Mitarbeiter dieser Abteilung können auf den gesamten Datenbestand zugreifen und in den Dateien ohne Einschränkung recherchieren. Die Aktivitäten werden automatisch protokolliert. In einigen Dateien befinden sich Bemerkungs- und Notizfelder, für die keine Benutzungseinschränkungen festgelegt sind.

Die Abteilung Wohnungswesen und Wohnungsbauförderung verarbeitet die Daten der Antragsteller auf Einzelplatz-PC. Die Daten für die Wohnberechtigungsscheine sind verschlüsselt auf der Festplatte des Rechners gespeichert und durch eine sechsstellige Nutzerkennzahl sowie ein persönliches Paßwort geschützt.

Ich habe dem Amt für Wohnungswesen empfohlen, die Recherchemöglichkeiten in den Dateien auf die erforderlichen Suchkriterien einzuschränken oder diese in einer Dienstanweisung festzulegen. Die Zugriffsprotokolle sind regelmäßig auszuwerten und Aufbewahrungs- bzw. Löschungsfristen dafür vorzugeben. Außerdem ist der Dateninhalt für sämtliche Felder zu bestimmen, um das Speichern unzulässig erhobener oder willkürlicher Daten auszuschließen (siehe auch Punkt 2.11.1). Die Sicherungskopien der Dateien sind in einem feuerfesten und einbruchssicheren Schrank aufzubewahren.

Der Amtsleiter hat in seiner Stellungnahme die Realisierung der Empfehlungen zugesagt.

2.12. Gesundheitswesen

2.12.1. Gesetz über den Öffentlichen Gesundheitsdienst im Land Mecklenburg-Vorpommern (ÖGDG M-V)

Die Landesregierung hat Ende 1993 einen Gesetzentwurf über den öffentlichen Gesundheitsdienst vorgelegt, der bereichsspezifische Bestimmungen zum Umgang mit personenbezogenen Daten enthielt und zu dem ich um Stellungnahme gebeten wurde.

Im Abschnitt zum Datenschutz war ursprünglich eine Regelung enthalten, daß personenbezogene Daten, die für Beratungen benötigt werden und Dritte betreffen, auch bei anderen Personen und Stellen ohne Kenntnis der Betroffenen erhoben werden können.

Diese Bestimmung normierte in gravierender Weise eine Einschränkung des Rechts auf informationelle Selbstbestimmung und war kaum geeignet, das notwendige Vertrauensverhältnis auf beiden Seiten herzustellen.

In der Diskussion zu dem Gesetzentwurf erklärten die zuständigen Referenten, daß es Zweck dieser Norm sei, auch Daten zur Familienanamnese und zum sozialen Umfeld einer zu beratenden Person zu verarbeiten und zu nutzen. Damit jedoch die Datenerhebung über Dritte bei anderen Personen und Stellen zu begründen, entspricht nicht den Grundsätzen der Verhältnismäßigkeit und Erforderlichkeit. Ob eine Beratung zum Erfolg führt, dürfte in erster Linie von der Mitarbeit und Einbeziehung des Betroffenen, auch in die Datenerhebung, abhängig sein.

Diese Daten können, soweit es erforderlich ist, beim Betroffenen selbst erhoben werden. In der ärztlichen Praxis geschieht dies regelmäßig ohne die Befugnis des Erhebens bei anderen Personen und Stellen. Außerdem sind Daten zur Familienanamnese auch personenbezogene Daten des Betroffenen, da sie mit ihm unmittelbar in Beziehung stehen.

Meine Empfehlung zur Neufassung der Datenschutznorm wurde aufgegriffen. Nunmehr ist geregelt, daß der öffentliche Gesundheitsdienst die im Rahmen der Beratung erforderlichen Daten über Dritte bei der zu beratenden Person erheben darf, und es wurde eine begrenzte Unterrichtungsregelung der Dritten aufgenommen.

Der Gesetzentwurf enthielt des weiteren die Bestimmung, daß der öffentliche Gesundheitsdienst personenbezogene Daten für andere ihm obliegende Aufgaben verarbeiten und nutzen darf, auch wenn sie einem besonderen Berufsgeheimnis unterliegen.

Mit dieser Formulierung wäre eine Zweckdurchbrechung möglich geworden. Die Regelung ist jedoch aus datenschutzrechtlicher Sicht besonders kritikwürdig. Sie ist unbestimmt und normiert nicht, welche Daten für welche anderen Aufgaben genutzt werden dürfen und unter welchen Voraussetzungen dies zulässig sein soll. Außerdem wäre es hiernach möglich, Daten, die im Rahmen einer freiwilligen Beratung erhoben wurden, auch für Pflicht- und Überwachungsaufgaben des öffentlichen Gesundheitsdienstes zu verwenden. Die ratsuchenden Bürger hätten somit keine Gewißheit, daß ihre im vertraulichen Gespräch offenbarten Angaben auch geheimgehalten werden.

Aus diesem Grunde hatte ich die Formulierung eines Nutzungsverbotes und einer Geheimhaltungspflicht empfohlen, die nur durch gesetzliche Meldepflichten, etwa nach dem Bundesseuchengesetz oder dem Strafgesetzbuch, durchbrochen werden können. Dies wurde mit der Begründung abgelehnt, daß zum Beispiel eine über die Geheimhaltungsvorschrift des Strafgesetzbuchs hinausgehende Beschränkung nicht erforderlich sei.

Ein Zweckbindungsgebot und die Gewährleistung der Trennung zwischen personenbezogenen Daten für Beratungsaufgaben sowie denen für andere Aufgaben wurden entsprechend meiner Empfehlung in das Gesetz aufgenommen.

2.12.2. Gemeinsames Krebsregister

Seit dem 1. Januar 1995 ist in der Bundesrepublik das Krebsregistergesetz (KRG) in Kraft, das durch Ausführungsbestimmungen der Bundesländer weiter ausgestaltet werden kann. Das KRG enthält bereits wesentliche Regelungen über die Meldungen an das Register sowie über den Umgang mit den Daten. Danach sind Ärzte berechtigt, Angaben über an Krebs erkrankte Patienten an eine Vertrauensstelle zu melden. Die Patienten sind zum frühestmöglichen Zeitpunkt über die Meldungen zu unterrichten und auf ihr Widerspruchsrecht hinzuweisen. Die personenbezogenen und epidemiologischen Daten werden in der Vertrauensstelle voneinander getrennt und letztere in einer Registerstelle gespeichert. Die Daten in der Registerstelle gestatten nach menschlichem Ermessen keinen Rückschluß auf eine bestimmte Person und stehen der wissenschaftlichen Forschung zur Verfügung.

Auf eine schriftliche Einwilligung der Patienten zum Zeitpunkt der Meldung hat der Gesetzgeber mit dem Hinweis verzichtet, daß bis dahin mindestens 20 % der Patienten noch nicht über ihre Krankheit aufgeklärt werden können oder aus anderen Gründen nicht einwilligungsfähig seien und deshalb die Erfassung unzureichend wäre. Die Datenschutzbeauftragten haben Empfehlungen zum KRG gegeben und im wesentlichen die Bestimmungen mitgetragen, da ein Verfahren angewendet wird, das die informationelle Selbstbestimmung der Betroffenen gewährleistet.

Die neuen Bundesländer und Berlin beabsichtigen, ein gemeinsames Krebsregister einzurichten und das ehemalige Krebsregister der DDR fortzuführen. Dazu sollen im wesentlichen gleichlautende Krebsregisterausführungsgesetze in den Ländern in Kraft treten. Die Datenschutzbeauftragten der neuen Länder sowie der Berliner Datenschutzbeauftragte haben am 8. September 1995 diese Gesetzentwürfe beraten und eine gemeinsame Stellungnahme (siehe Anlage 28) erarbeitet.

Die folgenden daraus resultierenden Empfehlungen habe ich an den Sozialminister unseres Landes gesandt und ihn gebeten, sie im Gesetzentwurf zu berücksichtigen:

- Es sollte ein Staatsvertrag für die Regelungen, die grundrechtsrelevante Wirkung entfalten, geschlossen werden. Vor allem ist zu regeln, welche Daten im einzelnen welchem Landesrecht unterliegen und wer für die datenschutzrechtliche Kontrolle zuständig sein soll.
- Die bereits vor dem Inkrafttreten des KRG gemeldeten Daten sollten ebenfalls von der Vertrauensstelle und nicht wie vorgesehen von der Registerstelle übernommen werden.
- Die Verfahrensfragen für Forschungsvorhaben bedürfen einer rechtlichen Regelung. Ebenso sind Bestimmungen zur organisatorischen, räumlichen und personellen Trennung der Registerstelle und der Vertrauensstelle sowie zur Aufsicht über das gemeinsame Krebsregister aufzunehmen.
- Es dürfen nur Daten der Leichenschauscheine an das Register übermittelt werden, die nicht über den Datenkatalog des Krebsregistergesetzes hinausgehen.
- Nach dem KRG können Daten für bestimmte Zwecke abgeglichen bzw. entschlüsselt werden, wofür die Einwilligung des Betroffenen bzw. seiner Angehörigen erforderlich ist. Bei Verstorbenen ohne Angehörige gibt es eine Regelungslücke, die zu schließen ist.
- Die vorgesehene Datenübermittlung an klinische Krebsregister ist ersatzlos zu streichen, da sie nicht durch den Gesetzeszweck des KRG gedeckt ist.
- Die im Gesetzentwurf vorgesehene uneingeschränkte Übertragung von Landesbefugnissen nach dem KRG auf ein Land sollte aus verfassungsrechtlichen Gründen nicht übernommen werden.
- Gemeldete Daten, die nicht unter das KRG fallen, sollten vorbehaltlich archivrechtlicher Regelungen gelöscht werden.

Inzwischen liegt ein aus datenschutzrechtlicher Sicht akzeptabler Referentenentwurf eines Krebsregister-Ausführungsgesetzes für das Land Mecklenburg-Vorpommern vor.

2.12.3. Altakten in den Gesundheitsämtern - ohne Befund

Im Ersten Tätigkeitsbericht hatte ich die Zustände bei der Aufbewahrung von Patientenakten ehemaliger Polikliniken in einem Gesundheitsamt beanstandet. Eine Nachkontrolle sollte zeigen, ob und inwieweit sich die Situation dort verändert hat.

Die seinerzeit beschriebenen baulichen Mängel waren inzwischen behoben. Allerdings standen die zum Erfassen, Sichern und Verwalten des Bestandes erforderlichen Arbeitskräfte immer noch nicht zur Verfügung und die Beschaffung geeigneter Hilfsmittel, etwa Regale, scheiterte bisher an unzureichenden finanziellen Mitteln.

Zum Zeitpunkt der Nachkontrolle war ca. die Hälfte des Bestandes grob vorsortiert. Allerdings wurden die ursprünglichen Sortierungsmerkmale der Polikliniken beibehalten, so daß es bei einem Personalwechsel schwer fallen dürfte, die erforderliche Übersicht zu wahren und die von Patienten oder Ärzten angeforderten Akten in einer angemessenen Zeit aufzufinden. Erste Fortschritte wurden beim Erfassen der Röntgen- und Schirmbildaufnahmen erzielt. Zu diesem Zweck ist eine Datei angelegt worden, die den Namen und Vornamen des Patienten sowie eine laufende Nummer, das Datum der Aufnahme, den Fundort, das Herausgabedatum, die Empfängeradresse und das Rückgabedatum enthält. Die formalen Erfordernisse des Landesdatenschutzgesetzes bei der automatisierten Datenverarbeitung, wie das Anlegen einer Dateibe-

schreibung und eines Geräteverzeichnisses, sind jedoch erst nach meiner Aufforderung erfüllt worden.

Unsicherheiten gab es zur Einsichtnahme Betroffener in ihre Akten bzw. zur Herausgabe von Unterlagen an Berechtigte. Ich habe dem Gesundheitsamt empfohlen, daß die Betroffenen ihre Akte im Beisein eines Arztes einsehen sollten, da sie selbst in der Regel nicht über den erforderlichen medizinischen Sachverstand verfügen und deshalb Fehlinterpretationen nicht auszuschließen sind. Die Akte kann mit Einwilligung des Betroffenen auch zur Einsichtnahme an den Hausarzt übersandt werden. Fordern Träger der gesetzlichen Sozialversicherung oder Berufsgenossenschaften zur Erfüllung von sozialen Aufgaben oder im Interesse des Patienten dessen Unterlagen an, ist die Zusendung ebenfalls nur mit seiner Einwilligung zulässig. Das Gesundheitsamt sollte sich in diesen Fällen von der anfordernden Stelle schriftlich bestätigen lassen, daß die Einwilligungserklärung vorliegt. Ihre Übermittlung an das Gesundheitsamt ist nicht erforderlich. Darüber hinaus ist zu beachten, daß nur die von der anfordernden Stelle bezeichneten Unterlagen übermittelt werden. Enthält eine Akte noch andere Schriftstücke, die mit dem konkreten Fall nicht in Verbindung stehen und in deren Weitergabe der Patient nicht eingewilligt hat, so ist deren Übermittlung unzulässig.

Das Gesundheitsamt hat zugesagt, entsprechend zu verfahren.

Die rechtliche Situation zum Umgang mit Patientenakten hat sich durch eine Regelung im Gesetz über den Öffentlichen Gesundheitsdienst im Land Mecklenburg-Vorpommern (ÖGDG M-V) gebessert. Danach haben jetzt die Landräte und die Oberbürgermeister (Bürgermeister) der kreisfreien Städte dafür zu sorgen, daß die medizinischen Unterlagen der aufgelösten Einrichtungen des Gesundheitswesens der DDR innerhalb der vorgesehenen Fristen sicher aufbewahrt werden und für Betroffene und sonstige Berechtigte zugänglich sind. Dies war ein wichtiger Schritt, um den Bestand der Patientenakten im Interesse der Bürger zu sichern.

2.12.4. Übermittlung von Daten Neugeborener - das gläserne Baby

Der Datenschutzbeauftragte eines Krankenhauses hat mich darauf aufmerksam gemacht, daß die Entbindungsstation regelmäßig Gesundheitsdaten von Neugeborenen an das Gesundheitsamt des Landkreises übermittelt. Zu diesem Zweck wurde ein Erhebungsbogen des ehemaligen Gesundheitsdienstes der DDR verwendet.

Schon meine Anfrage beim Amtsarzt, auf welcher rechtlichen Grundlage und zu welchem Zweck die Daten übermittelt werden, stieß auf Unverständnis. Das Standesamt würde dem Gesundheitsamt auf der Grundlage des Personenstandsgesetzes doch sowieso Geburtenmeldungen zusenden, und die würden zusammen mit den Daten der Entbindungsstationen archiviert. Im übrigen fordere das Gesundheitsamt die Daten nicht ab, sondern die Entbindungsstationen senden die ausgefüllten Erhebungsbogen zu. Das Gesundheitsamt hätte also keinen Grund, den Empfang der Daten aus den Krankenhäusern abzulehnen. Die Daten würden von den Fürsorgerinnen für Beratungszwecke genutzt. Die Aufforderungen für die Beratungen kämen von Haus- und Kinderärzten bzw. den Hebammen.

Die rechtlichen Grundlagen für Übermittlungen von Patientendaten aus Krankenhäusern sind im Landeskrankenhausgesetz (LKHG M-V) enthalten. Nach den Bestimmungen des LKHG M-V ist es zulässig, Patientendaten auf Wunsch des Betroffenen zur sozialen oder seelsorgerischen Betreuung und - soweit dies erforderlich ist - an Stellen außerhalb des Krankenhauses zu übermitteln. Daten der Neugeborenen dürfen danach mit Einwilligung der Personensorgeberechtigten im erforderlichen Umfang für Beratungszwecke übermittelt werden. In diesem Fall sind sie jedoch auf nicht mehr zulässigen Vordrucken in den Entbindungsstationen und ohne Einwilligung erhoben und übermittelt worden. Außerdem enthielt das Formular Angaben, die zur Anbahnung einer Beratung nicht erforderlich sind, etwa zu Beruf und Tätigkeiten der Personensorgeberechtigten. Des weiteren waren Felder für ansteckende Krankheiten, Hirnhautentzündung, Sprach- und Verhaltensstörungen und die PKZ der ehemaligen DDR vorgesehen.

Das Gesundheitsamt soll gemäß dem ÖGDG M-V Beratungen anbieten und kann die dafür erforderlichen Daten erheben, verarbeiten und nutzen. Zuvor bleibt es aber der freien Entscheidung des Betroffenen überlassen, ob er die Beratung annimmt. Von einer schriftlichen Einwilligung in die Beratung kann abgesehen werden.

Die Übermittlung der umfangreichen Daten von Neugeborenen an das Gesundheitsamt war damit weder nach den Bestimmungen des LKHG M-V noch nach denen des ÖGDG M-V zulässig. Die Verantwortung für die Übermittlung lag zweifellos beim Krankenhaus, da das Gesundheitsamt die Daten nicht angefordert hatte. Dennoch trägt das Gesundheitsamt Verantwortung in Bezug auf die unzulässige Archivierung der eingegangenen Daten.

Entsprechend meiner Empfehlung hat der Amtsarzt die Vernichtung der ausgefüllten Formulare zugesagt.

Von seiten des Krankenhauses wurden diese Datenübermittlung inzwischen eingestellt.

2.12.5. Schulärztliche Untersuchungen

Eine Mutter hat sich bei mir über ein Schreiben beschwert, in dem Eltern über eine geplante Untersuchung des kinder- und jugendärztlichen Dienstes eines Gesundheitsamtes informiert werden. Die für diesen Zweck erforderlichen Daten sollten von Schülern auf freiwilliger Basis erhoben werden. Das Schreiben war nicht als amtliches Schreiben ausgewiesen, so daß die Mutter Zweifel hatte, ob die angekündigte Untersuchung rechtmäßig sei. Sie bat mich, den Sachverhalt zu prüfen.

Schulärztliche Untersuchungen vor der Einschulung und während der Schulzeit gehören nach dem ÖGDG M-V zu den Aufgaben des kinder- und jugendärztlichen Dienstes der Gesundheitsämter. Sie werden durchgeführt, um Krankheiten und Fehlentwicklungen frühzeitig zu erkennen und den Gesundheitszustand der Kinder und Jugendlichen festzustellen, soweit dies für schulische Entscheidungen bedeutsam ist. Der Sozialminister ist gemäß ÖGDG M-V ermächtigt, im Einvernehmen mit der Kultusministerin Art, Umfang und Zeitpunkt dieser Untersuchungen festzulegen. Eine Rechtsverordnung dazu wurde bisher noch nicht erlassen. Sie ist aber dringend erforderlich, damit Rechtssicherheit hergestellt wird.

Ich habe dem Gesundheitsamt empfohlen, die an die Eltern gerichteten Informationsschreiben über schulärztliche Untersuchungen künftig eindeutig als amtliche Schreiben auszuweisen. Es sollte für den Empfänger außerdem klar erkennbar sein, daß der Unterzeichnende ein Mitarbeiter des Gesundheitsamtes ist. Die Eltern sind über den Umgang der auf freiwilliger Basis erhobenen Daten sowie die Dauer der Speicherung aufzuklären. Des weiteren ist die Rechtsgrundlage zu nennen, nach der die medizinische Untersuchung der Schüler durchgeführt wird.

Mit dem Sozialminister habe ich abgestimmt, daß ein Erhebungsbogen zur schulärztlichen Untersuchung erarbeitet und zur landeseinheitlichen Verwendung empfohlen wird. Inzwischen wurde mir der Entwurf eines Formulars zugesandt, der meine Zustimmung findet. Die Datenerhebung soll wie bisher auf freiwilliger Basis erfolgen. Sollte darüber hinaus zur Vorbereitung der Schuluntersuchung eine Übermittlung von Daten, wie zum Beispiel Name und Anschrift der Schüler, von der Schule an das Gesundheitsamt erforderlich sein, so ist es sinnvoll, dies im noch ausstehenden Schulgesetz zu normieren.

2.12.6. Krankenhausaufnahmevertrag

Ein Bürger hat bei mir angefragt, ob die Daten "Arbeitgeber" und "Beruf" im Zusammenhang mit der Aufnahme in ein Krankenhaus regelmäßig erhoben werden dürfen.

Nach den Bestimmungen des LKHG M-V ist es zulässig, Patientendaten, soweit es erforderlich ist, für folgende Zwecke zu erheben und zu speichern (§ 15 LKHG M-V):

- zur Erfüllung des Behandlungsvertrages, einschließlich der ärztlichen Dokumentationspflicht und Pflegedokumentation,
- zur sozialen und seelsorgerischen Betreuung des Patienten, wenn die Einwilligung nicht eingeholt werden kann und der mutmaßliche Wille des Patienten nicht entgegensteht,
- zur Leistungsabrechnung und Abrechnung von Ansprüchen aus der Behandlung.

Die Daten "Beruf" und "Arbeitgeber" können im Einzelfall bei Arbeitsunfällen und Berufskrankheiten erforderlich sein, um den zuständigen Kostenträger festzustellen, aber nicht regelmäßig zur Leistungsabrechnung und Abwicklung von Ansprüchen. Deshalb habe ich empfohlen, im Erhebungsbogen klar zum Ausdruck zu bringen, welche Daten ständig zur Aufgabenerfüllung angegeben werden müssen und welche auf freiwilliger Basis erhoben werden. Letzteres trifft zum Beispiel auch auf die Frage nach der "Konfession" zu, die im Zusammenhang mit dem Wunsch nach seelsorgerischer Betreuung gestellt werden kann (§ 17 Abs. 1 Nr. 10 LKHG M-V).

Der Verwaltungsdirektor des Krankenhauses hat zugesichert, bei einer Neuauflage der Formulare meine Empfehlung zu berücksichtigen. Bis dahin wird dem Vertrag ein entsprechendes Informationsblatt beifügt.

2.12.7. Datenübermittlung im Krankenhaus

Ein Patient hat sich bei mir darüber beschwert, daß während seiner Krankenhausbehandlung ein Befundbericht mit Diagnosen von einer Abteilung erstellt wurde, die nicht in diesem Umfang in die Behandlung einbezogen war. Es war ihm unklar, woher die Abteilung seine medizinischen Daten hatte. Außerdem hatte er bei einem Spaziergang auf dem Klinikgelände ein ausgefülltes Formular mit Daten einer Patientin gefunden und äußerte deshalb den Verdacht, daß es mit dem Patientendatenschutz hier offensichtlich nicht zum besten bestellt sei.

Der Direktor der Klinik hat auf meine Anfrage zum ersten Punkt mitgeteilt, daß die Aufklärung des Krankheitsbildes dieses Patienten eine umfassende Diagnose verlangte. Dies war bei der hochspezialisierten Behandlung nur durch die kooperative Zusammenarbeit verschiedener Fachabteilungen zu erreichen. Der Patient wurde über die notwendige Einbeziehung einer anderen Abteilung informiert und hat durch seine Teilnahme an der Untersuchung schließlich darin eingewilligt. Das Landeskrankenhausgesetz (§ 16 Abs. 3 LKHG M-V) und der Krankenhausaufnahmevertrag lassen die Datenübermittlung zwischen verschiedenen Fachabteilungen zu, soweit dies für eine Mitbehandlung erforderlich ist.

Ich konnte nicht feststellen, daß Daten übermittelt worden sind, die zur Behandlung nicht erforderlich waren. Gleichwohl halte ich es für angebracht, die Patienten nicht nur über die Behandlung, sondern auch über die Weitergabe ihrer Daten aufzuklären.

Zum zweiten Punkt hat der Direktor mitgeteilt, daß das auf dem Klinikgelände gefundene ausgefüllte Formular wahrscheinlich durch Unachtsamkeit eines Mitarbeiters verlorengegangen sei. Anläßlich einer Dienstbesprechung hat er den Vorfall ausgewertet und alle Mitarbeiter nochmals auf den sorgsamen Umgang mit Patientenunterlagen hingewiesen. Des weiteren hat er festgelegt, daß sämtliche Befunde und Schriftstücke unverzüglich den Krankenunterlagen beizufügen sind, um derartige Vorfälle künftig zu vermeiden.

2.12.8. Darf ein Rechtsanwalt eine Patientenakte einsehen?

Ein Krankenhaus erhielt Post von einem Rechtsanwalt. Der Anwalt wollte die Akte eines verstorbenen Patienten einsehen oder sie kurzzeitig mitnehmen, um zivilrechtliche Ansprüche für die durch ihn vertretenen Erben durchzusetzen. Der Datenschutzbeauftragte des Krankenhauses hat mich um Beratung in dieser Angelegenheit gebeten.

Im Landeskrankenhausgesetz (LKHG M-V) ist festgelegt, daß Patienten kostenfrei Einsicht in die Krankenunterlagen einschließlich der ärztlichen und pflegerischen Dokumentation zu gewähren ist (§ 18 Abs. 1 LKHG M-V) und daß Patientendaten an Personen oder Stellen außerhalb des Krankenhauses unter anderem zur Unterrichtung von Angehörigen und zur Durchsetzung von Ansprüchen aus dem Behandlungsvertrag, soweit dies erforderlich ist, übermittelt werden können (§ 17 Abs. 1 Nrn. 4 und 7 LKHG M-V).

Der Anspruch auf Einsichtnahme geht auf die Erben über, soweit es zur Klärung vermögensrechtlicher Fragen, etwa bei Schadensersatzansprüchen infolge eines vermuteten Behandlungsfehlers, erforderlich ist. Dieses Recht kann jedoch mit der ärztlichen Schweigepflicht kollidieren, die grundsätzlich auch gegenüber den Erben oder nahen Angehörigen gilt und nicht durch den Tod des Patienten erlischt (§ 203 Abs. 4 StGB). Der Arzt muß deshalb die Einsicht in die Krankenunterlagen verweigern, wenn kein Rechtfertigungsgrund vorliegt. Für diese Entscheidung muß er sorgfältig prüfen, ob der Verstorbene die partielle oder vollständige Einsichtnahme gegenüber den Erben mißbilligt hätte.

Die Erben müssen ihr Interesse an der Kenntnisnahme der Krankenunterlagen konkret darlegen, so daß der Arzt alle Umstände einbeziehen und sachgerecht entscheiden kann. Die Hinterbliebenen haben einen klagbaren Anspruch gegen den Arzt oder das Krankenhaus auf Einsichtsgewährung, wenn sie zum Beispiel Schadensersatzansprüche wegen eines Behandlungsfehlers geltend machen oder eine Anzeige wegen fahrlässiger Tötung erstatten wollen.

Ich habe dem Datenschutzbeauftragten des Krankenhauses empfohlen, von dem Rechtsanwalt ein Schriftstück zu erbitten und in die Akte zu übernehmen, aus dem hervorgeht, daß die Angehörigen das Einsichtsrecht durch ihn wahrnehmen lassen wollen. Darin sollte der Grund für die Einsichtnahme genannt sowie der Teil der Akte bezeichnet werden. Wenn der Arzt entschieden hat, Einsicht zu gewähren, könnten auch Kopien der Unterlagen, jedoch nicht die vollständige Originalakte, übermittelt werden. Die herausgegebenen oder übermittelten Kopien sind zu registrieren und der entsprechende Nachweis ist in die Akte zu übernehmen.

2.12.9. Patientendaten für die Berufsschule

Ein Mitarbeiter eines Krankenhauses hat angefragt, ob es zulässig sei, Patientendaten für Schulungszwecke außerhalb des Krankenhauses zu nutzen. Es war vorgesehen, die Daten von Krebspatienten für Ausbildungszwecke an eine berufliche Schule zu übermitteln. Name, Vorname, Anschrift, Geburtsdatum und Krankenkasse sollten dabei nicht übermittelt werden.

Nach dem LKHG M-V können Patientendaten für die im Krankenhaus durchgeführte Ausbildung in ärztlichen oder anderen Fachberufen des Gesundheitswesens genutzt werden, soweit der Zweck nicht mit anonymisierten Daten erreicht werden kann (§ 16 Abs. 1 LKHG M-V). Diese Voraussetzung war nicht erfüllt, denn die Schule ist nicht Teil des Krankenhauses.

Ich habe empfohlen, die Daten nicht an die berufliche Schule zu übermitteln.

2.12.10. Arztbericht an uns gefaxt - Diagnose: Datenschutz ungenügend

Im Okober 1995 ging versehentlich ein Fax in meiner Dienststelle ein, das für einen Arzt einer neurochirurgischen Abteilung bestimmt war. Es handelte sich dabei um einen recht umfangreichen Diagnose- und Befundbericht. Ich habe die Patientin über die Fehlleitung ihres Befundberichtes schriftlich informiert und den Chefarzt der absendenden Klinik um Stellungnahme gebeten.

In seiner Antwort führt er aus, daß die Übermittlung des Berichtes dringend erforderlich gewesen sei. Deshalb wurde der Arztbrief per Fax geschickt. Zur Fehlleitung sei es gekommen, weil die Faxnummer falsch registriert worden war.

Die Krankenhausleitung hat den Vorfall mit den Ärzten und Schwestern der Klinik ausgewertet. Der Chefarzt hat sich bei der Patientin entschuldigt. Ich habe das Klinikum auf die Risiken bei der Übermittlung von Patientendaten per Telefax und die notwendigen Sicherheitsmaßnahmen aufmerksam gemacht. Auf eine Beanstandung habe ich in diesem Fall verzichtet.

In meiner Dienststelle ist zum Thema "Datenschutz und Telefax" ein Informationsblatt erhältlich.

2.12.11. Wirtschaftsprüfer als Datenschutzbeauftragter im Krankenhaus?

Eine Wirtschaftsprüfungs- und Steuerberatungsaktiengesellschaft hat mir mitgeteilt, daß einer ihrer Mitarbeiter zum Datenschutzbeauftragten eines Klinikums bestellt worden ist. Daraufhin habe ich den Verwaltungsdirektor des Klinikums befragt, warum er einen externen Datenschutzbeauftragten bestellt hat. Der Verwaltungsdirektor hat dargelegt, daß im Rahmen der wirtschaftlichen Betriebsführung nach den Vorgaben des Ministeriums alle Möglichkeiten des Outsourcing genutzt werden sollen und außerdem kein Mitarbeiter zur Verfügung steht, der die erforderliche Fachkunde besitzt. Darüber hinaus sei bei den Mitarbeitern des Klinikums ein Interessenkonflikt mit anderen Aufgaben zu befürchten.

Die schriftliche Bestellung eines Datenschutzbeauftragten ist im Landeskrankenhausgesetz vorgeschrieben (§ 22 LKHG M-V). Dort ist auch festgelegt, daß nur Personen mit dieser Aufgabe betraut werden dürfen, die dadurch keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt sind.

Durch diese Regelung kommt indirekt die Intention des Gesetzgebers zum Ausdruck, einen Mitarbeiter des Krankenhauses mit dieser Aufgabe zu betrauen, denn sonst wäre die Erwähnung der Konfliktsituation überflüssig. Aus dieser Sicht ist beispielsweise der Leiter des Krankenhausrechenzentrums nicht besonders geeignet, da er sich zumindest im Hinblick auf die automatisierte Datenverarbeitung selbst kontrollieren müßte.

Des weiteren ist in der Gesetzesbegründung zum LKHG M-V ausgeführt, daß der Beauftragte für den Datenschutz laufend an Datenverarbeitungsverfahren zu beteiligen ist und Ansprechpartner für die Patienten sein soll. Auch dies spricht für einen internen Beauftragten. Die unterstützenden Kontrollbefugnisse könnten im Falle des Einsatzes eines externen Datenschutzbeauftragten nur unvollkommen wahrgenommen werden, da er nicht ohne weiteres befugt ist, Patientendaten zur Kenntnis zu nehmen.

Dem Verwaltungsdirektor habe ich empfohlen, einen internen Datenschutzbeauftragten zu bestellen.

Der Direktor sah hierzu noch Klärungsbedarf und hat mich zu einem Gespräch mit dem Vorstand des Klinikums eingeladen. Dabei wurde zunächst die Auffassung vertreten, daß mit der Bestellung eines externen Datenschutzbeauftragten auch die Verantwortung für den Umgang mit den Patientendaten übertragen wird. Die gesetzlichen Vorschriften lassen dies jedoch nicht zu. Deshalb konnte schließlich Einigung über die Bestellung eines internen Datenschutzbeauftragten erzielt werden. Ende des Jahres 1994 wurde mir der betreffende Mitarbeiter genannt und darauf hingewiesen, daß er unmittelbar dem Vorstand unterstellt und organisatorisch dem Verwaltungsdirektor zugeordnet ist.

Das Landeskrankenhausgesetz regelt außerdem, daß spätestens bis zum 1. Januar 1995 mindestens ein Datenschutzbeauftragter schriftlich zu bestellen und dem Sozialminister mitzuteilen ist. Ich habe den Sozialminister im September 1995 gebeten, mir die Namen sowie die Dienststellung der Beauftragten mitzuteilen. Der mir daraufhin zugesandten Aufstellung ist zu entnehmen, daß von den 38 Krankenhäusern des Landes bisher erst 8 dieser Verpflichtung nachgekommen sind. Der Sozialminister hat mein Schreiben zum Anlaß genommen, um die Krankenhäuser auf ihre gesetzliche Pflicht hinzuweisen.

2.12.12. Notarztprotokoll

Den Trägern des öffentlichen Rettungsdienstes ist die Verwendung eines landeseinheitlichen Einsatzprotokolls vorgeschrieben (§ 13 Abs. 1 Rettungsdienstgesetz Mecklenburg-Vorpommern). Der Sozialminister hatte mir den für diesen Zweck vorgesehenen Entwurf zugesandt und mich um datenschutzrechtliche Prüfung gebeten. Er hat mitgeteilt, daß angestrebt wird, das Protokoll bundeseinheitlich zu verwenden. Es ist als Original mit zwei Durchschriften auszufertigen und dient der Dokumentation. Darüber hinaus sollte es für statistische Zwecke genutzt werden.

Das Einsatzprotokoll enthält Identifikationsdaten einschließlich Krankenversicherung und Versichertenstatus des Patienten, rettungstechnische Daten, Angaben zum Notfallgeschehen, Befund, Diagnose, Daten über den Verlauf von Körperfunktionen, eingeleitete Maßnahmen, Angaben zur Übergabe des Patienten zur weiteren Behandlung und zum Ergebnis des Einsatzes sowie Bemerkungen.

Zur Gestaltung habe ich folgende Empfehlungen gegeben:

- Der Verwendungszweck des Originals und jeder einzelnen Durchschrift muß durch einen entsprechenden Aufdruck erkennbar sein.
- Es ist zu prüfen, ob jedes Datum vom Original auf die Mehrfertigungen durchgeschrieben werden muß.
- Daten für Forschungszwecke oder Statistiken sind zu anonymisieren, sobald der Zweck dies zuläßt. Das betrifft neben den Daten des Patienten auch Daten des Rettungsarztes und der Rettungsassistenten sowie die Einsatznummer und das vollständige Einsatzdatum.
- Im Feld der Identifikationsdaten des Patienten ist das Datum "Arbeitgeber" nicht regelmäßig erforderlich und darf nur bei Arbeitsunfällen erhoben werden.

Der Sozialminister hat die Arbeitsgemeinschaft in Mecklenburg-Vorpommern tätiger Notärzte e. V. (AGMN) beauftragt, zu meinen Empfehlungen Stellung zu nehmen. In der Stellungnahme wird ausgeführt, daß der jeweilige Verwendungszweck der Ausfertigung auf den Rand gedruckt wird: "Original - Verbleib beim Patienten/Krankenakte", 1. Durchschlag "Einsatzdokumentation Notarztwache/ erste Rettungsmittel", 2. Durchschlag "Einsatzdokumentation zweite Rettungsmittel". Das Original wird entweder Bestandteil der Patientenakte des aufnehmenden Krankenhauses, oder es verbleibt bei ambulanten Behandlungen beim Patienten, damit er es dem Hausarzt zur Aufnahme in die Patientenakte übergeben kann. Die erste Durchschrift wird zur Dokumentation des Einsatzes beim ärztlichen Leiter des Rettungsdienstes unter Verschluß aufbewahrt. Diese Daten werden auch zur Leistungsabrechnung genutzt. Die zweite Durchschrift ist zur Einsatzdokumentation in Fällen notwendig, in denen der Rettungswagen und der Notarzt zeitversetzt oder von verschiedenen Rettungsstellen aus am Rettungsort eintreffen. Die erste Rettungswagenbesatzung hat häufig schon therapeutische Maßnahmen eingeleitet, so daß alle vorausgegangenen und nachfolgenden Maßnahmen dokumentiert werden müssen. Treffen Rettungswagen und Notarzt gleichzeitig ein, oder sind sie vom gleichen Leistungserbringer, wird die zweite Durchschrift vor dem Ausfüllen entfernt. Ein entsprechender Hinweis ist auf diesem Exemplar aufgedruckt. Die Daten des Originals müssen nach Aussage der Arbeitsgemeinschaft deshalb vollständig durchgeschrieben werden.

Die statistische Aufbereitung erfolgt durch das Personal der Rettungsstelle und nicht mehr anhand des Protokolls durch Dritte. Für diesen Zweck werden anonymisierte Daten in einer Datei erfaßt und für weitere Auswertungen auf Datenträgern an die zuständigen Stellen gesandt. Einsatznummer, Patientendaten (außer Geschlecht und Alter), Namen des Personals oder Bezeichnung der Rettungsstelle werden zu diesem Zweck nicht gespeichert.

Der Sozialminister hat außerdem zugesichert, das Datum "Arbeitgeber" im Feld der Patientendaten künftig nicht zu erheben.

2.13. Personalwesen

2.13.1. Verwaltungsvorschrift für die Personalakte erlassen

Der Innenminister unseres Landes hat im Mai 1994 einen Entwurf für eine Verwaltungsvorschrift zu den §§ 100 bis 107 Landesbeamtengesetz von Mecklenburg-Vorpommern (LBG M-V) erarbeitet und mir zur datenschutzrechtlichen Stellungnahme übersandt.

Zu diesem Entwurf habe ich Empfehlungen gegeben.

Beispielsweise war in der ersten Fassung geregelt, daß die Personalakte auf der äußeren Seite mit dem Namen, dem Vornamen, dem Geburtsdatum und im Falle einer Schwerbehinderung auch mit dieser Eigenschaft zu kennzeichnen ist.

Eine Differenzierung nach den Beschäftigungsgruppen Beamte, Angestellte und Arbeiter kann unter dem Gesichtspunkt der Aufgabenwahrnehmung der Personalsachbearbeiter hingenommen werden, nicht jedoch die weitere Unterteilung nach Behinderungen. Deshalb habe ich empfohlen, eine derartige Kennzeichnung nicht zu verwenden.

Weiterhin war zum Beispiel geregelt, wie zu verfahren ist, wenn eine Personalakte trotz aller Sicherungsmaßnahmen verlorengeht. In diesem Fall habe ich empfohlen, neben allen anderen Sofortmaßnahmen auch den Betroffenen unverzüglich zu informieren.

Ferner war vorgeschrieben, daß grundsätzlich keine Schriftstücke aus der Personalakte zu entfernen sind. Diese Formulierung kann jedoch nicht aufrechterhalten werden, da auch in Personalakten Unterlagen mit vorgegebenen Aufbewahrungsfristen, wie zum Beispiel Führungszeugnisse, enthalten sein können, die nach Ablauf der Frist zu entfernen sind.

Meine Empfehlungen wurden in der Verwaltungsvorschrift berücksichtigt.

Vor dem Inkrafttreten der Vorschrift wurde ich darauf aufmerksam gemacht, daß es bedenklich sei, wenn alle veralteten Personenstandsurkunden (Eheschließungs- und Scheidungsurkunden) der Beschäftigten offen in der Personalakte aufbewahrt werden und jeder Zugangsberechtigte zum Beispiel sofort erkennen kann, daß der oder die Betreffende bereits mehrere Male verheiratet war. Ich habe empfohlen, diese Personenstandsurkunden in einem geschlossenen Umschlag aufzubewahren, wenn es aus bestimmten Gründen weiterhin erforderlich ist. Diese Empfehlung wurde ebenfalls in die Vorschrift mit aufgenommen.

Der Innenminister hat die Verwaltungsvorschrift als Richtlinie über die Führung von Personalakten - Erlaß des Innenministers vom 13. Oktober 1994, im Amtsblatt Mecklenburg-Vorpommern Nr. 45 vom 1. November 1994 - veröffentlicht. Sie gilt in den obersten Landesbehörden sinngemäß auch für die Personalaktenführung der Arbeitnehmer, soweit tarifrechtliche Bestimmungen nicht entgegenstehen. Den Landkreisen, Gemeinden/Städten und Ämtern sowie den sonstigen Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts wurde empfohlen, ebenfalls nach dieser Vorschrift zu verfahren.

2.13.2. Einheitlicher Personalbogen in Mecklenburg Vorpommern?

Nach dem LBG M-V dürfen Personalfragebogen seit dem 1. Januar 1994 nur noch verwendet werden, wenn dafür die Genehmigung der zuständigen obersten Dienstbehörde vorliegt (§ 100 Abs. 4 LBG M-V) und darüber hinaus der Personalrat sein Mitbestimmungsrecht wahrnehmen konnte (§ 68 Abs. 1 Nr. 18 Personalvertretungsgesetz - PersVG -). Bei Kontrollen in Personalämtern hatte ich festgestellt, daß selbst in diesem Berichtszeitraum teilweise noch alte Formulare der DDR-Verwaltung verwendet wurden bzw. in den Personalakten vorhanden waren. Vor diesem Hintergrund hat das Innenministerium einen landeseinheitlichen Muster-Personalbogen entworfen, der den öffentlichen Stellen zur Verwendung empfohlen werden soll.

Den ersten Entwurf des Formulars erhielt ich im Mai 1994 zur Stellungnahme. Im zweiten Entwurf waren nicht alle meine Empfehlungen berücksichtigt. So hatte ich unter anderem empfohlen, Angaben über Strafen und über wirtschaftliche Verhältnisse, soweit dies überhaupt erforderlich ist, gesondert zu erheben. Da diese Daten nur temporär persönliche Verhältnisse des Betroffenen widerspiegeln, die nach Ablauf von Aufbewahrungsfristen bzw. nach Veränderung der Verhältnisse zu löschen sind, wäre die Speicherung auf dem Personalbogen nur zulässig, wenn dieser nach Eintritt der Veränderung entsprechend aktualisiert wird. Darauf habe ich in einer erneuten Stellungnahme aufmerksam gemacht.

Schließlich hat mir der Innenminister im Mai 1995 einen dritten Entwurf zugesandt, der diese beiden Angaben nicht mehr enthielt. Dafür war allerdings der in der ersten Fassung nicht vorhandene "Geburtsname der Mutter" aufgeführt. Es wurde begründet, daß diese Angabe zur Anforderung eines Führungszeugnisses erforderlich sei. In einer weiteren Stellungnahme habe ich darauf hingewiesen, daß die Erhebung des Geburtsnamens der Mutter für diesen Zweck unverhältnismäßig ist, denn Führungszeugnisse - auch behördliche - werden in der Regel vom Bediensteten beantragt. Nur im Ausnahmefall geschieht das durch die Behörde. Das Datum von allen Beschäftigten zu fordern, entspricht deshalb nicht dem Grundsatz der Verhältnismäßigkeit. Im Oktober 1995 wurde schließlich mitgeteilt, daß den obersten Landesbehörden empfohlen wird, auf diese Abfrage im Personalbogen zu verzichten. Der Muster-Personalbogen soll demnächst veröffentlicht werden.

2.13.3. PERSYS

Seit 1993 planen die Personalstellen unseres Landes die Einführung eines landeseinheitlichen Personal- und Stellenverwaltungssystems (siehe Erster Tätigkeitsbericht, Seite 117, Punkt 2.22.2). Nach einer Ausschreibung wurde das System PERSYS von der Koordinierungsstelle für Informationstechnik in der Landesverwaltung als Standard ausgewählt.

Bei den Beratungen zur Einsatzvorbereitung von PERSYS habe ich die Auffassung vertreten, daß ein einheitliches System deutliche datenschutzrechtliche Vorteile gegenüber den noch vorhandenen selbstentwickelten Lösungen der einzelnen Ressorts hat. Die automatisierte Personaldatenverarbeitung allein mit Standardsoftware wie dBase oder Excel genügt nicht in vollem Umfang datenschutzrechtlichen Anforderungen, denn die Protokollierung von Zugriffen auf einzelne Datenfelder ist beispielsweise nicht möglich.

Inzwischen ist die Anpassung von PERSYS an die in der Ausschreibung festgelegten Bedingungen erfolgt. Die Musterdienstvereinbarung sowie das Sicherheits- und Datenschutzkonzept wurden mir im Entwurf zur Stellungnahme vorgelegt. Folgende Empfehlungen habe ich gegeben:

- Jeder Nutzer muß prüfen, ob jedes Datenfeld des Dateiverzeichnisses für seine Personalverwaltung erforderlich ist; nicht erforderliche Datenfelder sind zu sperren.
- Die Daten des Personalverwaltungssystems dürfen nicht für andere Zwecke genutzt werden.
- Die Personaldaten ausgeschiedener Beschäftigter sind zu sperren und spätestens im darauf folgenden Kalenderjahr zu löschen.
- Die in den Unterlagen verwendeten Begriffe sollten den im Datenschutzrecht üblichen Begriffen angepaßt werden.

Diese Empfehlungen wurden inzwischen in der Musterdienstvereinbarung bzw. im Sicherheits- und Datenschutzkonzept berücksichtigt.

Nicht gefolgt wurde meiner Empfehlung, eine Grundeinstellung der von allen Personalstellen ohne Einschränkung zu nutzenden Datenfelder nach dem Prinzip des erforderlichen Minimums vorzunehmen. Alle darüber hinausgehenden Datenfelder könnten danach nur genutzt werden, wenn die Personalstelle in Abstimmung mit dem Personalrat die Verarbeitung für einen festgelegten Personenkreis für zulässig erklärt. Das Innenministerium sah sich nicht in der Lage, eine derartige Grundeinstellung zu realisieren, da die Anforderungen der anderen Ministerien zu unterschiedlich seien. Die Einzelprüfung der Datenfelder bleibt somit den Personalstellen unter Beteiligung der Personalräte überlassen.

In das Sicherheits- und Datenschutzkonzept sind auch Hinweise aus Veröffentlichungen des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) eingeflossen. Das BSI-Grundschutzhandbuch enthält einen Katalog der Objekte, Bedrohungen und Schutzmaßnahmen sowie Hinweise zum Sicherheitsmanagement, zur Paßwortgestaltung, zu Zutritts- und Zugriffsregelungen, zur Protokollierung, zum Datensicherungsverfahren und zum Datenträgeraustausch (siehe auch Punkt 2.16.5). Darüber hinaus sind folgende Anlagen beigefügt:

- technische Systembeschreibung,
- Dateiverzeichnis,
- Liste der Standardauswertungen,
- Regelungen zur Zulässigkeit der freien Datenbankabfrage mittels der Abfragesprache "Structured Query Language" (SQL),
- Personalstammblatt,
- Liste der Zugriffsberechtigten,
- Menüführung einschließlich Maskenaufbau.

Die Voraussetzungen zum Einsatz von PERSYS sind aus datenschutzrechtlicher Sicht nunmehr erfüllt.

Gegenwärtig wird PERSYS noch nicht umfassend in den obersten Landesbehörden angewendet, da die dafür vorgesehenen Haushaltsmittel auf Empfehlung des Finanzausschusses des Landtages vorläufig gesperrt sind. Der Ausschuß hat unter anderem bemängelt, daß keine Wirtschaftlichkeitsrechnung und damit keine Abwägung zwischen dem Einsatz in einem PC-Netz und der Nutzung eines Großrechners für Personalverwaltungszwecke durchgeführt worden ist. Außerdem würden eigentliche Effekte des Projektes verschenkt, wenn keine Zusammenführung der in den Ressorts verwalteten Personalstellen möglich sei.

In einem Schreiben an den Finanzausschuß habe ich dazu Stellung genommen und angemerkt, daß bei der Erarbeitung des Konzeptes eingehend untersucht worden ist, ob eine zentrale Datenhaltung auf einem Großrechner im Rahmen des geltenden Rechts wirtschaftlich möglich ist (LBG M-V, DSG MV). Die Untersuchungen ergaben, daß dies nicht der Fall ist, da die im LBG M-V definierten Zugriffseinschränkungen auf Personaldaten nur mit unverhältnismäßig hohem Aufwand an technisch-organisatorischen Maßnahmen gewährleistet werden könnten. In der Betreuung der Hard- und Software des Großrechners wäre beispielsweise der Kreis der Personen, die unvermeidlich Zugang zu Personaldaten haben, nicht mehr mit den Vorschriften des LBG M-V vereinbar.

Hinsichtlich der Effektivität habe ich in der Stellungnahme ausgeführt, daß umfangreiche Auswertungsmöglichkeiten mit anonymisierten Daten bei der Anwendung von PERSYS auf einem PC-Netz des jeweiligen Ressorts vorhanden sind und Stellenstatistiken erstellt werden können. Eine Schnittstelle zum automatisierten Datenabruf, zum Beispiel durch das Finanzministerium, ist jedoch gesetzlich nicht zulässig (§ 107 Abs. 1 LBG M-V).

2.13.4. Landesbesoldungsamt prüft Anspruch

Ein Beamter erhielt vom Landesbesoldungsamt im August 1995 die Mitteilung, daß die Anspruchsvoraussetzungen zum Orts-, Sozial- und Verheiratetenzuschlag geprüft werden und zu diesem Zweck von ihm ein Datenerhebungsbogen auszufüllen sei. In dem Formular sollte der Betroffene angeben, ob er in erster Ehe oder in zweiter/folgender Ehe verheiratet sei. In einem anschließenden Abschnitt wurden dann Angaben zum Ehegatten oder geschiedenen Ehegatten gefordert, wenn Kinder aus der Ehe hervorgegangen sind. Dazu wurde ein weiterer Hinweis gegeben: "Wenn in 2. Ehe pp. verheiratet, bitte gesonderte Angaben über den/die geschiedenen Ehegatten - Vordruck für gesonderte Angaben wird auf Antrag übersandt."

Der Beamte hat sich bei mir darüber beschwert, daß die Formulierung im Datenerhebungsbogen nicht eindeutig sei und er daraus ableitet, Angaben über seine geschiedene Ehefrau machen zu müssen, obwohl er keine Unterhaltsverpflichtungen hat.

Ich habe der Finanzministerin empfohlen, nur noch den Status "verheiratet" zu erfragen und auf die Zusätze in 1./2. oder folgender Ehe zu verzichten. Angaben über den geschiedenen Ehegatten sollten nur gefordert werden, wenn Unterhaltsverpflichtungen bestehen und deshalb eine höhere Stufe des Ortszuschlages beantragt wird. Die Finanzministerin hat mir im Oktober 1995 mitgeteilt, diese Empfehlungen bei der nächsten Drucklegung des Erhebungsbogens zu berücksichtigen.

2.13.5. Wird der Flughafendetektiv nun Oberbürgermeister?

In einer kreisfreien Stadt unseres Landes wurde die Stelle des Oberbürgermeisters bundesweit ausgeschrieben. Nachdem die ersten Bewerbungen eingegangen waren, erhielt ich Kenntnis von einem Presseartikel mit der Überschrift "Vom Flughafen-Detektiv bis zum Mercedes-Benz-Vertreter". In dem Beitrag wurden 20 von den insgesamt 29 Bewerbern mit Namen, Vornamen, Beruf, Wohn- und Arbeitsort der Öffentlichkeit vorgestellt.

Daraufhin habe ich den amtierenden Oberbürgermeister um Stellungnahme gebeten. In der Antwort legte er dar, daß die Stadt nach dem Landespressegesetz zur Auskunft verpflichtet gewesen sei (§ 4 LPrG M-V). Dem würden weder das Landesdatenschutzgesetz noch andere Gesetze entgegenstehen. Da das Interesse an der Person des Stelleninhabers im Vorfeld am größten sei, habe man sich entschieden, diese Daten bereits vor der öffentlichen Sitzung der Bürgerschaft bekanntzugeben. Außerdem hätten sich die Genannten um ein öffentliches Amt beworben und hätten insofern wissen müssen, daß sie als Wahlbeamte und Politiker im Lichte der Öffentlichkeit stehen.

Jeder Bewerber hat jedoch ein Recht auf vertrauliche Behandlung seiner Bewerbung. Wäre dies nicht der Fall, könnten ihm Nachteile für sein gegenwärtiges Beschäftigungsverhältnis entstehen. Auch war die Veröffentlichung der Daten der Bewerber zu diesem Zeitpunkt nicht erforderlich, denn es war von vornherein klar, daß nicht alle in die engere Wahl kommen würden. Ein Ausschuß hat die Kandidaten nominiert, die dann der Stadtverordnetenversammlung vorgestellt wurden. Vor der Wahl des Oberbürgermeisters in öffentlicher Sitzung hätten dann lediglich die Daten der nominierten Kandidaten bekanntgegeben werden dürfen. Damit wäre das informationelle Selbstbestimmungsrecht der Kandidaten gewahrt worden, denn bis zur Nominierung konnten sie selbst noch entscheiden, ob sie sich der öffentlichen Wahl stellen oder ihre Kandidatur zurückziehen.

Da durch die Veröffentlichungen in der Presse die schutzwürdigen Interessen der Bewerber beeinträchtigt wurden, habe ich dem amtierenden Oberbürgermeister eine förmliche Beanstandung ausgesprochen und den Innenminister unseres Landes informiert.

Schließlich ist der Flughafendetektiv doch nicht Oberbürgermeister geworden. Der amtierende Oberbürgermeister wurde von der Stadtverordnetenversammlung wiedergewählt. Er teilte mir mit, daß er dem Datenschutz künftig mehr Beachtung schenken wird.

2.13.6. Lehre, Forschung, Ehre und keine Einsicht

Das Landeshochschulgesetz (LHG M-V) sieht vor, daß bis zum 31. Dezember 1996 für jeden Bewerber um eine Stelle des wissenschaftlichen und künstlerischen Personals an Hochschulen ein Verfahren zur Prüfung der persönlichen Eignung stattfindet (§ 130 Abs. 1 LHG M-V). Dies ist eine befristete Fortsetzung des Ehrenverfahrens nach § 2 des Hochschulerneuerungsgesetzes vom 19. Februar 1991. Darüber hinaus ist normiert, solche Verfahren auch für Bewerber an staatlichen Forschungseinrichtungen außerhalb von Hochschulen durchzuführen (§ 130 Abs. 3 LHG M-V).

Durch eine Information der Gewerkschaft Erziehung und Wissenschaft erhielt ich im Juli 1994 Kenntnis von dem für das Ehrenverfahren erarbeiteten neunseitigen Datenerhebungsbogen.

Bei dessen Prüfung stellte ich fest, daß der "Fragebogen für das Verfahren zur Prüfung der persönlichen Eignung durch die Zentrale Personalkommission gemäß § 130 des Landeshochschulgesetzes Mecklenburg-Vorpommern" in zweifacher Hinsicht nicht dem Gleichbehandlungsgebot entsprach. Ein ganzer Abschnitt des Bogens ist nur von Bewerbern aus der ehemaligen DDR auszufüllen. Darüber hinaus ist die Datenerhebung viel umfangreicher als die für den öffentlichen Dienst zur Anerkennung von Beschäftigungsdienstzeiten. Eine Nachfrage bei meinen Kollegen in den anderen neuen Ländern ergab, daß derartige Datenerhebungen dort nicht stattfinden. In meiner Stellungnahme habe ich der Kultusministerin empfohlen, den Fragenkatalog zu reduzieren und dazu konkrete Hinweise gegeben.

Daraufhin wurde mir im Oktober 1994 mitgeteilt, daß an die Einstellung des wissenschaftlichen und künstlerischen Personals an Hochschulen strengere Anforderungen zu stellen seien als sonst im öffentlichen Dienst üblich. Der Fragebogen sei von allen Bewerbern auszufüllen, unabhängig davon, ob sie aus Ost- oder Westdeutschland kommen.

Es trifft zwar zu, daß alle Bewerber den Fragebogen auszufüllen haben, aber allein 19 Einzelfragen muß ein Bewerber aus Westdeutschland nicht beantworten, denn der betreffende Abschnitt beginnt mit der Frage: "Haben Sie nach Vollendung Ihres 18. Lebensjahres und vor dem 3. Oktober 1990 Ihren Wohnsitz ständig oder zeitweise in der Deutschen Demokratischen Republik gehabt? - ja/nein - Wenn ja, beantworten Sie bitte nachfolgende Fragen!"

Im Februar 1995 habe ich der Kultusministerin empfohlen, den vom Innenminister herausgegebenen einheitlichen Fragebogen für den öffentlichen Dienst zu verwenden. Außerdem kann eine schriftliche Erklärung, ob der Bewerber für das Ministerium für Staatssicherheit/Amt für Nationale Sicherheit tätig war und ob er mit einer Überprüfung seiner Angaben durch den Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR einverstanden ist, eingeholt werden.

Die Kultusministerin hat mir im Mai 1995 mitgeteilt, daß sie an dem Fragebogen zur Prüfung der persönlichen Eignung festhält, und dies unter anderem damit begründet, daß dafür auch die Zustimmung der Personalräte vorliegt. Meine datenschutzrechtlichen Bedenken sind damit nicht ausgeräumt; aber mit Einsicht der Ministerin bis zum Ablauf des Termins ist wohl auch nicht mehr zu rechnen.

2.13.7. Entfernung von Unterlagen aus der Personalakte

Ein Beschäftigter einer Stadtverwaltung fragte an, ob es zulässig sei, daß in seiner Personalakte eine farbig markierte Leistungseinschätzung aus "DDR-Zeiten" sowie Unterlagen über einen privaten Sportunfall aufbewahrt werden.

Um die Frage beantworten zu können, kontrollierte ich die Personalakte im Personalamt. Der Personalamtsleiter erklärte, er habe die Leistungseinschätzung so von der ehemaligen Personalstelle (Kaderabteilung) übernommen und den Beschäftigten auch mehrfach darauf aufmerksam gemacht, daß er Unterlagen aus der Personalakte entfernen lassen kann, wenn sie sich als unbegründet oder falsch erwiesen haben (§ 104 LBG M-V). Einen dafür erforderlichen Nachweis habe der Beschäftigte jedoch nicht erbracht. Die vom Petenten erwähnte Sportunfallmeldung befand sich nicht in der Personalakte.

Ich habe den Petenten über das Ergebnis informiert und ihn auf sein Recht gemäß § 104 LBG M-V hingewiesen.

Die Kontrolle habe ich zum Anlaß genommen, um auch den verwendeten Personalfragebogen zu prüfen. Das doppelseitige Formular wird von den Beschäftigten ausgefüllt und in allen Personalakten als erstes Blatt abgelegt. Das Formular stammte von der ehemaligen Verwaltung und es war immer noch die Erhebung der PKZ vorgesehen. Daß diese Abfrage nicht mehr zulässig ist, habe ich bereits erläutert (siehe auch Punkt 2.2.7 dieses Berichtes und Punkt 2.3.4 Erster Tätigkeitsbericht, Seite 26 f.).

Die fortgesetzte Erhebung der PKZ habe ich gegenüber dem Oberbürgermeister beanstandet und ihn aufgefordert, die alten Personalfragebogen zu vernichten sowie die bereits ausgefüllten gegen neue auszutauschen. Die betroffenen Beschäftigten sind über die notwendigen Maßnahmen und den Grund des Austausches zu informieren. Außerdem sollten die Personalakten auf Vereinbarkeit mit dem geltenden Personalaktenrecht geprüft werden.

Der Oberbürgermeister hat zugesichert, meine Empfehlungen zu realisieren.

2.13.8. Fürsorge oder Mißtrauen

Ein Angestellter eines städtischen Klinikums fragte an, ob sein Arbeitgeber berechtigt sei, sich beim behandelnden Arzt nach der Rechtmäßigkeit der Krankmeldung zu erkundigen.

Auf meine Anfrage hin teilte mir der ärztliche Direktor des Klinikums mit, er habe vermutet, daß der Krankenschein des Angestellten gefälscht sei. Die Unterschriften auf dem Kranken- und dem Verlängerungsschein seien unleserlich gewesen. Da der Betroffene selbst Arzt sei, hätte auch die Möglichkeit der Fälschung bestanden.

Allein dieser Verdacht rechtfertigt jedoch nicht die Nachfrage des Direktors bei dem behandelnden Arzt. Da der behandelnde Arzt der Schweigepflicht unterliegt, darf er eine derartige Auskunft nicht geben (§ 203 StGB).

Bestehen Zweifel an der Rechtmäßigkeit einer Krankmeldung, so hat der Arbeitgeber nur die Möglichkeit, eine gutachterliche Stellungnahme des Medizinischen Dienstes der Krankenversicherung einzuholen (§ 275 Abs. 1 Nr. 3 b Fünftes Buch Sozialgesetzbuch).

Der ärztliche Direktor hat seine Mitarbeiter über diese Möglichkeit informiert und zugesagt, meine Hinweise künftig zu beachten. Der Petent wurde über dieses Ergebnis informiert.

2.13.9. Weitergabe eines ärztlichen Attestes an die Hauptfürsorgestelle

Eine schwerbeschädigte Arbeitnehmerin hat sich an mich gewandt, weil die Amtsgemeinde, bei der sie beschäftigt war, ohne ihre Einwilligung ein ärztliches Attest an die Hauptfürsorgestelle gegeben hat. Ihr Hausarzt hatte das Attest für ihren Rentenantrag angefertigt. Sie hatte es ohne Aufforderung in der Personalstelle abgegeben, da ihr damit bescheinigt wurde, welche körperlichen Arbeiten sie nicht mehr ausführen kann. Im Rahmen eines Kündigungsverfahrens übermittelte der Arbeitgeber das Attest an die Hauptfürsorgestelle. Die Petentin bat mich um Stellungnahme zu dieser Datenübermittlung und erhoffte sich eine Unterstützung in dem bevorstehenden Kündigungschutzprozeß.

Nach dem Schwerbehindertengesetz hat die Hauptfürsorgestelle die Interessen der schwerbehinderten Arbeitnehmer zu vertreten und ihnen unter anderem Kündigungsschutz zu gewähren. Dazu muß der Arbeitgeber der Hauptfürsorgestelle alle erforderlichen Auskünfte erteilen (§ 13 Abs. 3 SchwbG). Diese Auskünfte beziehen sich auf die Arbeitsplatzgestaltung und andere betriebliche Verhältnisse, nicht aber auf ein ärztliches Attest.

Eine Anfrage beim Amtsvorsteher ergab, daß er keinen Verstoß gegen datenschutzrechtliche Bestimmungen bei dieser Datenübermittlung erkannt hatte. Seiner Ansicht nach war sie aufgrund der Amtshilfe zulässig gewesen. Die Verpflichtung zur Amtshilfe kann jedoch nicht das Recht auf informationelle Selbstbestimmung außer Kraft setzen. Daten dürfen nur auf der Basis einer Rechtsvorschrift bzw. mit Einwilligung oder Kenntnis des Betroffenen übermittelt werden.

Von einer Beanstandung gegenüber dem Amtsvorsteher habe ich abgesehen. Zur Wahrung ihrer Interessen wäre die Arbeitnehmerin von der Hauptfürsorgestelle möglicherweise ohnehin aufgefordert worden, eine entsprechende Bescheinigung vorzulegen. Gleichwohl war die Datenübermittlung vom Arbeitgeber an die Hauptfürsorgestelle unzulässig. Dies habe ich dem Amtsvorsteher mitgeteilt und ihn aufgefordert, künftig die datenschutzrechtlichen Bestimmungen beim Umgang mit personenbezogenen Daten einzuhalten.

Der Petentin habe ich meine Auffassung zur Übermittlung des Attestes an die Hauptfürsorgestelle mitgeteilt und darauf aufmerksam gemacht, daß es nicht zu meinem Tätigkeitsbereich gehört, die Zulässigkeit oder Unzulässigkeit einer Kündigung zu beurteilen.

2.13.10. Übermittlung von Personaldaten an die Staatsanwaltschaft - Einsicht besser als Beschlagnahme

Ein Dienstherr hatte gegen einige seiner Beschäftigten Anzeige bei der Staatsanwaltschaft wegen des Tatvorwurfs der Bestechlichkeit erstattet. Im Rahmen des Ermittlungsverfahrens trat die Staatsanwaltschaft an den Dienstherren heran, um Auskünfte aus der Personalakte über Bankverbindungen der Bediensteten sowie über das Aufgabenfeld der Betroffenen zu erhalten. Die Staatsanwaltschaft begründete ihr Auskunftsersuchen damit, daß sie im Falle der Beschlagnahme Zugriff auf die Unterlagen hat. Insofern sei auch eine Datenübermittlung zulässig.

Daraufhin wandte sich das Rechtsamt der Stadt mit der Frage an mich, ob diese Datenübermittlung zulässig sei.

Der Umgang mit Personaldaten bei Dienst- und Arbeitsverhältnissen ist für Beamte im Landesbeamtengesetz von Mecklenburg-Vorpommern (§§ 100 ff. LBG M-V), für Arbeiter und Angestellte im Landesdatenschutzgesetz von Mecklenburg-Vorpommern (§ 31 DSG MV) und in den tariflichen Bestimmungen geregelt.

Für die Ermittlung der Staatsanwaltschaft bei Behörden ist § 161 StPO maßgeblich. Diese Vorschrift normiert, daß die Staatsanwaltschaft von allen öffentlichen Behörden Auskunft verlangen kann und Ermittlungen jeder Art entweder selbst vornehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen lassen kann. Demnach ist die Behörde im Ermittlungsverfahren gegenüber der Staatsanwaltschaft zur Auskunft verpflichtet.

Außerdem ist hier der Grundsatz der Verhältnismäßigkeit zu berücksichtigen. Eine Auskunft aus der Personalakte ist immer einer Einsichtnahme bzw. einer Überlassung der Personalakte vorzuziehen.

Der Behörde habe ich empfohlen, der Staatsanwaltschaft die geforderten Daten zu übermitteln. So gelangen der Staatsanwaltschaft nur die Daten zur Kenntnis, die im Rahmen des Ermittlungsverfahrens erforderlich sind.

2.13.11. Muß der Chef über jeden Unfall informiert werden?

Eine Landesbeamtin hat sich an mich gewandt und geschildert, daß ihr Sohn einen Verkehrsunfall hatte. Wegen des Beihilfeanspruchs hatte sie den Unfall der Beihilfestelle mitgeteilt. Daraufhin erhielt sie von dort eine Unfallanzeige, die auch von ihrem Dienststellenleiter unterschrieben werden sollte. Sie beschwerte sich nun insbesondere darüber, daß ihr Dienstherr über den Unfall ihres Sohnes und die damit im Zusammenhang stehenden personenbezogenen Daten Kenntnis erhalten habe, obwohl dies nach ihrer Auffassung nicht erforderlich gewesen sei, und daß er die Unfallmeldung unterschreiben sollte, obwohl er keine Angaben zum Unfallhergang machen konnte.

Die Finanzministerin hat das Verfahren im Erlaß zur "Geltendmachung von auf das Land Mecklenburg-Vorpommern übergegangenen Schadensersatzansprüchen im Falle der Verletzung oder Tötung von Beamten, Versorgungsberechtigten, deren Angehörigen sowie Angestellten und Arbeitern" geregelt (veröffentlicht im Amtsblatt M-V 1993, S. 1565). Von der Anzeigepflicht sind ausschließlich solche Schadensfälle mit Beteiligung von Dritten betroffen, bei denen sich daraus Ansprüche des Landes ergeben oder ergeben könnten. Die Anzeige des Unfalls hat auf einem Vordruck zu erfolgen, der dem Erlaß beigefügt ist. Sie ist vom Dienststellenleiter bzw. seinem Beauftragten zu unterschreiben.

Die Finanzministerin teilte mir mit, daß die Unterschrift des Dienststellenleiters bei Unfällen beihilfeberechtigter Angehöriger in der Tat entbehrlich sei und daß ein neues Formular konzipiert wurde. Die ausschließliche Prüfung und Bearbeitung dieser Regreßfälle wurde aufgrund meines Hinweises nunmehr dem Landesbesoldungsamt übertragen.

Die Petentin habe ich über die datenschutzgerechte Änderung des Verfahrens informiert.

2.13.12. Personaldaten im Finanzministerium

Auf einer Beratung mit den internen Datenschutzbeauftragten wurde mir mitgeteilt, daß vom Finanzministerium auch Personaldaten von Beschäftigten aus anderen Ressorts erhoben und dort gespeichert werden. Die Datenerhebung erfolgt ohne Beteiligung der Betroffenen bei den Personalstellen. Sie dient der Entscheidung über die Einstellung von Beamten in den Landesdienst, wenn sie ein festgesetztes Alter überschritten haben (§ 48 Landeshaushaltsordnung), oder zur Entscheidung über die Gewährung einer Gehaltszulage für Angestellte in Höhe des Differenzbetrages zwischen Bundesangestelltentarifvertrag-Ost und Bundesangestelltentarifvertrag (§ 9 Haushaltsgesetz 1994). Die Finanzministerin hat die Datenerhebung und Speicherung damit begründet, daß in beiden Fällen ihre Einwilligung aus haushaltsrechtlichen Gründen erforderlich ist. Darüber hinaus muß sie die Personalausgaben kontrollieren und die Versorgungslasten abschätzen, da nur eine begrenzte Anzahl von Beamten übernommen bzw. nur maximal 240 Angestellte die Zulage erhalten können.

Zur Durchführung des Verfahrens werden die Beschäftigungsdienststellen aufgefordert, folgende Daten jedes Einzelfalles auf einem Formular zu übermitteln: Name, Vorname, Geburtsdatum sowie Daten über Ausbildung, Qualifizierung, vorherige Beschäftigungsstellen und -zeiten. Außerdem sollen die Personaldienststellen eine Einschätzung des Beihilferisikos abgeben.

Mein Vorschlag, auf die Speicherung von Personaldaten zu verzichten und statt dessen Stellenplandaten zu verwenden, wurde abgelehnt, da bei neuen Anträgen alle anderen Vorgänge beigezogen und ausgewertet werden müssen und dafür Stellenplandaten nicht ausreichend seien. Außerdem wäre mit den teilanonymisierten Daten keine Kontrolle der gesetzlich vorgegebenen Anzahl von Entscheidungsfällen möglich.

Kurz vor Redaktionsschluß für diesen Tätigkeitsbericht hat mir die Finanzministerin mitgeteilt, daß sie den Umfang der gespeicherten Daten auf das für die Auswertungen notwendige Maß (Name, Vorname, Geburtsdatum, Besoldungs- oder Vergütungsgruppe) beschränkt. Die Datenerhebung zur Bewilligung der Gehaltszulage für Angestellte ist nicht mehr erforderlich, da das Haushaltsgesetz 1995 keine entsprechende Regelung enthält.

Meine Empfehlung, die Betroffenen über den Zweck und den Umfang der gespeicherten Personaldaten zu informieren, wird berücksichtigt. Die Speicher- bzw. Löschfristen werden noch mit dem Ministerium geklärt.

2.13.13. Sozialauswahl bei betriebsbedingten Kündigungen

Ein Beschäftigter einer Stadtverwaltung hat mich über folgende Verfahrensweise des Personalamtes informiert:

Zur Vorbereitung betriebsbedingter Kündigungen hatte das Amt allen Arbeitern und Angestellten in einem Rundschreiben mitgeteilt, daß die Stadtverwaltung aufgrund finanzieller Schwierigkeiten zu Strukturveränderungen und zum Stellenabbau gezwungen sei. Sie wurden deshalb gebeten, ein beiliegendes Formular ausgefüllt an das Personalamt zu senden. Neben Angaben zum Familienstand sollten unter anderem auch Angaben zu bestehenden Unterhaltsverpflich-

tungen gemacht werden, um später eine Auswahl nach sozialen Gesichtspunkten vornehmen zu können.

Hierbei handelt es sich um eine Erhebung personenbezogener Daten auf Vorrat, denn es wurden auch von solchen Arbeitern und Angestellten der Stadtverwaltung Daten erhoben, die nicht entlassen werden sollten. Somit wurde in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung eingegriffen.

Nach bisheriger Rechtsprechung des Bundesarbeitsgerichtes erstreckt sich die soziale Auswahl innerhalb einer Verwaltung oder eines Betriebes auf Arbeitnehmer, die miteinander verglichen werden können. Die Auswahl richtet sich in erster Linie nach arbeitsplatzbezogenen Merkmalen und nicht nach der bislang ausgeübten Tätigkeit. Es muß zunächst die künftige Aufgabenverteilung und Struktur bekannt sein, bevor die personelle Auswahl erfolgt.

In dem Rundschreiben der Stadtverwaltung waren keine Hinweise über die Art und den Umfang der Verarbeitung und Nutzung dieser Daten enthalten. Das Personalamt hätte den Betroffenen mitteilen müssen, daß diese Daten beispielsweise in einem Kündigungsschutzverfahren verwendet werden. Der Hinweis, wo und in welcher Form (zum Beispiel in geschlossenem Umschlag) der Erhebungsbogen abzugeben ist, fehlte ebenfalls. Bedenken hatte ich außerdem, ob tatsächlich alle personenbezogenen Daten für die Sozialauswahl erforderlich sind. Das betraf insbesondere die Höhe der monatlichen Unterhaltsverpflichtungen.

Ich habe dem Oberbürgermeister diese Bedenken mitgeteilt und ihn gebeten, die Erhebungsbögen zurückzuziehen und die bereits eingegangenen zu vernichten. Die Sozialauswahl darf erst stattfinden, wenn bekannt ist, welche Arbeitsplätze aus betriebsbedingten Gründen wegfallen müssen.

Der Oberbürgermeister war der Ansicht, daß den Mitarbeitern Sinn und Zweck der Datenerhebung in dem Rundschreiben ausführlich erläutert wurde. Außerdem seien sie gebeten worden, den Fragebogen an das Personalamt zu schicken. Es entspräche den Gepflogenheiten, daß diese Vorgänge dem Personalamt in verschlossener Form übersendet werden. Ein Hinweis wäre somit nicht mehr notwendig gewesen.

Gegenüber dem Oberbürgermeister habe ich deutlich gemacht, daß sich meine Bedenken insbesondere gegen die nicht erforderliche und damit unzulässige Datenerhebung bei allen Angestellten und Arbeitern richteten. Ich habe darauf hingewiesen, daß ich das Verfahren beanstanden werde, wenn erneut alle Arbeiter und Angestellten in die Sozialauswahl einbezogen werden (§ 28 DSG MV).

Der Oberbürgermeister teilte mir daraufhin mit, daß das Rundschreiben und der Fragebogen bereits zurückgenommen wurden, da noch kein Bedarf für die Daten bestand. Zur Vorbereitung einer notwendigen Sozialauswahl werde er jedoch weiter an der schriftlichen Befragung festhalten. Es werden dann allerdings nur diejenigen Beschäftigten einbezogen, für die Vergleichsgruppen gebildet werden können. Zum Zeitpunkt der ersten Abfrage konnten die in Frage kommenden Planstellen noch nicht konkret benannt werden, und daher wurden alle Beschäftigten mit Ausnahme der Beamten angesprochen.

Den Petenten habe ich über das Ergebnis informiert.

2.14. Bildung, Kultur, Wissenschaft und Forschung

2.14.1. Noch immer kein Archivgesetz (Teil II)

Häufig erhalte ich Anfragen zum Umgang mit Unterlagen, die die Behörden zur Erfüllung ihrer Aufgaben nicht mehr benötigen. Das bereits mehrfach angemahnte Archivgesetz (siehe auch Erster Tätigkeitsbericht, Punkt 2.14.4, Seite 89 ff.), das diesen Bereich regeln würde, ist noch immer nicht in Kraft. Die Rechtsunsicherheit bei der Prüfung, wer unter welchen Umständen mit Archivdaten umgehen darf, und der damit verbundene hohe zeitliche Aufwand zur Entscheidungsfindung bestehen daher fort.

Im Juni 1994 nahm ich an einer Beratung zum Landesarchivgesetz im Kultusministerium teil. Die Mitwirkenden verständigten sich auf einen gemeinsamen Text als weitere Arbeitsgrundlage und vereinbarten, diesen zu redigieren und dem Alternativentwurf des hiesigen Landesverbandes im Verein deutscher Archivare gegenüberzustellen. Die Ministerin bat mich im August 1994, zu beiden Entwürfen Stellung zu nehmen. Ich habe empfohlen, vor allem folgende Punkte zu berücksichtigen:

- Die nach § 203 Absatz 1 StGB geschützten Beratungsunterlagen bestimmter Stellen (z. B. freiwillige Familienberatung, Sexualberatung oder AIDS-Beratung) dürfen dem zuständigen Archiv nur in anonymisierter Form angeboten und übergeben werden.

- Die Übergabe maschinell lesbarer Datenträger bedarf einer eigenen Regelung.

- Die Verknüpfung personenbezogener Daten aus verschiedenen Unterlagen oder Datenträgern darf nur zulässig sein, wenn schutzwürdige Belange Betroffener oder Dritter nicht beeinträchtigt werden.

- Da das Archivgesetz die Rechtsgrundlage für die Aufgaben und die Arbeit der staatlichen Archive bildet, müssen seine Vorschriften - und nicht lediglich die Grundsätze - über die Archivierung und Benutzung der achivwürdigen Unterlagen auch für die übrigen öffentlichen Archive, wie kommunale Archive, gelten; ansonsten bestünde die Gefahr der Aufweichung des Schutzes personenbezogener Daten.

Im November 1994 gab es zwei weitere Treffen, bei denen die Änderungsvorschläge der Teilnehmer diskutiert wurden. "Im Zuge der Ressortabstimmung" erhielt ich im Juni 1995 einen überarbeiteten Entwurf des Kultusministeriums zur erneuten Stellungnahme. In diesem Entwurf sind alle wesentlichen von mir vorgebrachten Punkte berücksichtigt.

Ich hoffe, daß die Kultusministerin den Entwurf nun bald in den Landtag einbringt und daß ein Landesarchivgesetz verabschiedet werden kann.

2.14.2. Konfession im Studienbuch?

Häufig fragen Eltern und Lehrer bei mir nach, welche Daten in Schulen erhoben werden dürfen.

Eine Mutter wollte beispielsweise wissen, ob es zulässig sei, daß in den Studienbüchern der gymnasialen Oberstufe regelmäßig nach der Konfession gefragt wird. Die Seite des Studienbuches sei darüber hinaus so gestaltet, daß das Mißverständnis aufkommen könnte, es handele sich um die Konfession der Eltern, denn der Eintrag steht direkt und ohne optische Trennung neben den Namen der Erziehungsberechtigten.

Das Studienbuch dient als Nachweis des Bildungsganges und ist bei der Abiturprüfung vorzulegen. Die darin aufzunehmenden Daten sind in der Abiturprüfungsverordnung festgelegt.

Auf meine Anfrage hin konnte die Kultusministerin nicht begründen, daß die Angabe der Konfession im Studienbuch erforderlich ist. Sie hat allerdings darauf verwiesen, daß es auch in anderen Bundesländern erhoben würde. Ich habe empfohlen, die Abiturprüfungsverordnung zu überarbeiten und auf das Erheben und Verarbeiten dieses Datums zu verzichten. Die Kultusministerin hat zugesagt, bei der Novellierung der Verordnung die Empfehlung zu berücksichtigen.

Eine spezielle Rechtsvorschrift zum Umgang mit Daten in der Schule ist bisher noch nicht in Kraft. Um jedoch den großen Informationsbedarf zum Umgang mit Daten in der Schule zu befriedigen, habe ich 1994 ein Informationsblatt herausgegeben, das kostenlos bei mir erhältlich ist.

2.14.3. Wo bleibt die Rechtsverordnung zum Umgang mit Studentendaten?

Im November 1994 habe ich in einer Hochschule den Umgang mit Studentendaten kontrolliert. Das Dezernat für Studentische Angelegenheiten verarbeitet personenbezogene Daten der immatrikulierten Studenten sowie der Teilnehmer an Studienkollegs und an Sprachkursen. Der Umgang mit den Daten ist für die Studien- und Prüfungsverwaltung sowie für die Statistik und die Hochschulplanung erforderlich. Zur Verarbeitung der Daten betreibt das Dezernat ein lokales Netz, das aus einem Server und elf Terminals besteht.

Die Daten werden bei der Immatrikulation und bei der Prüfungsanmeldung von den Betroffenen erhoben und um die Leistungsbewertung ergänzt. Das Dezernat übermittelt innerhalb der Universität diese Daten an die Fakultät, an der der Student eingeschrieben ist. Diese Übermittlung ist zur Gewährleistung des Studienablaufes erforderlich. Für statistische Zwecke übermittelt das Dezernat einmal pro Semester aggregierte Daten an das Statistische Landesamt.

Für den Umgang mit personenbezogenen Daten habe ich empfohlen, entsprechende Regelungen in die Immatrikulationsordnung aufzunehmen und die in § 17 DSG MV festgelegten technisch-organisatorischen Maßnahmen umzusetzen. Der Rektor will diesen Empfehlungen folgen.

§ 59 LHG M-V regelt, daß die im Zusammenhang mit der Immatrikulation zu erhebenden personenbezogenen Daten durch eine Satzung festzuschreiben sind. An der Hochschule war jedoch keine Satzung in Kraft, die entsprechende Aussagen enthielt. Allerdings ist geplant, die Immatrikulationsordnung zu überarbeiten und als Satzung zu erlassen.

Des weiteren ist in § 123 LHG M-V normiert, daß die Kultusministerin durch Rechtsverordnung den Umgang mit den erforderlichen personenbezogenen Daten der Studienbewerber, Studenten und Prüfungskandidaten für Verwaltungszwecke bestimmt. Auch diese Rechtsverordnung lag zum Zeitpunkt der Kontrolle nicht vor. Auf meine Anfrage hin teilte mir die Ministerin mit, daß ein Entwurf der Verordnung voraussichtlich ab Mitte Februar 1995 den Hochschulen, den Ressorts und mir zur Stellungnahme zugeleitet wird. Auf Nachfrage zum Arbeitsstand der Rechtsverordnung erhielt ich die Information, daß das LHG M-V novelliert und dabei auch die Norm zum Umgang mit personenbezogenen Daten geändert werden soll. Deshalb werde zunächst nicht weiter an der Rechtsverordnung gearbeitet.

Anfang Juli 1995 erhielt ich den Referentenentwurf eines Gesetzes zur Änderung des LHG M-V. Die Norm zum Umgang mit personenbezogenen Daten ist im Entwurf um den Evaluierungszweck ergänzt worden, um Aussagen zur Qualität von Lehre und Forschung gewinnen zu können. In meiner Stellungnahme habe ich empfohlen, folgende weitere Regeln zum Umgang mit personenbezogenen Daten für Evaluierungszwecke aufzunehmen:

- Beschränkung des zu evaluierenden Personenkreises auf wissenschaftliches und künstlerisches Personal der Hochschulen,
- Konkretisierung des Evaluationszwecks, der Erhebungsmerkmale und des Erhebungsverfahrens,
- möglichst frühzeitige Anonymisierung der erhobenen Daten über das wissenschaftliche und künstlerische Personal,
- Verbot der Nutzung der Daten für andere Zwecke, insbesondere keine Nutzung zu konkreten personellen Maßnahmen oder zu Eingriffen in die Lehr- und Forschungstätigkeit,
- Herstellen von Transparenz für die Betroffenen.

Bisher liegt mir keine Mitteilung der Kultusministerin vor, ob und inwieweit meine Empfehlungen berücksichtigt werden.

2.14.4. Soziologische Forschung

Anfragen von Bürgern und Berichte in den Medien zeigten, daß der Informationsbedarf zum Umgang mit personenbezogenen Daten für soziologische Forschungszwecke groß ist. Die folgenden Beispiele sollen einige Aspekte des Datenschutzes in diesem Bereich verdeutlichen.

Umfrage zur Sozialstruktur der Mieter

Eine regionale Tageszeitung hat mich aufgrund von Leseranfragen darüber informiert, daß ein Institut im Auftrag einer Wohnungsgesellschaft Mieterbefragungen zur Wohnbefindlichkeit und zur Sozialstruktur durchführt. Die Wohnungsgesellschaft wollte ermitteln, welche Verbesserungen die Mieter wünschen und wieviel Geld sie dafür ausgeben würden. Zu diesem Zweck sollten sie auf freiwilliger Basis einen Fragebogen ausfüllen. Dieser wurde von den Hausmeistereien zugestellt und anschließend wieder eingesammelt. Falls ein Mieter zu dem angegebenen Abholtermin verhindert war, konnte er die Unterlagen auch bei Nachbarn oder in der Geschäftsstelle abgeben.

Der Datenerhebungsbogen enthielt eine laufende Nummer, aber keine direkt personenidentifizierenden Angaben wie Name, Vorname und Adresse. Neben Fragen zur Wohnung wurden auch solche zum Alter der im Haushalt lebenden Personen, zur Einkommensgruppe, zur Höhe des Wohngeldes, zum Beruf und zur Schulbildung gestellt. Eine Mieterin befürchtete, daß insbesondere aus der fünfstelligen laufenden Nummer des Fragebogens ein Rückschluß auf den Absender des Bogens möglich sei.

In einem Gespräch habe ich dem wissenschaftlichen Leiter des Projektes empfohlen, ein Datenschutz- und IT-Sicherheitskonzept zu erarbeiten und unter anderem zu gewährleisten, daß die laufende Nummer nicht zur Reidentifizierung verwendet werden kann. Laufende Numerierungen bei freiwilligen und anonymen Datenerhebungen sind generell bedenklich, weil hierdurch die Anonymität in Frage gestellt sein könnte bzw. rückgängig gemacht werden kann.

Die gleiche Forschungsgruppe hat mich im Frühjahr 1995 gebeten, zu einer weiteren geplanten anonymen Befragung zur Wohnbefindlichkeit von Mietern Stellung zu nehmen. Die Teilnahme an diesem Projekt sollte ebenfalls freiwillig sein.

Ich habe empfohlen, die Freiwilligkeit der Teilnahme im Anschreiben deutlich hervorzuheben und die ausgefüllten Fragebogen dem Vermieter nicht zugänglich zu machen, da er mit seinem Zusatzwissen aus einzelnen Details möglicherweise einen Personenbezug herstellen kann. Die Forschungsgruppe hat diese Hinweise berücksichtigt.

Berufliche Verläufe im Umbruch

Ein Bürger erhielt im Oktober 1994 ein Schreiben von einer Forschungsgruppe aus Bremen. Darin wurde er gebeten, sich an der Studie "Berufliche Verläufe im Umbruch" zu beteiligen. Die Studie hatte das Ziel, Berufswege von ehemaligen DDR-Bürgern vor und nach der Wende zu erforschen. Zu diesem Zweck war dem Schreiben ein umfangreicher Fragebogen beigefügt. Der Bürger wollte nun von mir wissen, ob der Landesbeauftragte für den Datenschutz wirklich - wie im Anschreiben versichert - über das Forschungsprojekt informiert ist und ob die Fragen im einzelnen datenschutzrechtlich korrekt seien.

In dem Anschreiben wird erläutert, daß für die Untersuchung eine Stichprobe aus den Adressen der Absolventen von Berufs- und Hochschulen der Regionen Rostock und Leipzig gezogen wurde, zu der auch der Betroffene gehöre. Die Teilnahme an der Befragung sei natürlich freiwillig, es wird jedoch gebeten, den Fragebogen vollständig ausgefüllt bis zum 9. Oktober 1994 zurückzusenden. Das Schreiben war außer vom wissenschaftlichen Leiter der Forschungsgruppe vom Sozialminister unseres Landes, vom Staatsminister für Wirtschaft und Arbeit des Landes Sachsen und vom Präsidenten der Bundesanstalt für Arbeit unterschrieben. Für die Betroffenen mußte deshalb der Eindruck entstehen, daß die Forschungsergebnisse von hohem öffentlichen Interesse sind und daß die Aussagen den Tatsachen entsprechen. Ersteres scheint mir unstrittig. Informationen über das Projekt lagen mir bis zur Bürgeranfrage allerdings nicht vor.

Meine Anfrage bei der Kultusministerin ergab, daß auch dort das Forschungsprojekt unbekannt war, aber die Universität Rostock bereits um Auskunft zur Adressenübermittlung gebeten wurde. Der Kanzler der Universität hat daraufhin mitgeteilt, daß er sein prinzipielles Einverständnis zur Datenübermittlung im März 1992 gegeben hatte. Eine Genehmigung der Kultusministerin zur Datenübermittlung sei zu diesem Zeitpunkt nicht erforderlich gewesen, da das Landesdatenschutzgesetz noch nicht in Kraft war.

Vom Leiter der Forschungsgruppe wurde mir mitgeteilt, daß der Landesbeauftragte für den Datenschutz der Freien Hansestadt Bremen am 18. Oktober 1994 über das Projekt informiert worden war, da sich die datenverarbeitende Stelle in Bremen befinde. Aus den in der Anlage beigefügten Kopien war jedoch ersichtlich, daß Anfragen zur Adressenübermittlung schon 1992 und 1993 an die Universität Rostock und das Kultusministerium Mecklenburg-Vorpommern gestellt worden waren. Es wurde also weder die Adressenübermittlung noch die Datenerhebung von einem Landesbeauftragten für den Datenschutz begleitet, aber gerade dieser Eindruck war durch das Anschreiben bei dem Petenten erweckt worden.

Zum Verfahren der Auswahl der Studienteilnehmer hatte der Kanzler der Universität Rostock ursprünglich eine aus datenschutzrechtlicher Sicht günstige Variante - das sogenannte Adreßmittlungsverfahren - vorgeschlagen.

Dieses Verfahren hätte den Vorteil gehabt, daß der Forschungsbereich nicht die Adressen aller Absolventen erhalten hätte und die Befragung tatsächlich anonym gewesen wäre. Leider hat die Universität, entgegen ihrer Empfehlung, schließlich doch eine Diskette mit den Adressen aller Absolventen an den Forschungsbereich übersandt. Bei dem Adreßmittlungsverfahren wäre ihrer Auffassung nach der Verwaltungsaufwand zu hoch gewesen. Ich habe auf das nunmehr geltende Recht für Datenübermittlungen im Landesdatenschutzgesetz hingewiesen.

Zusammenfassend ist festzustellen, daß die Forschung über berufliche Verläufe sicherlich im öffentlichen Interesse lag und wichtige arbeitsmarktpolitische Entscheidungen unterstützen kann. Aber bei rechtzeitiger Einbeziehung der Datenschutzbeauftragten wären zahlreiche Verbesserungen des Verfahrens im Interesse der betroffenen Absolventen möglich gewesen, die letztlich wohl auch eine höhere Beteiligungsquote zur Folge gehabt hätten.

Telefoninterviews zur Gewalt in der Stadt

Durch einen Presseartikel bin ich darauf aufmerksam geworden, daß eine Forschungsgruppe telefonische Bürgerbefragungen in ausgewählten Teilen einer größeren Stadt durchführen wollte. Ziel der Interviews sollte die Gewinnung von Aussagen zur persönlichen Lebenssituation in den Stadtteilen sein, um im Ergebnis die Gewaltbereitschaft vorbeugend verhindern zu können. Zu diesem Zweck seien Telefonnummern nach dem Zufallsprinzip ausgesucht worden. Die Interviewer würden die Namen derjenigen, die angerufen werden, nicht kennen.

Ich habe dem Forschungsteam mitgeteilt, daß ich die zugesicherte Anonymität bei dieser Befragung nicht gewährleistet sehe, da die Telefonnummer ohne Schwierigkeit einer bestimmten oder bestimmbaren Person zuzuordnen ist. Im Handel sind inzwischen CD-ROM (Compact Disc Read Only Memory) erhältlich, mit deren Hilfe man aus einer bekannten Telefonnummer in Deutschland den dazugehörigen Anschlußinhaber und dessen Adresse ermitteln kann. Außerdem melden sich bei einem Anruf ohnehin viele Bürger namentlich, so daß die Anonymität auch aus diesem Grunde fragwürdig ist. Darüber hinaus bergen Telefoninterviews die Gefahr in sich, daß andere die Gunst der Stunde nutzen und sich am Telefon gegenüber vertrauensseligen Bürgern als Mitarbeiter des Forschungsteams ausgeben und persönliche Lebensumstände der für sie interessanten Einwohner ausforschen.

Vor diesem Hintergrund habe ich mich an die Medien gewandt und den Bürgern geraten, unbekannten Anrufern prinzipiell keine telefonische Auskunft über persönliche Angelegenheiten zu geben.

2.14.5. Medizinische Forschung

Des öfteren erreichen mich Anfragen zur medizinischen Forschung. Die folgenden Beispiele zeigen, unter welche Bedingungen medizinische Forschung und Datenschutz sich recht gut miteinander vereinbaren lassen.

Abgleich mit Einwohnermeldedaten

Eine Klinik für Psychiatrie und Psychotherapie beabsichtigte, die Häufigkeit seelischer Erkrankungen in einem Landkreis zu untersuchen. Dazu wollte sie eine Liste ihrer Patienten an ein Einwohnermeldeamt übermitteln, um feststellen zu lassen, wieviele der Patienten inzwischen verzogen oder verstorben sind. Da die Wissenschaftler nur die Anzahl der verzogenen und die Anzahl der verstorbenen Patienten wissen wollten, sahen sie in dem Verfahren kein datenschutzrechtliches Problem und wollten dies von mir bestätigt haben.

Der entscheidende Punkt ist hier aber nicht die Bekanntgabe der jeweiligen Anzahl der verzogenen oder verstorbenen Patienten, sondern die Liste mit Patientendaten (lfd. Nr., Name, Vorname, Geburtsdatum), die vorab an das Einwohnermeldeamt übermittelt werden soll. Bereits der Umstand, daß eine bestimmte Person einen Arzt oder ein Krankenhaus aufgesucht hat, unterliegt grundsätzlich dem Geheimnisschutz gemäß § 203 StGB. Nach den Datenschutzbestimmungen des Landeskrankenhausgesetzes dürfen Patientendaten ohne Einwilligung des Patienten verarbeitet und genutzt werden, soweit seine schutzwürdigen Belange nicht beeinträchtigt werden oder die für das Krankenhaus zuständige oberste Aufsichtsbehörde festgestellt hat, daß das öffentliche Interesse an der Durchführung des Forschungsvorhabens diese Belange erheblich überwiegt. Da es sich bei der Datenübermittlung an das Einwohnermeldeamt um die Offenbarung eines Geheimnisses handeln würde, habe ich der Forschungsgruppe mitgeteilt, daß dafür die Genehmigung der obersten Aufsichtsbehörde vorliegen muß.

Ich habe empfohlen, im Falle der Erteilung einer Genehmigung das Anschreiben an das Einwohnermeldeamt so zu gestalten, daß aus ihm kein Bezug zu bestimmten Krankheiten, etwa psychiatrische Krankheiten, hergestellt werden kann. Wie im Landeskrankenhausgesetz gefordert, ist der Datenschutzbeauftragte des Krankenhauses an dem Verfahren zu beteiligen (§ 20 Abs. 2 Satz 3 LKHG M-V).

Die Antwort der Mitarbeiter der Klinik steht noch aus.

Forschungsprojekt "Regionale Basisstudie Vorpommern"

Mitte des Jahres 1995 erhielt ich Kenntnis von einem medizinischen Forschungsprojekt zur Untersuchung des Gesundheitszustandes der Bevölkerung der Region Vorpommern. Um die Vorbeugung und Behandlung insbesondere von Herz-Kreislauf-Erkrankungen, Diabetes und Tumoren zu verbessern, sollen nach einem Zufallsprinzip circa sechs Prozent der Bevölkerung dieser Region ausgewählt werden und auf freiwilliger Basis an einer Befragung mit anschließender medizinischer Untersuchung teilnehmen. Zur repräsentativen Auswahl der Teilnehmer hat die Forschungsgruppe von der zuständigen Aufsichtsbehörde die Genehmigung zur Übermittlung eines Einwohnermelderegisterauszuges beantragt. Die Einwohnermeldeämter sollten danach Name, Geburtsname, Vorname, Geburtstag und Wohnanschrift aller gemeldeten Einwohner, bei denen keine Auskunftssperre vorliegt, übermitteln. Daraus sollten circa 10 000 Einwohner ausgewählt und gebeten werden, an dem Projekt teilzunehmen.

Ich habe das Projekt mit der Forschungsgruppe beraten und empfohlen, anstelle der Übermittlung des vollständigen Melderegisterauszuges das Adreßmittlungsverfahren anzuwenden. Dieser Vorschlag wurde nicht angenommen, da der gesamte Aufwand bei den Einwohnermeldeämtern liegen würde und darüber hinaus die Befürchtung bestand, daß hierunter die Repräsentativität der Studie leiden könnte.

In Abstimmung mit dem Innenministerium wurde schließlich ein Verfahren empfohlen, womit nur die Daten der zufällig ausgewählten Einwohner übermittelt werden und nicht ein vollständiger Melderegisterauszug. Danach gibt die Forschungsgruppe den Einwohnermeldeämtern bestimmte Merkmale vor, damit hieraus statistische Klassen gebildet werden können, beispielsweise nach Geschlecht und Geburtsjahrgang. Das Einwohnermeldeamt sortiert die Namen innerhalb der Klassen in alphabetischer Reihenfolge und versieht jeden Datensatz mit einer fortlaufenden Nummer (zum Beispiel erhält Nr. 1 die männliche Person der Altersgruppe 40 bis 44 Jahre mit dem Namen "Aal"). Die Forschungsgruppe erhält zunächst nur die Anzahl der Einwohner je Klasse, um daraus nach statistischen Methoden Nummern zu ziehen. Die gezogenen Nummern werden an die Meldeämter übermittelt und dort den Einwohnern zugeordnet. Anschließend übergibt das Einwohnermeldeamt die Daten der ausgewählten Personen an die Forschungsgruppe. Die Wissenschaftler verfügen somit über Namen, Vornamen, Geburtstag und Wohnanschrift von sechs Prozent der Einwohner dieser Region und nicht - wie ursprünglich vorgesehen - von nahezu einhundert Prozent. Der Antrag zur Genehmigung der Datenübermittlung wurde von der Forschungsgruppe gemäß dieser Empfehlung geändert.

Nach der Befragung und Untersuchung erhalten die Teilnehmer, sofern sie es wünschen, über ihren Hausarzt ihre Befunde mit entsprechenden Empfehlungen. Danach werden die personenbezogenen Daten und die Gesundheitsdaten getrennt gespeichert. Die wissenschaftliche Auswertung erfolgt anonym.

Auch meine weiteren Empfehlungen zur umfassenden Aufklärung der Betroffenen und zur Datenerhebung über Ehe- bzw. Lebenspartner wurden berücksichtigt, so daß nunmehr die datenschutzrechtlichen Voraussetzungen geschaffen sind und das Projekt 1996 beginnen kann.

Untersuchung zur Häufigkeit von Asthma und Allergien bei Kindern und Jugendlichen in Vorpommern (Projekt ISAAC)

Zu Beginn des Jahres 1995 wurde ich durch eine Bürgerin auf eine wissenschaftliche Untersuchung zur Häufigkeit von Asthma und Allergien bei Kindern und Jugendlichen in Vorpommern (Projekt ISAAC) aufmerksam gemacht. Eine Forschungsgruppe hatte zusammen mit einem Informationsschreiben an Eltern und Schüler personenbezogene Datenerhebungsbogen mit verschiedenen Fragen zur Gesundheit und zur sozialen Situation an Schüler verteilen lassen. Einen Fragebogen sollten die Eltern ausfüllen und den Kindern in einem beigefügten Umschlag verschlossen mitgeben. Der andere Fragebogen war von den Kindern mit Unterstützung eines Wissenschaftlers in der Schule auszufüllen. Körperliche Untersuchungen waren nicht vorgesehen.

Das Kultusministerium hatte die Befragung an den Schulen mit den Maßgaben genehmigt, daß die Teilnahme freiwillig ist, daß auf diese Freiwilligkeit hingewiesen wird und daß die schriftliche Einwilligung der Sorgeberechtigten für die Befragung der Kinder vorliegt.

Die Information und der Fragebogen für die Eltern enthielten jedoch keinen ausdrücklichen Hinweis auf die Freiwilligkeit der Datenerhebung, sondern folgende Formulierung: "Wir würden uns freuen, wenn auch Sie dieses wichtige Forschungsprojekt unterstützen." In den Informationen fehlte der Hinweis, daß Name und Adresse für eventuelle Nachfragen im Einzelfall benötigt werden. Außerdem wären Eltern und Schüler über den Zeitpunkt des Löschens von solchen Daten, die Personen identifizierbar machen, zu informieren gewesen.

Da die Befragung schon abgeschlossen war, habe ich empfohlen, bei künftigen Forschungsprojekten mit freiwilliger Teilnahme dies eindeutig zum Ausdruck zu bringen, im Text hervorzuheben und die Betroffenen über die Verarbeitung und Nutzung der Daten umfassend aufzuklären.

Der Leiter der Forschungsgruppe hat zugesichert, daß er künftig so verfahren wird.

2.14.6. Routinekontrolle im Landesprüfungsamt für Heilberufe

Im Mai 1994 habe ich eine Routinekontrolle im Landesprüfungsamt für Heilberufe durchgeführt.

Das Amt ist zuständig für die Vorbereitung und Durchführung von Prüfungen für akademische und nichtakademische Heilberufe.

Darüber hinaus hat das Amt von den Kreis- und Bezirksärzten sowie aus den Archiven der ehemaligen DDR Unterlagen und Urkunden über medizinische und pharmazeutische Ausbildungsabschlüsse übernommen, um sie zu erfassen und elektronisch zu speichern. Diese Übernahme war notwendig, da sich jeder Mediziner oder Angehörige eines Heilberufes aus unserem Bundesland zur Beantragung einer Berufserlaubnis hierher wenden und die Ausstellung eines Duplikats seiner Ausbildungsurkunde verlangen kann. Die Urkunden werden über einen Scanner eingelesen, auf WORM-Platten (Write Once Read Many) gespeichert und danach wieder an die jeweiligen Archive zurückgegeben. Sie sind in einer Verwaltungsdatei nach Aktenplannummer sowie Name, Vorname und Geburtsdatum der Betroffenen gespeichert. Eine weitere Datei enthält Angaben über den Entzug von Berufserlaubnissen. Die Dateien werden zu festgelegten Zeiten gesichert und die Kopien in einem Sicherheitsschrank aufbewahrt.

Zur automatisierten Verarbeitung der Urkunden habe ich dem Landesprüfungsamt empfohlen, die persönlichen Paßwörter in festzulegenden Abständen zu wechseln, um den Zugriffsschutz zu verbessern. Dieser Hinweis wurde berücksichtigt.

Die zur Vorbereitung und Durchführung der Prüfungen in den Heilberufen erhobenen Daten werden bisher nicht automatisiert verarbeitet. Die Betroffenen müssen einen Meldebeleg ausfüllen, um an den einzelnen Prüfungsabschnitten teilnehmen zu können. Er wird im Amt aufbewahrt, und eine Mehrfertigung wird an das Institut für medizinische und pharmazeutische Prüfungsfragen (IMPP) in Mainz versandt. Ich habe empfohlen, in diesen Beleg einen Datenschutzhinweis aufzunehmen, um die Betroffenen über die Art und den Umfang der Verarbeitung und Nutzung der Daten sowie über den Empfänger der übermittelten Daten aufzuklären. Allerdings werden die Belege bundeseinheitlich gedruckt und verwendet. Deshalb wird das Landesprüfungsamt die Betroffenen über die Datennutzung und -übermittlung im Zusammenhang mit den Erläuterungen zur Prüfungsanmeldung informieren.

2.15. Was gibt es Neues über InVeKoS?

Bereits im Ersten Tätigkeitsbericht informierte ich über das Integrierte Verwaltungs- und Kontrollsystem (InVeKoS) für flächenbezogene Beihilfen in der Landwirtschaft (siehe Punkt 2.15.1, Seite 92).

Im März 1994 habe ich den Umgang mit personenbezogenen Daten in einem Amt für Landwirtschaft kontrolliert.

Jeder landwirtschaftliche Betrieb innerhalb des Zuständigkeitsbereiches kann dort einen Antrag auf Agrarförderung stellen. Dazu werden Daten wie Name des Unternehmens, Anschrift des Betriebssitzes, Bankverbindung, Name und Anschrift des verantwortlichen Betriebsleiters sowie weitere Daten zum Betrieb, zu den angebauten Kulturen und Flächengrößen mit Einwilligung der Betroffenen erhoben. Es wird darauf hingewiesen, daß die Daten maschinell verarbeitet und auch zu Kontrollzwecken genutzt werden. Nach der Prüfung der Unterlagen erhalten die Antragsteller Bewilligungsbescheide. Die Zahlungsdaten werden auf Disketten gespeichert und über das Landwirtschaftsministerium an die Bundeskasse nach Frankfurt/Main übermittelt. Von dort aus werden die bewilligten Beträge auf die jeweiligen Konten überwiesen.

Dem Amt für Landwirtschaft habe ich unter anderem empfohlen, die genutzten Disketten in einem Verzeichnis zu erfassen, damit der aktuelle Bestand jederzeit überprüft werden kann. Die Antragsteller sind darüber zu informieren, an welche Stellen ihre Daten übermittelt werden. Die Empfehlungen wurden realisiert.

Die nächste Stufe der Verarbeitung der Antragsdaten kontrollierte ich anschließend im Landwirtschaftsministerium. Auf der Grundlage der Verordnung (EWG) Nr. 3508/92 wird dort eine automatisierte Datenbank für Kontrollzwecke geführt. Es ist vorgeschrieben, daß fünf Prozent aller Antragsteller stichprobenartig kontrolliert werden müssen. Neben den aufwendigen Vor-Ort-Kontrollen ist auch die Satellitenfernerkundung zugelassen. Mit Hilfe der gefertigten Satellitenfotos kann die Schlaggröße und die Anbaukultur erkannt und dann mit den Angaben des Antragstellers verglichen werden. Zur Auswertung dieser Aufnahmen wurde ein Vertrag mit einer privaten Firma abgeschlossen.

In meinem Kontrollbericht habe ich das Landwirtschaftsministerium darauf hingewiesen, daß es sich bei der Auswertung der Satellitenfotos durch diese Firma um Datenverarbeitung im Auftrag handelt. Deshalb wäre das Ministerium verpflichtet gewesen, mich nach Vertragsabschluß über diese Beauftragung zu informieren (§ 4 Abs. 3 Satz 2 DSG MV). Ich habe unter anderem empfohlen, den Datenschutzhinweis in den Anträgen auf Agrarförderung neu zu formulieren.

Im Februar 1995 teilte mir das Landwirtschaftsministerium mit, daß meine Empfehlungen zu InVeKoS künftig berücksichtigt werden.

2.16. Technisch-organisatorische Maßnahmen

2.16.1. Einige Sicherungsmaßnahmen für Personalcomputer

In der öffentlichen Verwaltung werden personenbezogene Daten häufig mit Personalcomputer (PC) verarbeitet. Obwohl einige Sicherheitsfunktionen auch schon im BIOS (Basic Input/Output System) vieler PC zu finden sind, können die nach § 17 DSG MV erforderlichen technisch-organisatorischen Maßnahmen ohne zusätzliche Sicherheitshard- und -software meistens nicht realisiert werden. Verschiedene Hersteller bieten solche Produkte seit längerer Zeit an.

In PC vorhandene Sicherheitsfunktionen sind beispielsweise Urladepaßwörter und konfigurierbare Sperrmöglichkeiten für Schnittstellen und Laufwerke. Je nach Implementation ist aber oft nur ein kleiner Eingriff in das Gerät notwendig, um diese Sperren zu überwinden.

PC-Sicherheitsprodukte enthalten Funktionen, wie zum Beispiel Paßwortschutz, Bildschirmschoner mit Paßwort, Nutzer- und Rechteverwaltung, konfigurierbare Protokollierung von Management- oder Benutzeraktionen sowie Verschlüsselung von Daten auf Datei- oder Datenträgerebene, deren Überwindung mit erheblichem technischen Aufwand verbunden ist.

Andere Produkte sind dazu bestimmt, die Auswirkungen und ggf. die Ausbreitung von dysfunktionaler Software einzuschränken (Fehler, Trojanische Pferde, Viren, Würmer usw.). Diese Werkzeuge basieren auf einer Vielzahl geeigneter Verfahren:

- Scanner: Programm, das nach speziellen Codesequenzen zum Beispiel von Viren oder "Trojanischen Pferden" sucht. Es ist auf die regelmäßige Aktualisierung des Produktes zu achten.
- Integrity Checker: Programm, das die auf einem Rechner gespeicherte Software und auch Daten auf unzulässige Veränderungen hin überprüft.
- Monitor: Programm oder Hardware zur Prüfung von Schreiboperationen auf Datenträgern. Schreibzugriffe auf Programme und Systembereiche werden abgewiesen.
- Programmsignaturverfahren: Das Ausführen von Programmen wird von einem Freigabeprozeß abhängig gemacht, bei dem die Programme digital signiert werden. Wenn keine passenden Signaturen zu einem Programm vorliegen, wird das Programm nicht abgearbeitet.

Besondere Aufmerksamkeit muß dem normalerweise unkomlizierten Import und Export von Daten und Programmen geschenkt werden. Nach Möglichkeit sind bei Arbeitsplatzcomputern die Schnittstellen zu sperren. Bei vernetzten PC sollte auf Diskettenlaufwerke möglichst ganz verzichtet werden.

Vor der Entscheidung für ein bestimmtes Sicherheitsprodukt sollte der Anwender sich bei unabhängigen Stellen, wie dem Bundesamt für Sicherheit in der Informationstechnik, über die Leistungsfähigkeit dieses Produktes informieren.

2.16.2. Empfehlungen zum Einsatz von tragbaren Computern

Behörden, deren Mitarbeiter personenbezogene Daten auch im Außendienst speichern sollen, haben mich gebeten, Hinweise für den datenschutzgerechten Einsatz von tragbaren Computern (Laptops, Notebooks) zu geben.

Im Außendienst sind bauliche Zugangskontrollmaßnahmen verständlicherweise nicht zu realisieren. Daten und Geräte verlassen den kontrollierten Bereich der Büroumgebung und sind in erhöhtem Maße Gefahren wie Diebstahl oder Verlust ausgesetzt. Zusätzlich begünstigt der modulare Aufbau tragbarer Geräte den Diebstahl einzelner Komponenten. Ohne Werkzeug zu benutzen, kann man mit einem Griff beispielsweise die Festplatte ausbauen.

Die im folgenden empfohlenen technischen und organisatorischen Maßnahmen sollen dazu beitragen, Risiken beim Einsatz tragbarer Computer so zu minimieren, daß auch hier der Schutz personenbezogener Daten weitgehend gewährleistet wird.

Technische Maßnahmen

Um Hardware-Manipulationen zu erschweren, sollten die Notebookgehäuse verplombt werden. Alle Schnittstellen und das Diskettenlaufwerk des Notebooks sind grundsätzlich zu sperren. Die Berechtigung zum Entsperren darf nur der Systemverwalter besitzen. Falls ein Übertragen von Daten regelmäßig nötig ist, darf das nur nach entsprechenden Berechtigungsprüfungen erfolgen.

Alle zur Abarbeitung auf dem Notebook freigegebenen Programme müssen so abgespeichert werden, daß unberechtigte Veränderungen ausgeschlossen sind (z. B. softwaremäßige Versiegelung). Dienstprogramme wie Norton-Utilities, PC-Tools usw. sollten unterwegs nicht zur Verfügung stehen. Das Notebook ist mit Sicherheitshard- und -software auszustatten, die folgende Funktionen bereitstellt:

- Identitäts- und Authentizitätsprüfungen
- Protokollierung auswählbarer Aktivitäten
- Verschlüsselung von Daten
- Realisierung von Zugriffsbeschränkungen
- ein geeignetes Backup-Verfahren in der Büroumgebung
- Suche von Schadprogrammen (Viren, Trojanische Pferde, ...).

Einer Kombination aus Soft- und Hardwarekomponenten ist der Vorzug zu geben, weil dadurch die Verarbeitungsgeschwindigkeit am wenigsten beeinträchtigt wird und Manipulationen sehr erschwert werden. Die Verwendung von entsprechend ausgestatteten PCMCIA-Karten (Personal Computer Memory Card International Association) bieten sich hierfür an. Nur der Besitzer der Karte hat Zugriff auf die Festplatte, und nur mit ihr können die verschlüsselten Daten verarbeitet werden.

Organisatorische Maßnahmen

Die Beschaffung von Hard- und Software der öffentlichen Stelle sollte zentral erfolgen und die nötige Sicherheitsausstattung mit beinhalten, damit auf allen Geräten ein einheitliches Sicherheitskonzept umgesetzt werden kann. Die Geräte sind nach Dienstende grundsätzlich in der Dienststelle unter Verschluß aufzubewahren. In einer Dienstanweisung ist die Nutzung für private Zwecke ist zu untersagen. Dort sollte auch festgeschrieben werden, daß der Einsatz eines Notebooks im Außendienst einer formellen Freigabe bedarf.

2.16.3. Protokollierung

Öffentliche Stellen sind nach § 17 DSG MV verpflichtet, ihre automatisierte Datenverarbeitung so zu gestalten, daß nachträglich feststellbar ist, wer wann welche Daten gelesen oder eingegeben bzw. übermittelt hat. Das ist mit einer Protokollierung der Benutzeraktivitäten zu erreichen, deren Umfang, Kontrolle sowie Speicherdauer sich an der Sensibilität der Daten orientieren sollte. Eine Protokollierung ist freilich nur insoweit sinnvoll, wie auch eine Auswertung der Protokolldaten erfolgt. Diese Auswertung muß mit angemessenem Aufwand möglich sein.

Bei jedem Verfahren ist zu prüfen, mit welchem Protokollierungsumfang die gesetzlichen Bestimmungen erfüllt werden. In einigen Gesetzen sind die Protokollierungsverpflichtungen ausdrücklich genannt, etwa in § 42 Abs. 1 SOG MV (siehe auch Punkt 2.17.2).

Bei Art und Umfang der Protokollierung ist insbesondere zu unterscheiden zwischen Administration und Nutzung. Die Aktivitäten der Administration beinhalten Basisfunktionen, die den Betrieb des Datenverarbeitungs-Systems überhaupt erst möglich machen. Das sind unter anderem: Systemgenerierung, Benutzereinrichtung, Rechtevergabe, Änderungen an Dateien, Datensicherungsmaßnahmen oder Fehlerbeseitigung. Die Protokolle dieser Aktionen sind in geschützten Dateien zu speichern. Diese sollten nur zusammen mit dem internen Datenschutzbeauftragten eingesehen werden können (Vier-Augen-Prinzip).

Es ist zweckmäßig, die Nutzeraktivitäten auf Anwendungsebene zu protokollieren, weil so Unregelmäßigkeiten bei der Anmeldeprozedur (außer Paßwörtern), der Benutzung von automatisierten Abrufverfahren und Löschungen von Daten sowie bei Dateneingaben und Datenübermittlungen am besten zu erfassen sind.

Protokolldaten lassen sich leicht zur Kontrolle der Mitarbeiter mißbrauchen. Wenn jedoch ausschließlich zu Zwecken der Datenschutzkontrolle oder der Datensicherung protokolliert wird, dann dürfen die Daten auch nur zu diesem Zweck genutzt werden (§ 9 Abs. 2 DSG MV). Die Prüfung der Protokolle sollte deshalb nach einem Revisionskonzept erfolgen, das den Inhalt der Protokolle sowie Auswertungsverfahren und Speicherungsdauer festlegt.

Vom Arbeitskreis "Technische und organisatorische Datenschutzfragen" (siehe Abschnitt 2.21) wurde eine Orientierungshilfe zu Fragen der Protokollierung ausgearbeitet, die in meiner Dienststelle kostenlos erhältlich ist.

2.16.4. Verschlüsselung im Dienste des Datenschutzes

Die Fortschritte in der Kryptografie machen es möglich, daß sichere Verschlüsselungsverfahren heute nicht mehr beispielsweise nur Geheimdiensten, sondern bereits dem Normalverbraucher preisgünstig zur Verfügung stehen. Kryptografische Verfahren eignen sich für den Schutz der Daten auf Laptops und in Rechnernetzen, aber auch zur Erhöhung der Datensicherheit auf vernetzten PC und Stand-alone-Geräten. Mit kryptografischen Methoden lassen sich die Vertraulichkeit und die Integrität von Daten sichern. Darüber hinaus sind Verschlüsselungsverfahren verwendbar, um jeder Aktion in einem IT-System einen Urheber zuordnen zu können (Zurechenbarkeit). Somit kann auch die Verbindlichkeit elektronischer Kommunikation sichergestellt werden.

Jeder Datenschutzbeauftragte sollte sich Grundkenntnisse über Verschlüsselungsverfahren aneignen, um sie im Rahmen seiner Beratungstätigkeit als Hilfsmittel zum Schutz personenbezogener Daten empfehlen zu können.

Gegenwärtig kommen zwei unterschiedliche Verfahrensklassen zum Einsatz:

Symmetrische Verschlüsselungsverfahren verwenden zur Ver- und Entschlüsselung den gleichen Schlüssel. Die geheimzuhaltenden Schlüssel müssen deshalb zwischen den Partnern ausgetauscht werden. Bei mehreren Partnern bedingt das eine aufwendige Schlüsselverwaltung. Bekannte symmetrische Verschlüsselungsverfahren sind DES (Data Encryption Standard) und dessen Weiterentwicklung Triple-DES.

Bei den asymmetrischen Verfahren wird ein Schlüsselpaar erzeugt: der öffentliche Schlüssel und der geheime Schlüssel. Ein mit dem öffentlichen (allgemein zugänglichen) Schlüssel verschlüsseltes Dokument kann nur mit dem dazugehörigen privaten (geheimen) Schlüssel entschlüsselt werden. Werden die Schlüssel umgekehrt verwendet, dann kann mit dem öffentlichen Schlüssel geprüft werden, ob ein Dokument vom Besitzer des geheimen Schlüssels verschlüsselt, also elektronisch unterschrieben wurde (elektronische Signatur). Für beide Anwendungen müssen die Schlüssel nicht vertraulich ausgetauscht werden. Voraussetzung für die Sicherheit des Verfahrens ist jedoch, daß der öffentliche Schlüssel authentisch ist. In der Praxis wird häufig das Verfahren RSA eingesetzt (benannt nach den Entwicklern Rivest, Shamir und Adleman). RSA erfordert eine höhere Rechenleistung als DES. Deshalb wird es nur für kleine Datenmengen oder in Kombination mit dem DES zum Schlüsselaustausch verwendet. Mit RSA ist sowohl Verschlüsselung als auch Signatur möglich.

Triple-DES sowie RSA mit 1024 Bit Schlüssellänge gelten nach den heutigen Erkenntnissen und der mittelfristig abschätzbaren Entwicklung der Rechentechnik als hinreichend sicher. Es ist allerdings schwer voraussagbar, wie sich die Rechentechnik und insbesondere die Erkenntnisse über die Kryptoalgorithmen in den nächsten Jahrzehnten entwickeln werden. Möglicherweise gelten die heute noch als sicher anzusehende Verschlüsselungsverfahren in wenigen Jahren als unbrauchbar.

Für Netze sowie für Einzelanwendungen wird eine Vielzahl von Verschlüsselungshard- und -software angeboten, um eine sichere Kommunikation und Datenspeicherung zu gewährleisten. Neben den Verschlüsselungsverfahren selbst entscheiden auch die verwendeten kryptografischen Protokolle und die sorgfältige Implementation sowie die Einsatzumgebung über die Sicherheit des Produktes.

Beim breiten Einsatz kryptografischer Methoden ergeben sich eine Reihe verfahrenstechnischer und rechtlicher Probleme. Die Bestätigung der Echtheit von öffentlichen Schlüsseln (Zertifizierung) und deren Verteilung sind nur mit einer geeigneten Infrastruktur realisierbar. Es muß eine vertrauenswürdige Instanz (Trust-Center) gefunden werden, die diese Aufgabe zugewiesen bekommt.

Damit beweissichere elektronische Verfahren beispielsweise zum Abschluß von Verträgen eingesetzt werden können, müssen elektronische Signaturen und handgeschriebene Unterschriften rechtlich gleichgestellt werden. Mit dem Referentenentwurf einer Verordnung über die Elektronische Unterschrift (VEU) aus dem Bundesinnenministerium werden erste Versuche in diese Richtung unternommen.

2.16.5. IT-Sicherheitskonzepte - nur überflüssige Bürokratie?

In vielen Bereichen der öffentlichen Verwaltung wird Informationstechnik (IT) eingesetzt, um Verwaltungsprozesse zu beschleunigen und die Arbeit effizienter zu gestalten. Einige Behörden begeben sich damit jedoch in eine Abhängigkeit von dieser Technik, die beim Versagen bis zur Arbeitsunfähigkeit führen kann: Anträge werden nicht mehr bearbeitet, Zahlungen an falsche Empfänger geleistet oder Auskünfte nicht mehr erteilt. Der datenschutzgerechte Umgang mit elektronisch gespeicherten personenbezogenen Daten ist dann in hohem Maße gefährdet.

Deshalb ist für jedes IT-Verfahren ein Datenschutz- und IT-Sicherheitskonzept zu erarbeiten, das die erforderlichen und angemessenen technischen und organisatorischen Maßnahmen enthält. Die Empfehlungen des BSI oder der IT-Strukturrahmen für die Landesverwaltung Mecklenburg-Vorpommern (ITSR) können hierbei geeignete Hilfen sein. Laut ITSR ist der IT-Sicherheitsbeauftragte dafür zuständig, in Zusammenarbeit mit dem Datenschutzbeauftragten ein Sicherheitskonzept mit geeigneten Maßnahmekatalogen zu erstellen. Es sollten aber auch die Mitarbeiter der entsprechenden Fachabteilungen beteiligt werden, da deren Kenntnisse, etwa über die Arbeitsorganisation, unerläßlich sind.

In den BSI-Handbüchern wird der Aspekt des Schutzes personenbezogener Daten und der Gewährleistung des informationellen Selbstbestimmungsrechtes zwar noch nicht in ausreichendem Maße berücksichtigt, aber die vorgestellten Verfahren sind prinzipiell anwendbar, um IT-Sicherheitskonzepte zu erstellen.

Im BSI-Sicherheitshandbuch werden dazu vier Schritte vorgeschlagen:

1. Die Schutzbedürftigkeit des IT-Verfahrens ist festzustellen. Ein Verfahren beinhaltet dabei Hardware, Software und verarbeitete - insbesondere personenbezogene - Daten.
2. Die Bedrohungen sind zu ermitteln, die das ausgewählte Verfahren gefährden könnten.
3. Im Rahmen einer Risikoanalyse wird bewertet, wie stark sich diese Bedrohungen auf das Verfahren auswirken können, welche Risiken also tatsächlich bestehen.
4. Es werden diejenigen Maßnahmen ausgewählt und im Sicherheitskonzept festgehalten, die notwendig und angemessen sind, um das Risiko auf ein hinnehmbares Maß zu reduzieren.

Ein vereinfachtes Verfahren, bei dem sich der Aufwand zur Erstellung von Sicherheitskonzepten an der Schutzwürdigkeit der Anwendung orientiert, wird im BSI-Grundschutzhandbuch beschrieben. Daten, Hard- und Software werden entsprechend ihrer Schutzbedürftigkeit mit Hilfe dreier Schutzstufen klassifiziert. Erfolgt eine Zuordnung zur niedrigsten Schutzstufe, sind keine zusätzlichen Sicherheitsmaßnahmen notwendig. Die Zuordnung zur mittleren Schutzstufe verlangt die Erstellung eines Sicherheitskonzeptes durch Auswahl geeigneter Maßnahmen aus dem Katalog des Grundschutzhandbuches, ohne vorher eine detaillierte Risikoanalyse durchführen zu müssen. Die Ausarbeitung eines Sicherheitskonzeptes mit der oben beschriebenen aufwendigen Methode des BSI-Sicherheitshandbuches ist nur noch erforderlich, wenn die Zuordnung zur höchsten Schutzstufe erfolgt ist.

Das im BSI-Grundschutzhandbuch dargestellte Vorgehen halte ich für praktikabel, wenn die Schutzwürdigkeit der personenbezogenen Daten ausreichend berücksichtigt wird. Diese sollten grundsätzlich mindestens der mittleren Schutzstufe zugeordnet werden.

Für alle vorgestellten Verfahren gilt jedoch, daß bei einem zu hohen und damit nicht akzeptierbaren Restrisiko möglicherweise ganz auf den Einsatz des IT-Verfahrens verzichtet werden muß. Deshalb ist bereits in der Planungsphase eine ausreichende Berücksichtigung von Datenschutz und IT-Sicherheit besonders wichtig.

Ein beispielhaftes IT-Sicherheitskonzept wurde für das Landesweite Polizei Informationssystem (LAPIS) erstellt. Nach anfänglichen Schwierigkeiten (siehe Punkt 2.17.2) wurde unter angemessener Berücksichtigung der Gefährdungen bei der Verarbeitung personenbezogener Daten das im BSI-Sicherheitshandbuch vorgeschlagene Verfahren angewandt. So entstand ein Sicherheitskonzept, das sich auf einzelne Dienststellen, eingebundene Verfahren, benutzte Netze und verwendete Endsysteme bezieht und das aufgrund seiner Modularität einfach erweiterbar ist und entsprechend der technischen Weiterentwicklung fortgeschrieben werden kann. Ich wurde rechtzeitig beteiligt und konnte dadurch bereits in der Planungsphase datenschutzrechtliche Empfehlungen geben.

2.16.6. Dienstanweisungen und Dienstvereinbarungen

Dienstanweisungen

Bei einigen Kontroll- und Informationsbesuchen habe ich festgestellt, daß bisweilen keine oder nur unzureichende Dienstanweisungen zur Einhaltung des Datenschutzes vorlagen. Dienstanweisungen sind jedoch ein notwendiges und durchaus geeignetes organisatorisches Hilfsmittel, um den Mitarbeitern Hinweise für den datenschutzgerechten Umgang mit personenbezogenen Daten bei der täglichen Arbeit zu geben. Für einige Bereiche der öffentlichen Verwaltung sind solche Dienstanweisungen ausdrücklich vom Gesetzgeber gefordert, zum Beispiel für Leistungsträger gemäß § 35 Abs. 1 SGB I in § 78a SGB X und für Krankenkassen und Kassenärztliche Vereinigungen in § 286 Abs. 3 SGB V. Eine allgemeine Dienstanweisung zum Datenschutz sollte jedoch in jeder Behörde vorhanden sein.

Folgendes müßte sie mindestens beinhalten:

- Hinweise zu personellen Fragen

    • Verantwortlichkeiten und Zuständigkeitsregelungen
    • Vertretungsregelungen
    • Art und Weise der Verpflichtung auf Wahrung des Datengeheimnisses
    • Regelungen zu Besuchern, Wartungs- und Reinigungspersonal

- Regelungen zur automatisierten Verarbeitung personenbezogener Daten
    • Datenträgerverwaltung
    • Löschen von Daten
    • Datensicherung
    • Gestaltung und Verwendung von Paßwörtern
    • Einsatz von privater Hard- und Software

- Regelungen zum Verfahren bei Auskunftsersuchen Betroffener
- Regelungen zum Umgang mit Schriftgut (Entsorgung, Lagerung usw.)
- Erläuterung bereits bestehender Maßnahmen zum Datenschutz

Dienstvereinbarungen

In öffentlichen Stellen werden immer mehr automatisierte Verfahren zum Umgang mit personenbezogenen Daten der Beschäftigten eingeführt oder ältere Verfahren dem Stand der Technik angepaßt. In diesem Zusammenhang bin ich mehrfach darum gebeten worden, bei der Ausarbeitung von Dienstvereinbarungen zu beraten oder bei vorliegenden Vereinbarungen die datenschutzgerechte Ausgestaltung zu prüfen.

Auch Kontroll- und Informationsbesuche haben oft gezeigt, daß Dienstvereinbarungen nicht den Anforderungen entsprachen oder nicht vorhanden waren. Sie sind jedoch notwendig, um die Mitbestimmung der Personalvertretung gemäß § 70 PersVG sicherzustellen und das informationelle Selbstbestimmungsrecht derjenigen zu schützen, deren personenbezogene Daten automatisiert verarbeitet werden. Gemäß § 66 Abs. 2 PersVG werden solche Dienstvereinbarungen zwischen Behördenleiter und Personalvertretung abgeschlossen, wenn automatisierte Verfahren zum Umgang mit personenbezogenen Daten der Beschäftigten eingeführt oder wesentlich geändert werden.

Um die datenschutzgerechte Ausgestaltung der Dienstvereinbarungen zu gewährleisten, sollte der behördliche Datenschutzbeauftragte immer beteiligt werden. Hat das betreffende Verfahren landesweite Bedeutung, sollte ich in die Beratungen mit einbezogen werden.

Diese Vorgehensweise ist bereits erfolgreich bei der Ausarbeitung der Musterdienstvereinbarung zum Einsatz des Personal- und Stellenverwaltungssystems PERSYS für die Landesverwaltung Mecklenburg-Vorpommern (siehe Punkt 2.13.3) praktiziert worden.

Mein Beratungsangebot bei der Ausarbeitung von Dienstvereinbarungen wurde auch in anderen Bereichen in Anspruch genommen, beispielsweise beim Einsatz von ISDN-Anlagen (siehe Punkt 2.18.1) in obersten Landesbehörden, Stadtverwaltungen und Krankenhäusern.

2.17. Einzelverfahren und Vorhaben im Land

2.17.1. Geld und Arbeitszeit verschenkt durch Verzicht auf Beratung?

Während des ersten Berichtszeitraumes arbeitete ich erfolgreich mit dem Interministeriellen Ausschuß für Informations- und Telekommunikationstechnik (IMA-IT) zusammen. Unter Federführung des Innenministers koordiniert dieser Ausschuß den Einsatz von Informations- und Telekommunikationstechnik in den öffentlichen Stellen des Landes. Seit Mitte 1993 wurde ich nicht mehr zu den Sitzungen des IMA-IT eingeladen.

Werden automatisierte Verfahren zur Verarbeitung personenbezogener Daten eingesetzt, sind technisch-organisatorische Maßnahmen zu treffen, die einen angemessenen Schutz dieser Daten sicherstellen. Viele dieser Maßnahmen sind mit finanziellen Aufwendungen verbunden. Die frühzeitige Berücksichtigung meiner Empfehlungen kann dazu beitragen, diese Kosten zu minimieren.

Das neue Verfahren zum Haushalts-, Kassen-, Rechnungswesen PROfiskal (siehe Punkt 2.17.3) ist ein solches automatisiertes Verfahren mit landesweiter Bedeutung. Allerdings wurde ich erst auf eigenes Bemühen hin in die Planung dieses Verfahrens mit einbezogen.

Auch die verfahrensunabhängige, datenschutzgerechte Ausgestaltung der gesamten IT-Landschaft muß gewährleistet sein. Ich denke dabei zum Beispiel an den Einsatz von Produkten, die einen angemessenen Sicherheitsstandard für Personalcomputer realisieren. Die Definition eines Landesstandards im ITSR ist dringend notwendig. Nach Abschluß entsprechender Rahmenverträge könnten geeignete Produkte wesentlich kostengünstiger beschafft werden, als es einzelnen Dienststellen bisher möglich ist.

Schon in meinem Ersten Tätigkeitsbericht habe ich empfohlen, die gemäß § 16 DSG MV zu führenden Dateibeschreibungen und Geräteverzeichnisse mit den Anforderungen der IT-Verzeichnisse der Landeshaushaltsordnung und der IT-Richtlinien des Landes abzustimmen und ein automatisiertes Verfahren zu entwickeln, das den Verwaltungsaufwand minimiert. Noch immer wird jedoch kostbare Arbeitszeit verschwendet, indem diese Verzeichnisse unabhängig voneinander und manuell geführt werden.

Seit November 1995 werde ich an der Überarbeitung des Abschnittes Datenschutz/Datensicherheit des ITSR beteiligt. Der Innenminister hat mich um Stellungnahme zum Entwurf dieses Teils des ITSR gebeten. Auch zu den Sitzungen der Arbeitsgruppe, die Anforderungen an landeseinheitliche Verfahren für Bürokommunikation und Schriftgutverwaltung definieren soll, wurde ich eingeladen, um rechtzeitig datenschutzrechtliche Empfehlungen zu geben. Möglicherweise ist das ein erster Schritt, die Kontakte zum IMA-IT wieder zu intensivieren.

2.17.2. IT-Sicherheit bei der Landespolizei im zweiten Anlauf

Im Rahmen des Projektes LAPIS (siehe auch Punkt 2.16.5) werden alle Polizeidienststellen des Landes mit einheitlicher Informations- und Kommunikationstechnik ausgestattet. Ziel ist eine umfassende DV-Unterstützung am Arbeitsplatz jedes Polizeibeamten. Sowohl Bürokommunikationsfunktionen (etwa Kommunikation zwischen den Dienstellen oder Textverarbeitung) als auch polizeispezifische Anwenderfunktionen (etwa INPOL-Land, INPOL-Bund, ZEVIS und polizeiliche Vorgangsbearbeitung) werden an den neuen Arbeitsplätzen zur Verfügung stehen.

Erste Konzepte zur Realisierung dieses Projektes gab es bereits 1992. Seit November 1993 nehme ich an den Projektbesprechungen teil und berate in mehreren Arbeitskreisen zu Fragen des Datenschutzes und der IT-Sicherheit von LAPIS.

Mit der Realisierung von LAPIS wird eine neue Qualität in der polizeilichen Datenverarbeitung erreicht. Bedingt durch die zentrale Datenhaltung und die einheitliche Ausstattung der einzelnen Polizeiarbeitsplätze kann prinzipiell von jedem Rechner aus jedes Einzelverfahren genutzt werden. Da jeder Bürger, sowie er mit der Polizei in Berührung kommt, sei es als Beschuldigter oder Verdächtiger, als Opfer, Geschädigter, Zeuge, Hinweisgeber oder Auskunftsperson, elektronische Spuren hinterläßt, entstehen nunmehr qualitativ neue Anforderungen an die Wahrung des informationellen Selbstbestimmungsrechtes des Betroffenen. Ein Informationssystem dieser Qualität versetzt die Polizei in die Lage, in einem bisher nicht vorstellbaren Umfang auch solche personenbezogene Daten gezielt abrufbar vorzuhalten, die der einzelne Bearbeiter nicht in jedem Fall benötigt. Deshalb spielen Fragen des Datenschutzes und der IT-Sicherheit eine entscheidende Rolle bei der Ausgestaltung von LAPIS.

Frühzeitig habe ich die Erstellung eines umfassenden Datenschutz- und IT-Sicherheitskonzeptes empfohlen. Die Definition und Umsetzung von Maßnahmen zur Sicherstellung von Vertraulichkeit, Verfügbarkeit und Integrität sind Voraussetzung für den Betrieb von LAPIS. Zur Erstellung eines solchen Konzeptes wurde im Auftrag des Innenministers der Arbeitskreis Sicherheit ins Leben gerufen. Zukünftigen Anwendern, Firmenvertretern und Projektverantwortlichen habe ich in diesem Rahmen meine Empfehlungen zu Datenschutzfragen erläutert. Ein externer Dienstleister wurde mit der Ausarbeitung eines Konzeptentwurfs beauftragt. Dieser Entwurf lag zum geplanten Start der Pilotphase am 1. Juni 1994 jedoch nicht vor.

Nachdem ich meine Bedenken mitgeteilt hatte, die Pilotphase ohne vorliegendes Datenschutz- und IT-Sicherheitskonzept zu starten, wurde vom Innenminister der Starttermin um drei Monate verschoben. Die verbleibende Zeit wurde intensiv genutzt, um die Struktur des Konzeptes zu überarbeiten und die für den Pilotbetrieb notwendigen Teilkonzepte fertigzustellen. Alle für LAPIS verwendeten Hard- und Softwarekomponenten und alle beteiligten Organisationseinheiten werden nun als einzelne Module betrachtet (siehe Punkt 2.16.5), die entsprechend des Projektfortschrittes separat bearbeitet werden können.

Am 1. September 1994 konnte dann "im zweiten Anlauf" die LAPIS-Pilotphase mit einem vorliegenden IT-Sicherheitskonzept starten. Zu diesem Zeitpunkt waren noch längst nicht alle im Konzept geforderten technisch-organisatorischen Maßnahmen zum Datenschutz umgesetzt. In einem Zeitplan wurden jedoch Termine für die Realisierung der einzelnen Maßnahmen festgeschrieben. Im Rahmen der weiteren Begleitung des Projektes wird die Einhaltung dieser Termine regelmäßig überprüft.

Zwei der im Sicherheitskonzept vorgesehenen technisch-organisatorischen Maßnahmen erscheinen mir besonders erwähnenswert - die Verschlüsselung von Daten bei der Übertragung in Weitverkehrsnetzen und die Protokollierung von Nutzeraktivitäten.

Die Übertragung der Daten zwischen den verschiedenen an LAPIS angeschlossenen Dienststellen erfolgt innerhalb einer geschlossenen Nutzergruppe im Weitverkehrsnetz LAVINE (Landesdaten-Vermittlungs- und Informationsnetz), dem Behördennetz Mecklenburg-Vorpommerns. Dazu werden gemietete öffentliche Leitungen genutzt. Wegen der besonderen Sensibilität der in LAPIS verarbeiteten personenbezogenen Daten und unter Berücksichtigung der Gefährdung der Vertraulichkeit bei der Übertragung habe ich Verschlüsselung gefordert. Nach eingehender Untersuchung der Risiken bei der Nutzung solcher Übertragungswege wurde diese Forderung in das Sicherheitskonzept aufgenommen. Zur Zeit laufen die Untersuchungen nach geeigneter Hard- und Software, die auch entsprechende Anforderungen aus dem Geheimschutzbereich erfüllen kann.

Das erste INPOL-Land-Verfahren, das in LAPIS in Betrieb genommen wurde, ist das neu konzipierte PED-Verfahren (Polizeiliche Erkenntnisdatei). In den Errichtungsanordnungen für die einzelnen PED-Dateien war eine automatisierte Protokollierung aller Zugriffe auf den PED-Datenbestand zunächst nicht vorgesehen. Der im § 42 Abs. 1 SOG MV genannten Forderung nach "überprüfbarer Aufzeichnung der Abrufe" wäre auf diese Art und Weise nicht entsprochen worden. Mitarbeiter des Innenministeriums und des LKA formulierten entsprechend meinen Empfehlungen Vorgaben, nach denen ein automatisches Protokollierungsverfahren durch entsprechende Ergänzungen in der PED-Software realisiert wurde. Das Verfahren wurde mir vor der Übernahme in die PED-Produktionsumgebung vorgestellt. Es entspricht nunmehr einschließlich der automatisierten Auswertungsmöglichkeiten meinen Empfehlungen (siehe auch Punkt 2.16.3).

2.17.3. Profiskal

Das Finanzministerium unseres Landes plant, die zur Zeit im Bereich des Haushalts-, Kassen- und Rechnungswesen (HKR) eingesetzte HKR-Software durch die an die Bedürfnisse Mecklenburg-Vorpommerns angepaßte Standardsoftware PROfiskal zu ersetzen. Das neue Verfahren soll zentral auf Rechnern des DVZ zur Anwendung kommen, auf denen auch alle Daten gehalten werden. Die Kassen und Dienststellen des Landes werden mit Terminalanbindungen über das Behördennetz Mecklenburg-Vorpommerns LAVINE an das Verfahren angeschlossen.

Durch das neue System werden in beträchtlichem Umfang personenbezogene Daten verarbeitet, beispielsweise Namen, Anschriften, Bankverbindungen, Daten eventueller Mahnungen und eingeleiteter Vollstreckungsverfahren von Zahlungspflichtigen. In ähnlichem Ausmaß finden Übermittlungen von und zu anderen öffentlichen Stellen statt. So soll das System zum Beispiel personenbezogene Daten im Rahmen des Zahlungsverkehrs zwischen den Landesbehörden und den Landesbediensteten erhalten und Informationen über erfolgte Auszahlungen an andere Stellen übergeben, etwa zur Überwachung der Zahlungseingänge im BAFöG-Verfahren. In Anbetracht der Dimension und Komplexität des Verfahrens, der hierfür eingesetzten Datenverarbeitungs- und Kommunikationstechnik sowie der damit verbundenen personellen und organisatorischen Struktur sind technisch-organisatorische Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit erforderlich.

Im Juni 1994 wurde eine Projektgruppe mit Vertretern des Finanzministeriums, des DVZ und der Softwarefirma gebildet, um den Stand des Projektes sowie die bei der Implementierung und Anpassung auftretenden Probleme zu besprechen. Im Juli 1994 erhielt ich Unterlagen zu dem Verfahren. Seitdem nehme ich an den Projektsitzungen teil und kann daher rechtzeitig datenschutzrechtliche Hinweise geben. So habe ich empfohlen, unter anderem folgende Punkte zu berücksichtigen:

- Der für die Aufgabenerfüllung nicht erforderliche uneingeschränkte Zugriff aller Nutzer auf die gesamte Datei der Zahlungspartner (Zahlungspflichtige und Zahlungsempfänger) muß vor Beginn der Echtdaten-Verarbeitung unterbunden werden.

- Die Verwendung von Freitextfeldern ist verbindlich zu regeln.

- In Dienstanweisungen ist festzulegen, welche Recherchen unter welchen Voraussetzungen zulässig sind.

- Es ist eine klare Abgrenzung zwischen Einmalzahlern und ständigen Zahlungspartnern zu treffen, da nur letztere dauerhaft gespeichert werden dürfen.

- Vor Beginn der Echtdaten-Verarbeitung ist ein Datenschutz- und IT-Sicherheitskonzept zu erstellen, in dem alle erforderlichen technisch-organisatorischen Maßnahmen aufgeführt werden.

Die von mir empfohlene Trennung zwischen Einmalzahlern und ständigen Zahlungspartnern ist bereits erfolgt. Des weiteren erhielt ich im Oktober 1995 den ersten Entwurf des Betriebshandbuches, das auch eine Konzeption zum Datenschutz und zur Datensicherheit beinhaltet.

Die bisherige Zusammenarbeit mit dem Finanzministerium und dem DVZ bei der Einführung des neuen HKR-Verfahrens war konstruktiv. Auch nach Beginn der Echtdaten-Verarbeitung im Laufe des Jahres 1996 werde ich das Projekt weiterhin beratend begleiten.

2.17.4. ARGUS: Rechtspflege oder Verwaltung?

Im Februar 1994 hatte der Justizminister unseres Landes bekanntgegeben, daß die Gerichte Mecklenburg-Vorpommerns vernetzt werden sollen.

An den Planungen zu diesem Verfahren war ich nicht beteiligt worden. Deshalb bat ich darum, mich über Einzelheiten zu informieren. Mir wurden die Unterlagen des "Allgemeinen Register- und Informationssystems für Gerichte und Staatsanwaltschaften" (ARGUS) zur Prüfung überlassen. Bei dieser Prüfung war zu berücksichtigen, daß das DSG MV für Gerichte nur gilt, soweit sie Verwaltungsaufgaben wahrnehmen. Lediglich in diesem Fall stehen dem Landesdatenschutzbeauftragten die im DSG MV genannten Kontrollbefugnisse zu. Und auch nur dann besteht die Pflicht, ihn rechtzeitig über die Entwicklung und Nutzung von Verfahren, mit denen personenbezogene Daten verarbeitet werden, zu benachrichtigen (§ 29 Abs. 5 DSG MV). Es war also zunächst zu prüfen, ob durch ARGUS ausschließlich rechtspflegerische Tätigkeiten in den Gerichten unterstützt oder ob damit auch Verwaltungsaufgaben wahrgenommen werden sollen.

Nicht in jedem Fall sind diese beiden Bereiche eindeutig voneinander zu trennen. Ein inzwischen allgemein anerkanntes Hilfsmittel zur Klassifizierung der in einem Gericht anfallenden Tätigkeiten ist die sogenannte Hamburger Liste. Diese Liste hat der Hamburger Senat auf Ersuchen der Bürgerschaft im Frühjahr 1993 erstellt, um alle verfassungsrechtlichen Möglichkeiten einer Datenschutzkontrolle bei Gerichten sicherzustellen und Fragen der Kontrollbefugnis des Hamburgischen Datenschutzbeauftragten zu klären. Zwischen dem Justizminister und mir bestand Einigkeit darüber, daß die "Hamburger Liste" als Leitlinie für die vorzunehmende Abgrenzung grundsätzlich auch in Mecklenburg-Vorpommern geeignet ist.

Die Prüfung der ARGUS-Unterlagen unter Anwendung dieser Liste ergab, daß - wenn das Verfahren so realisiert wird, wie es in den Unterlagen beschrieben worden ist - tatsächlich auch verwaltungstechnische Tätigkeiten von ARGUS wahrgenommen werden. Allerdings kam der Justizminister bei seiner Prüfung zu dem Ergebnis, daß "bislang ausschließlich rechtspflegerische Aufgaben und entsprechende Hilfstätigkeiten, aber keine Verwaltungsangelegenheiten" unterstützt werden.

Im Ergebnis der Diskussionen um den Einsatz von ARGUS kamen wir überein, daß ich in Zukunft auch über solche Verfahrensentwicklungen unterrichtet werde, bei denen es zweifelhaft sein kann, ob Verwaltungsanteile in den Programmen enthalten sind.

Ich habe Vorschläge zur Änderung des DSG MV unterbreitet, wie eine klarere Regelung der Zuständigkeit des Landesdatenschutzbeauftragten bei den Gerichten erreicht werden kann (siehe hierzu auch Abschnitt 4).

2.18. Post- und Fernmeldewesen, Datenfernverarbeitung

2.18.1. Vorsicht beim komfortablen Telefonieren

Bei Kontroll- und Informationsbesuchen habe ich festgestellt, daß inzwischen in vielen öffentlichen Stellen digitale Telekommunikationsanlagen (TK-Anlagen) eingesetzt werden. Es handelt sich dabei in den meisten Fällen um ISDN-Anlagen, die noch wesentlich leistungsfähiger als herkömmliche digitale TK-Anlagen sind. ISDN steht für Integrated Services Digital Network (digitales diensteintegrierendes Netz) und gilt als digitales Kommunikationsnetz der Zukunft. ISDN integriert die Übertragung von Sprache, Text, Bild und Daten in einem Netz. Für alle Dienste werden einheitliche Rufnummern, Gebühren und Schnittstellen zur Verfügung gestellt. Zahlreiche nützliche Funktionen vereinfachen die Kommunikation.

Gefährdungen beim Einsatz von ISDN-TK-Anlagen

Werden ISDN-TK-Anlagen nicht datenschutzgerecht eingesetzt, so ist unter Umständen die Anonymität der Kommunikation gefährdet. Kommunikationsprofile einzelner Beschäftigter könnten erstellt, das Verhalten und die Leistung von Beschäftigten überwacht oder gezielt Gespräche abgehört oder aufgezeichnet werden.

Die Steuerung des gesamten Kommunikationsvorganges und der Gebührenabrechnung der einzelnen Gespräche erfolgt durch die TK-Anlagensoftware. Dazu werden auch personenbezogene Daten in der ISDN-TK-Anlage gespeichert. In ISDN-TK-Anlagen können drei Gruppen von gespeicherten Daten unterschieden werden:

- Bestandsdaten: zum Beispiel Art des Endgerätes, Einträge im elektronischen Telefonbuch, nutzbare Funktionen
- Verbindungsdaten: zum Beispiel Kommunikationspartner, Zeit und Dauer des Gespräches, Gebühreninformationen
- Inhaltsdaten: zum Beispiel Gesprächsinhalte, Texte, Daten.

Im folgenden werden einige datenschutzrechtlich relevante Eigenschaften von ISDN-TK-Anlagen kurz beschrieben:

<u>Gesprächsdatenerfassung</u>
Zur ordnungsgemäßen Abrechnung der Kosten kann man zu jedem Kommunikationsvorgang Gesprächsdaten (Nebenstellennummer, Zielnummer, Gesprächsdauer usw.) speichern. Werden diese Daten zweckentfremdet verwendet, wäre es durchaus möglich, Kommunikationsprofile zu erstellen und beispielsweise Mitarbeiter zu überwachen.

<u>Rufnummernanzeige</u>
Findet ein Kommunikationsvorgang zwischen zwei ISDN-fähigen Nebenstellen statt, kann die Telefonnummer des Anrufenden auf einem Display beim Angerufenen angezeigt werden. Durch uneingeschränkte Nutzung dieses Merkmals wird die Anonymität der Kommunikation gefährdet, da auch Personen, die am Gespräch unbeteiligt sind, den Gesprächspartner allein schon durch einen Blick auf das Display feststellen können. Noch einfacher geht das bei den ISDN-TK-Anlagen, die darüber hinaus noch die Anzeige des Namens des Anrufers gestatten. Einrichtungen, denen gegenüber der Anrufer anonym bleiben möchte, sollten die Rufnummernanzeige ständig abschalten; dies betrifft beispielsweise Beratungsstellen.

Konferenzschaltung
Eine Konferenzschaltung ermöglicht, daß mehr als zwei Gesprächspartner gleichzeitig miteinander kommunizieren. Zu Beginn und Ende einer Konferenz ertönt ein Signal. Ist den Beteiligten die Bedeutung dieses Signals nicht bekannt, können Gespräche ohne Wissen der Teilnehmer mitgehört werden.

Aufschalten
Durch Aufschalten ist es möglich, ein bestehendes Gespräch mitzuhören. Auch hier erfolgt eine Signalisierung durch einen entsprechenden Ton, dessen Bedeutung den Nutzern der ISDN-TK-Anlage bekannt sein muß, um einen Mißbrauch weitgehend auszuschließen.

Raumüberwachung
Endgeräte moderner ISDN-TK-Anlagen verfügen oft über Freisprecheinrichtungen, die ein Telefonieren bei aufgelegtem Hörer gestatten. Diese Einrichtung kann unter bestimmten Voraussetzungen auch dazu benutzt werden, einen Raum akustisch zu überwachen und die dort geführten Gespräche mitzuhören.

Der datenschutzgerechte Einsatz von ISDN-TK-Anlagen ist nur dann gewährleistet, wenn zumindest die im § 17 Abs. 2 DSG MV geforderten technisch-organisatorischen Maßnahmen umgesetzt worden sind. Dabei sind folgende Grundschutzmaßnahmen vorzusehen:

- Durch geeignete bautechnische Maßnahmen sind die ISDN-TK-Anlage und die Bedienplätze vor unberechtigtem Zugang zu schützen. Dazu sind Zutrittsregelungen und -kontrollen notwendig.
- Voreingestellte Paßwörter sind sofort nach der Inbetriebnahme der Anlage zu ändern.
- Auf die Nutzung von Fernwartungszugängen ist nach Möglichkeit zu verzichten.
- Alle Administrationsaktivitäten sind zu protokollieren.
- Durch genaue Buchführung der Anlagenkonfiguration ist die Revisionssicherheit zu gewährleisten.

Ich empfehle, die Hinweise des BSI zu berücksichtigen, die im Band 1 der "Schriftenreihe zur IT-Sicherheit" (Sicherheitsmaßnahmen beim Betrieb von digitalen Telekommunikationsanlagen) veröffentlicht wurden.

Dienstvereinbarungen über die Nutzung von ISDN-TK-Anlagen

Der Abschluß einer Dienstvereinbarung zwischen Personalvertretung und Behördenleitung gehört zu den grundlegenden organisatorischen Maßnahmen, ohne die eine ISDN-TK-Anlage nicht in Betrieb genommen werden darf. Eine solche Dienstvereinbarung sollte aus zwei Teilen - dem Hauptteil und der Anlage - bestehen.

In den Hauptteil gehören folgende allgemeingültige und für einen längeren Zeitraum geltende Regelungen:

- Grundsatzbestimmungen (Zweck, Gegenstand, Geltungsbereich),
- Nutzungsumfang (dienstlich, privat, Sprache, Text, Daten, Hinweise zu technischen Details im Anhang),
- verarbeitete personenbezogene Daten (Art und Zweck der Verarbeitung),
- Gesprächsdatenverarbeitung (Ausnahmen der Gesprächsdatenerfassung, Einzelheiten der Gebührenabrechnung für private und dienstliche Gespräche),
- Betriebsführung der Anlage (Systemverwaltung, Wartung, Datenschutz und Datensicherheitsmaßnahmen),
- Kontroll- und Mitwirkungsrechte (Beteiligung des Personalrates und des internen Datenschutzbeauftragten),
- Schlußbestimmungen (Inbetriebnahme, Änderungsverfahren im Rahmen von Fortschreibungen, Kündigungsregelungen).

Besonders sensibel sind Regelungen zur Gesprächsdatenerfassung und zur Gebührenabrechnung. Es sollte vereinbart werden, daß sowohl für Privat- als auch für Dienstgespräche nur die folgenden Gesprächsdaten erfaßt werden:

- Nebenstellennummer
- Zielnummer (mindestens um die letzten drei Ziffern gekürzt)
- Datum
- Gesprächsende
- Verbindungsdauer
- Gebühreneinheit
- Gesprächskosten.

Keine Gesprächsdatenerfassung darf z. B. für Mitglieder der Personalvertretung oder für Personen, die der ärztlichen Schweigepflicht unterliegen, erfolgen.

Die Behördenleitung darf Gesprächsdaten von Dienstgesprächen nur stichprobenweise oder aus einem konkreten Anlaß kontrollieren. Einblick in die Gesprächsdaten der Privatgespräche darf nur der Betroffene selbst erhalten. Ausschließlich zur eigenen Kontrolle von Gebühren der Privatgespräche sollte es jedem Mitarbeiter möglich sein, eine vollständige Gesprächsdatenerfassung, das heißt mit vollständiger Zielnummer, zu beantragen.

Der Anhang sollte folgende technische Details, die öfter aktualisiert werden müssen, enthalten und somit der bereits erwähnten Dokumentationspflicht genügen:

- Hardware- und Softwarebeschreibung einschließlich Schnittstellenbeschreibung (Standort und Typ aller Anlagenbestandteile, installierte Software, Datenverbindungen und Schnittstellen zum öffentlichen Netz)
- ISDN-Dienste und Nutzungskonzepte (alle aktivierten Telekommunikationsdienste und dazugehörige Nutzungshinweise)
- Auflistung aller verwendeten Endgeräte und deren Verteilung
- Verzeichnis aller freigegebenen Leistungsmerkmale für Teilnehmer und Vermittlung
- Regelung aller Wartungsaktivitäten (Zugangsberechtigte, Wartungssoftware, Zugriffsberechtigungen, Sicherungsmaßnahmen, Datensicherungsregelungen)
- Art und Umfang der Protokollierung von Administrationsaktivitäten
- Umgang mit Revisionsunterlagen.

Über den Inhalt der Dienstanweisung müssen alle Mitarbeiter in geeigneter Weise informiert werden. Es hat sich bewährt, allen Mitarbeitern die verfügbaren Funktionen in einer kurzen Übersicht zu erläutern und insbesondere auf die verschiedenen Signalisierungstöne hinzuweisen.

2.18.2. Elektronische Mitteilungssysteme - e-mail um jeden Preis?

Es gibt zahlreiche Bestrebungen, die Kommunikation innerhalb oder zwischen den Behörden durch elektronische Mitteilungssysteme zu unterstützen. Der wohl am meisten genutzte Dienst solcher Bürokommunikationssysteme ist Electronic Mail (e-mail). Hierüber wird elektronische Post zwischen verschiedenen, beliebig weit voneinander entfernten Rechnern ausgetauscht. Es ist damit zu rechnen, daß in Zukunft immer mehr rechtsverbindliche Informationen und insbesondere personenbezogene Daten auf diesem Wege übermittelt werden. Als Übertragungswege werden in der Regel öffentliche (Telefon-) Leitungen benutzt. Diese Leitungen sind von den Kommunikationspartnern nicht kontrollierbar, so daß Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit der übermittelten Daten bedroht sein können. Nur durch eine Vielzahl umfassender, aufeinander abgestimmter Sicherheitsmaßnahmen ist der Schutz elektronisch gespeicherter, bearbeiteter und übermittelter Daten möglich.

Die Innenministerkonferenz hat im Sommer 1993 beschlossen, ab Anfang 1995 ein elektronisches Mitteilungssystem für den Datenaustausch zwischen Bund und Ländern einzusetzen. Im Rahmen des Informationsverbundes Berlin-Bonn (IVBB) sollen ebenfalls solche Systeme verwendet werden.

Auch in Behörden Mecklenburg-Vorpommerns kommen elektronische Mitteilungssysteme als Basis für Bürokommunikationverfahren zum Einsatz. Das Landesweite Polizei Informationssystem (siehe Punkt 2.17.2) verfügt schon über entsprechende Komponenten. Zur Zeit wird der IT-Strukturrahmen, der verbindliche Festlegungen für alle Landesbehörden Mecklenburg-Vorpommerns hinsichtlich der Planung, der Beschaffung und des Betriebes informationstechnischer Systeme und Verfahren enthält, unter anderem um den Abschnitt Bürokommunikation ergänzt. Ich habe den Entwurf dieses Abschnittes dahingehend überprüft, ob er den datenschutzrechtlichen Anforderungen entspricht und im Ergebnis auf die notwendigen Sicherheits-

anforderungen beim Einsatz elektronischer Mitteilungssysteme hingewiesen und entsprechende Empfehlungen gegeben:

· Authentizität von Benutzern, Nachrichten und Systemmeldungen
Für den Empfänger einer Nachricht muß jederzeit die Möglichkeit bestehen, anhand bestimmter Kriterien die Authentizität des Absenders, der Nachricht sowie der an ihn gerichteten Systemmeldungen (zum Beispiel Empfangs- und Weiterleitungsbestätigungen, Sendeanforderungen, Teilnehmerkennungen, Teilnehmereinstufungen) zu überprüfen.

· Vertraulichkeit von übertragenen Daten
Für alle Arten von Daten in elektronischen Mitteilungssystemen - Nachrichten sowie Verkehrs- und Verbindungsdaten - muß die Vertraulichkeit gewahrt bleiben. Sie ist durch geeignete Maßnahmen, etwa kryptografische Verfahren, sicherzustellen.

· Integrität von Nachrichten und Meldungen
Es ist zu gewährleisten, daß bei Speicherung und Weiterleitung von Daten keine unbefugte, unerkannte Veränderung vorgenommen werden kann.

· Fälschungssichere Kommunikationsnachweise
Die für die Anerkennung einer elektronischen Kommunikation erforderlichen fälschungssicheren Sende-, Empfangs- und Übertragungsnachweise müssen dem Anwender auf Wunsch zur Verfügung stehen.

· Verhindern der Bildung von Kommunikationsprofilen
Die Erstellung von Kommunikationsprofilen ist zu verhindern. Gespeicherte Protokollierungsdaten dürfen nur zu Zwecken des Datenschutzes und der Datensicherung verwendet werden.

Es empfielt sich, nur Produkte einzusetzen, die alle Sicherheitsfunktionen der X.400-Empfehlung aus dem Jahre 1988 beinhalten, einem international anerkannten Standard für Verfahren der "elektronischen Post".

Bei der Übertragung von personenbezogenen Daten ist eine Verschlüsselung vorzusehen, die auf einem hinreichend sicheren Verfahren basiert. Dabei muß insbesondere eine ordnungsgemäße Schlüsselerzeugung, -verwaltung und -verteilung gewährleistet sein. Verschlüsselungskomponenten sind durch technische, bauliche und organisatorische Maßnahmen vor dem Zugriff Unbefugter zu schützen.

Zur Absicherung der Integrität der Daten sind Verfahren der "elektronischen Unterschrift" zu verwenden (siehe Punkt 2.16.4), die ebenfalls auf kryptografischen Verfahren beruhen.

Die Funktion des Systemverwalters sollte von der des Verwalters des elektronischen Mitteilungssystems getrennt werden. Es ist grundsätzlich separat administrierbare Hard- oder Software - zum Beispiel in Form eines Kommunikationsservers - für das elektronische Mitteilungssystem vorzusehen.

Bei Verwendung von öffentlichen Übertragungswegen sind die vorhandenen Sicherheitsmechanismen dieser Netze, wie geschlossene Benutzergruppen, Rufnummernidentifikation und automatische Rückruffunktion zu nutzen.

Die eingesetzte Software sollte Funktionen zur Beweissicherung einer stattgefundenen Kommunikation beinhalten (zum Beispiel Zustellungs- und Empfangsnachweis).

Die 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung auf die Risiken bei der Nutzung elektronischer Mitteilungssysteme hingewiesen und entsprechende Empfehlungen formuliert (siehe Anlage 15).

2.18.3. Internet - Gefahr und Nutzen für öffentliche Stellen

Auch in den öffentlichen Stellen unseres Landes wächst das Bedürfnis nach Zugang zu internationalen Kommunikationsdiensten, wie dem weltumspannenden Datennetz Internet. Die damit verbundenen Risiken für den Schutz personenbezogener Daten werden dabei bisweilen weit unterschätzt.

Bei der Entwicklung des Internet haben Datenschutz- und Datensicherheitsaspekte kaum eine Rolle gespielt. Schutzmechanismen müssen daher vielfach nachgerüstet werden. Ständig werden Fehler in Protokollen oder Softwarekomponenten gefunden, deren Ausnutzung das unbefugte Eindringen in fremde Netze und Rechner ermöglicht. Medienmeldungen aus aller Welt, in denen von erfolgreichen Eindringversuchen aus dem Internet in angeblich ausreichend gesicherte Netze oder in einzelne Rechner selbst in Hochsicherheitsbereichen berichtet wird, verdeutlichen die Gefahren für Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch gespeicherten Daten.

Aus datenschutzrechtlicher Sicht ist der Anschluß einer öffentlichen Stelle an das Internet deshalb nur vertretbar, wenn

- ein nachweisbarer Kommunikationsbedarf mit Internet-Teilnehmern besteht,
- der Schutzbedarf festgestellt sowie die sich aus dem Anschluß ergebenen Risiken eingehend analysiert wurden und
- Schutzmaßnahmen ergriffen werden, die diese Risiken soweit reduzieren, daß Gefährdungen für personenbezogene Daten weitgehend ausgeschlossen werden.

Diese Anforderungen sind oft nur schwer zu erfüllen, weil allein schon aufgrund der großen Zahl von Internet-Teilnehmern auch die Gefahr des potentiellen Mißbrauchs sehr groß ist.

Wenn das Restrisiko jedoch unvertretbar hoch bleibt, sollte ein Netzwerk nicht an das Internet angebunden werden. Der Zugriff auf Internet-Dienste ist in diesem Fall auf nicht vernetzte Personalcomputer zu beschränken, auf denen keine sensiblen Daten verarbeitet werden.

Ist der Anschluß des Netzes einer öffentlichen Stelle an das Internet trotz der bekannten Risiken unbedingt erforderlich, empfehle ich, zumindest die nachfolgenden Hinweise zu berücksichtigen.

Analyse des Kommunikationsbedarfs

Für jeden Benutzer des lokalen Netzes ist festzustellen, welche Dienste des Internet genutzt und welche dem Internet angeboten werden sollen. Wird bei der Analyse des Kommunikationsbedarfes festgestellt, daß die Anbindung an das Internet notwendig ist, muß der Schutzbedarf aller im lokalen Netz zu verarbeitenden Daten bestimmt werden.

Feststellung des Schutzbedarfes und Bewertung der Risiken

In Anlehnung an die Empfehlungen des BSI-Grundschutzhandbuches sind folgende Fragen zu beantworten:

- Welche Datenpakete dürfen auf der Grundlage welchen Protokolls bis zu welchem Rechner im Netz weitergeleitet werden?
- Welche Informationen sollen nicht nach außen gelangen?
- Wie können die interne Netzstruktur und Benutzernamen nach außen unsichtbar gemacht werden?
- Welche Authentisierungsverfahren sollen benutzt werden; sind benutzerspezifische Authentisierungsverfahren notwendig?
- Welche Zugänge werden benötigt (zum Beispiel nur über einen Internet-Service-Provider)?
- Welche Datenmengen werden voraussichtlich übertragen?
- Welche Rechner mit welchen Daten befinden sich im Netz, die geschützt werden müssen?
- Welche Nutzer gibt es im Netz, und welche Dienste sollen dem einzelnen Nutzer zur Verfügung gestellt werden?
- Welche Aktivitäten im Netz sind zu protokollieren?
- Welche Dienste dürfen auf keinen Fall genutzt werden?
- Wird sichergestellt, daß nur die Dienste genutzt werden können, die ausdrücklich freigegeben worden sind? (Was nicht erlaubt ist, ist verboten.)
- Welcher Schaden kann im zu schützenden Netz verursacht werden, wenn Unberechtigte Zugang erhalten?
- Welche Restrisiken verbleiben, nachdem die vorgesehenen Schutzmaßnahmen realisiert wurden?
- Welche Einschränkungen würden Benutzer durch den Einsatz geeigneter Schutzmaßnahmen akzeptieren?

Die jeweiligen Stellen sollten zunächst versuchen, genaue Kenntnisse über die Möglichkeiten und Gefährdungen der einzelnen angebotenen Dienste zu erlangen (etwa durch entsprechende Tests mit an das Internet angeschlossenen Einzelplatz-PC). Im Rahmen der empfohlenen Kommunikationsanalyse kann dann leichter beurteilt werden, welcher Nutzer welche Dienste an welchem Rechner tatsächlich benötigt.

Nachdem die Kommunikationserfordernisse analysiert und der Schutzbedarf festgestellt wurden, ist ein Sicherheitskonzept zu erarbeiten, das Bestandteil der gesamten Sicherheits- und Datenschutzpolitik der öffentlichen Stelle werden muß.

Realisierung von Schutzmaßnahmen

Ein geeignetes Mittel, um die durch eine Internetanbindung hervorgerufenen Sicherheitsrisiken zu reduzieren, ist der Einsatz einer Firewall ("Brandschutzmauer"). Eine Firewall ist eine Schwelle zwischen zwei Netzen, die überwunden werden muß, um in Systeme im jeweils anderen Netz einzudringen. So soll erreicht werden, daß nur zugelassene netzübergreifende Aktivitäten möglich sind und Mißbrauchsversuche rechtzeitig erkannt werden.

Eine Firewall läßt sich durch verschiedene Konzepte realisieren. Im wesentlichen unterscheidet man die Grundkonzepte Packet Filter und Application Gateway.

Ein Packet Filter ist ein als Router bezeichneter Rechner, der Datenpakete nach erlaubter und unerlaubter Nutzung von Kommunikationsdiensten filtert. Damit läßt sich einschränken, welche Rechner an der Kommunikation beteiligt sein dürfen und welche Kommunikationsdienste erlaubt sind. Das gilt sowohl für das zu schützende Behördennetz als auch für das unsichere Netz (zum Beispiel Internet).

Ein Application Gateway ist ein speziell konfigurierter Rechner, über den die gesamte Kommunikation zwischen dem zu schützenden und dem unsicheren Netz stattfindet. Mit dem Application Gateway findet die Kontrolle der Kommunikationsbeziehungen, anders als beim Packet Filter, auf der Anwendungsebene statt. Hierbei besteht zum Beispiel die Möglichkeit, ausführliche Protokolle zu führen und eine benutzerbezogene Authentisierung für die unterschiedlichen Dienste durchzuführen.

Firewalls können an verschiedenen Stellen des zu schützenden Netzes installiert werden. Aus Sicherheitsgründen empfiehlt es sich, für das entsprechende Netz nur einen zentralen Internet-Zugang einzurichten und diesen Zugang dann durch eine Firewall zu schützen. Werden innerhalb des Netzes keine weiteren Schutzmechanismen installiert, spricht man von einer zentralen Firewall. Ein Nachteil dieser Lösung ist, daß einzelne Teile des Netzes nicht differenziert nach dem möglicherweise unterschiedlichen Sicherheitsniveau geschützt werden können, so daß sich die Stärke der Firewall am schutzbedürftigsten Teil des Netzes orientieren muß. Ein weiterer Nachteil ist die komplizierte Benutzerverwaltung, da sie in diesem Fall fernab von den einzelnen Fachbereichen zentral erfolgen muß.

Eine aus datenschutzrechtlicher Sicht empfehlenswerte Lösung sind gestaffelte Firewalls. Es handelt sich dabei um eine Kombination aus zentralen und dezentralen Komponenten. Durch eine zentrale Firewall wird ein Mindestschutz für das Gesamtnetz gegenüber dem Internet realisiert. Dezentrale Firewalls in den Teilnetzen mit besonderem Schutzbedarf stellen dort das erforderliche Schutzniveau sicher. Die schon genannten Nachteile einer zentralen Firewall werden vermieden. Darüber hinaus ist mit dieser Lösung auch eine Kontrolle der verwaltungsinternen Verbindungen möglich. Da die Forderungen einzelner Nutzer besser abgebildet werden können, wird auch die Gefahr unkontrollierter (und damit sicherheitsgefährdender) Internet-Zugänge reduziert. Die Anbindung des Gesamtnetzes sollte aber auch in diesem Fall nur über ein zentrales Gateway erfolgen, das durch die zentrale Firewall geschützt wird.

Für alle Arten von Firewalls gilt, daß der personelle und sachliche Aufwand hoch ist. Es ist unverzichtbar, hochspezialisierte Fachleute einzusetzen, um gegen mindestens ebenso spezialisierte Angreifer gewappnet zu sein. Dieser Aufwand ist jedoch immer dann gerechtfertigt, wenn in den an das Internet anzuschließenden Netzen personenbezogene Daten verarbeitet werden.

Die bereits dargestellten Restrisiken können nur anwendungsbezogen aufgefangen werden. So bleibt es auch beim Einsatz von Firewalls notwendig, sensible Daten nur verschlüsselt zu übertragen. Das betrifft neben personenbezogenen Daten auch Paßwörter und sonstige Authentifikationsdaten.

Die Datenschutzbeauftragten haben im Arbeitskreis "Technische und organisatorische Datenschutzfragen" (AK Technik) eine Orientierungshilfe zu diesem Thema erarbeitet (siehe auch Abschnitt 2.21), in der Sicherheitsrisiken dargestellt, Firewallkonzepte erläutert und Empfehlungen zum Schutz gegeben werden. Die Orientierungshilfe ist in meiner Dienststelle kostenlos erhältlich.

2.18.4. Mecklenburg-Vorpommern auf der Datenautobahn

Seit November 1995 "fährt" Mecklenburg-Vorpommern auf der Datenautobahn MVonline (Arbeitstitel), einem multimediafähigen, digitalen Netzwerk, das von den Medien als "Deutschlands erstes offenes, staatliches Regional-Informationsnetz" betitelt wurde. MVonline steht allen Bürgern, Unternehmen, Behörden, Vereinen, Schulen und Institutionen zur besseren Information und Kommunikation in Mecklenburg-Vorpommern zur Verfügung und soll die Basis für ein vom Wirtschaftsministerium gefördertes landesinternes Informationssystem sein. Beispielsweise könnten Firmen sich und ihre Produkte in diesem Netz darstellen und Bürger Informationen aus einer Vielzahl von Angeboten abrufen. Das Abschließen eines elektronischen Vertrages, um einen in MVonline angebotenen Urlaubsplatz verbindlich zu buchen, wäre nur eine von vielen denkbaren Nutzungsmöglichkeiten.

Insbesondere beim Angebot kostenpflichtiger Multimedia-Dienste wird deutlich, daß bei deren Nutzung personenbezogene Daten anfallen, die neue datenschutzrechtliche Probleme aufwerfen können.

Multimedia-Dienste stellen eine neue Qualität unter den Telekommunikationsdiensten dar. Bisher bestand nur die Möglichkeit, Informationen für eine nicht bestimmbare Anzahl von Nutzern bereitzustellen (Fernsehen, Zeitungen, Kataloge usw.). Die Inanspruchnahme solcher Angebote war kaum kontrollierbar. Müssen Nutzer nun für die Inanspruchnahme bestimmter Informationsangebote Gebühren entrichten, oder muß ein rechtsverbindlicher Nachweis für einen unter Nutzung dieser Dienste abgeschlossenen Vertrag erbracht werden, fallen personenbezogene Daten an. Durch die Speicherung dieser Daten könnte das Konsum- und Medienverhalten des einzelnen in bisher nicht bekanntem Maße kontrolliert werden. Es würden beispielsweise detaillierte Informationen darüber vorliegen, wann welcher Zeitungsartikel abgerufen oder welche Ware auf elektronischem Wege gekauft wurde.

Daher ist eine datenschutzgerechte Gestaltung von Abrechnungsverfahren unabdingbar. Im Interesse des Kunden, der Multimedia-Dienste in Anspruch nimmt, sollten solche Abrechnungsverfahren entwickelt werden, die einen anonymen Zugang zu Dienstleistungsangeboten unter Wahrung der Abrechnungssicherheit gewährleisten. Nach dem heutigen Stand der Technik kommen dafür vor allem die sogenannten Prepaid-Verfahren in Frage. Bei ihnen erfolgt eine Zahlung im voraus. Die Verwendung von Chipkarten, auf denen ein Guthaben gespeichert werden kann, bietet sich dafür an. Auf eine zentrale Speicherung von Verbindungs- und Nutzungsdaten kann auf diese Weise weitgehend verzichtet werden. Es werden also keine personenbezogene Daten gespeichert, die für die Inanspruchnahme einer Netzdienstleistung nicht erforderlich sind.

Falls es in besonderen Fällen unumgänglich ist, die Identität des Nutzers zu offenbaren, darf die Speicherung seiner personenbezogenen Daten nur in dem unbedingt notwendigen Umfang und nicht länger als erforderlich erfolgen. Eine strenge Zweckbindung ist zu gewährleisten.

Multimedia-Dienste werden besonders dann interessant, wenn Zugang zu internationalen Angeboten besteht. Das Internet bietet eine Vielzahl entsprechender Dienste, und fast jeder Dienstanbieter stellt eine Einwahlmöglichkeit zur Verfügung. Auch MVonline hat diesen Service. Neben den im Punkt 2.18.3 beschriebenen Sicherheitsproblemen spielt auch die landesspezifische Datenschutzgesetzgebung eine wichtige Rolle. Es muß sichergestellt sein, daß Anbieter von Multimedia-Diensten nicht die in ihrem Land geltenden Datenschutzregelungen umgehen, indem sie sich in Ländern ohne entsprechende Schutzgesetze oder mit Regelungen auf niedrigerem Niveau niederlassen. Hier ist die EU gefordert, die Harmonisierung der Gesetzgebung voranzutreiben.

Werden in Multimedia-Netzen Presseerzeugnisse angeboten - die Schweriner Volkszeitung ist beispielsweise weltweit im Internet zu lesen - und stehen elektronische Pressearchive zur Verfügung, wird es ein Vergessen von Informationen nicht mehr geben. Wie die Wahrung von Rechten Betroffener, etwa der Anspruch auf Gegendarstellung, in ausreichendem Maß sichergestellt werden kann, ist noch vollkommen offen.

2.19. Neue Techniken

2.19.1. Doch kein "Gläserner Autofahrer"

Im Herbst 1993 erhielt ich von Mitarbeitern verschiedener Firmen erste Informationen über die vom Bundesverkehrsminister geplante Einführung von Systemen zur automatischen Gebührenerhebung auf Autobahnen (AGE). Sie boten an, die noch in der Entwicklung befindlichen Systeme den Datenschutzbeauftragten im Rahmen des Arbeitskreises "Technische und organisatorische Datenschutzfragen" zur Erörterung datenschutzrechtlicher Fragen vorzustellen.

Die Präsentation eines AGE-Systems, zu der ich im Januar 1994 Firmenvertreter und Kollegen nach Schwerin eingeladen hatte, machte deutlich, daß Anforderungen des Datenschutzes bei der weiteren Entwicklung eine entscheidende Rolle spielen werden. Ohne ausreichende Berücksichtigung datenschutzrechtlicher Vorgaben besteht die Gefahr, daß wesentlich mehr personenbezogene Daten mit einem solchen System verarbeitet werden, als für den eigentlichen Zweck erforderlich sind.

Ein im Auftrag des Bundesverkehrsministeriums und unter Federführung des TÜV Rheinland durchgeführter Feldversuch auf der A555 zwischen Köln und Bonn gab ausgewählten Anbietern von AGE-Systemen die Möglichkeit, ihre technischen Lösungen und Einsatzkonzepte zu testen. Die Datenschutzbeauftragten nutzten das Angebot des Bundesverkehrsministeriums und des TÜV Rheinland, sich während des Feldversuches einen ersten Überblick über alle im Test befindlichen Systeme zu verschaffen.

Der BfD formulierte erste Anforderungen für die datenschutzgerechte Ausgestaltung von AGE-Systemen und der AK Technik wurde beauftragt, alle im Rahmen des Feldversuches getesteten Lösungen dahingehend zu prüfen, inwieweit sie in ihren technischen Details geeignet sind, diese Anforderungen zu erfüllen.

Der AK Technik arbeitete die im folgenden erläuterten Bewertungskriterien aus. Sie sollten eine einheitliche Beurteilung der verschiedenen Projekte ermöglichen.

· Anonymität
Der Grundsatz der "datenfreien Fahrt" muß gewährleistet bleiben. Deshalb ist die Erhebung von Daten auf das für die Gebührenerhebung notwendige Minimum zu reduzieren. Bewegungsdaten sollten nur beim Benutzer der Autobahn gespeichert werden. Zahlung und Abrechnung von Benutzungsentgelten müssen anonym erfolgen. Die Aufdeckung der Identität eines Benutzers darf nur bei begründetem Mißbrauchsverdacht erfolgen.

· Vertraulichkeit
Werden personenbezogene Daten erhoben, so sind sie vertraulich zu behandeln. Durch entsprechende technisch-organisatorische Maßnahmen ist zu gewährleisten, daß die Daten sowohl gegen Mißbrauchsversuche Externer (etwa Hacker) als auch Interner (etwa Mitarbeiter von Betreibergesellschaften) geschützt werden.

· Integrität
Auch unter schwierigen Bedingungen (schlechtes Wetter, schnelle Spurwechsel) muß gewährleistet sein, daß die richtigen Daten jeweils den richtigen Benutzern zugeordnet werden. Die Berechnung muß fehlerfrei und manipulationssicher sein.

· Transparenz
Das gesamte Verfahren muß für den Benutzer transparent sein. Dazu gehört, daß Anzeigen und Belege für erfolgte Abbuchungen verfügbar sind und rechtzeitig auf ein zu geringes Guthaben hingewiesen wird. Die Aufdeckung seiner Identität bei einer Kontrolle (etwa beim Falschzahler) muß für den Benutzer erkennbar sein. Funktionsstörungen von Hard- und Software müssen ihm angezeigt werden. Eine klare Trennung von Zahlungs- und Nutzungsdaten ist erforderlich.

· Rücknahmefestigkeit
Systemkomponenten sind so zu gestalten, daß die Datenschutz- und Datensicherungsfunktionen nicht einseitig durch den Systembetreiber oder durch Dritte zurückgenommen oder unterlaufen werden können.

Im Januar 1995 veranstaltete der AK Technik gemeinsam mit dem Berliner Datenschutzbeauftragten einen Workshop, zu dem ich neben den Datenschutzbeauftragten des Bundes und der Länder alle Teilnehmer des Feldversuches und Vertreter aus Wissenschaft und Forschung eingeladen hatte. Die Datenschutzbeauftragten konnten sich detailliert über die verschiedenen Projekte informieren und frühzeitig Empfehlungen für eine datenschutzgerechte Gestaltung der Technik, der Organisation und der rechtlichen Rahmenbedingungen unterbreiten. Die Anbieter von AGE-Systemen hatten so die Möglichkeit, datenschutzrechtliche Forderungen noch rechtzeitig bei der Systementwicklung zu berücksichtigen. Jeder Anbieter stellte im Rahmen der Präsentation sein Projekt ausführlich unter besonderer Berücksichtigung der oben genannten Bewertungskriterien vor und erörterte gemeinsam mit allen Teilnehmern Vor- und Nachteile seines Verfahrens.

Im AK Technik wurde der Workshop ausgewertet. Der BfD faßte die Ergebnisse zusammen und übermittelte sie in Form eines Anforderungskataloges dem Bundesverkehrsministerium. Nach dem derzeitigen Stand der Technik können die dort genannten Anforderungen nur von Systemen erfüllt werden, bei denen die Entrichtung von Gebühren im voraus erfolgt, beispielsweise mit einer Chipkarte als Guthabenkarte.

Die 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder verabschiedete im März 1995 eine Entschließung, in der auf die Gefahren beim Betrieb von Systemen zur automatischen Erhebung von Straßennutzungsgebühren hingewiesen wird (siehe Anlage 16).

Im November 1995 beendete der TÜV Rheinland die Auswertung des Feldversuches auf der A 555. In seinem Abschlußbericht kommt er zu dem Ergebnis, daß insbesondere die Anforderungen an die Anonymisierung, die Trennung von Zahlungs- und Nutzungsdaten sowie die Transparenz der Erhebungs- und Kontrollvorgänge von im Feldversuch vorgestellten Systemen nicht vollständig erfüllt sind. Keines der vorgestellten Kontrollverfahren war in der Lage, die Anforderungen des Datenschutzes zu erfüllen.

Im November 1995 war Medienmeldungen zu entnehmen, daß die Bundesregierung die Pläne aufgegeben hat, eine Autobahngebühr für Personenkraftwagen einzuführen.

2.19.2. Satellitentechnik

Der AK Technik hat untersucht, welche Überwachungsmöglichkeiten durch die Auswertung der Aufnahmen von Satelliten bestehen.

Hauptanwendungsgebiet der Satellitentechnik ist zur Zeit die Landwirtschaft. Im Integrierten Verwaltungs- und Kontrollsystem (siehe Abschnitt 2.15) wird sie zur Datenerhebung verwendet. In anderen Verfahren werden die Daten der hochauflösenden Erderkundungssatelliten Landsat (USA) und SPOT (Frankreich) sowie vom Wettersatelliten NOAA (USA) genutzt.

Ziel ist die Entwicklung von Verfahren, die eine möglichst genaue Erfassung der landwirtschaftlichen Nutzflächen, deren Eigenschaften sowie eine frühzeitige Ertragsprognose ermöglichen. Dazu führt die EU ein Programm zum Einsatz der Fernerkundung in der Agrarstatistik durch. In einzelnen sogenannten operationellen Aktionen werden Teilgebiete bearbeitet, deren Ergebnisse zum Schluß in die EU-Agrarstatistik Eingang finden sollen.

Die regionale Flächenerfassung wird hauptsächlich in den südeuropäischen Ländern durchgeführt, weil es in Nordeuropa wegen der Wetterbedingungen schwierig ist, genügend große Flächen gleichzeitig zu erfassen.

Für eine Ertragsschnellschätzung werden von 50 repräsentativen Flächen der EU-Länder im Laufe des Jahres 3-4 Aufnahmen gemacht und ausgewertet. Eine Überwachung und Vorausschätzung der Ernten auch außerhalb der EU wird angestrebt. Zur Bestimmung der Fläche und der Anbauart werden vorzugsweise Bilder vom SPOT verwendet.

In Entwicklung befindet sich ein System, in dem unter Einbeziehung der Daten vom NOAA und von Daten europäischer Wetterstationen Vegetations- und Bodentemperaturindizes sowie Ertragsschätzungsmodelle erstellt werden. Alle Informationen sollen in ein Informationssystem auf Gemeinschaftsebene einfließen.

Zur Verbesserung der Ergebnisse wird die Entwicklung und Anwendung neuer Verfahren und Sensoren vorangetrieben. Vielversprechend ist der Einsatz der Radarsatelliten (ERS-1 und -2), weil deren Bilder wetterunabhängig sind.

Vor allem aus technischen Gründen sind die Überwachungsmöglichkeiten begrenzt. So ist beispielsweise die Beobachtung eines Punktes auf der Erde nicht ohne weiteres möglich. Die erforderliche Apparatur würde zu groß und zu schwer, um sie auf eine geostationäre Bahn von 36.000 km Entfernung zu befördern. Umlaufende Satelliten liefern Informationen nur in bestimmtem Zeitabständen und bei guten Wettervoraussetzungen. Bereits archivierte Daten werden nur zufällig von einem genau bestimmten Ort zu einer bestimmten Zeit vorhanden sein, so daß eine systematische Auswertung nicht erfolgversprechend ist. Es können allerdings in einem gewissen Rahmen zu bestimmten Zeitpunkten Aufnahmen eines Punktes der Erdoberfläche gemacht werden. Die angebotene Auflösung beträgt zur Zeit im zivilen Bereich allerdings bestenfalls einen Meter Kantenlänge pro Bildpunkt.

Die Untersuchungen des AK Technik haben deutlich gemacht, daß sich die Satellitentechnik auch in absehbarer Zukunft nicht direkt zu einem Überwachungspotential für den einzelnen entwickeln wird. Allein mit Ergebnissen der Satellitenfernerkundung ist keine Beobachtung oder Überwachung möglich. Erst durch die Zusammenführung mit anderen Daten ist in manchen Fällen ein Personenbezug herzustellen.

2.19.3. Chipkarte

Datenschützer begleiten die Entwicklung der Chipkarte seit ihrer Einführung aufmerksam und mit Sorge. So gab es beispielsweise bereits ernstzunehmende Hinweise darauf, daß die inzwischen bundesweit eingeführte Krankenversichertenkarte relativ leicht zu fälschen ist.

Stand der Technik ist heute die Prozessor-Chipkarte. Sie verfügt durch einen integrierten Prozessor über eigene Rechenleistung. Im Gegensatz zur Magnetstreifenkarte ist dadurch die gegenseitige Authentifikation von Karte und dazugehörigem Lesegerät möglich. Unbefugte Manipulationen können somit erheblich erschwert werden. Nur nach korrekter Eingabe einer PIN (Persönliche Identifikations-Nummer) ist ein Zugriff auf die Karte möglich. Bei Manipulationsversuchen oder falscher PIN-Eingabe könnte sich die Karte selbst unbrauchbar machen. Der Umgang mit einer PIN ist jedoch problematisch, da sich kaum jemand die Vielzahl der PIN und Paßworte merken kann, die heute im täglichen Leben benötigt werden. Deshalb werden diese meist irgendwo notiert, und es besteht die Gefahr des Verlustes von PIN und Karte.

Ein Ausweg könnte die Multifunktionskarte sein. Schon heute reicht der Speicherbereich der Chipkarten aus, um mehrere verschiedene Anwendungen zu integrieren. So lassen sich die Anwendungen Geldkarte, Telefonkarte, Gesundheitskarte und Betriebsausweis durchaus auf einer Karte zusammenfassen. Daraus ergeben sich jedoch Probleme hinsichtlich der Abgrenzung der einzelnen Anwendungen. Deshalb sollten zunächst nur Multifunktionskarten mit artverwandten Anwendungen, wie beispielsweise Kleingeldbörse, Telefonkarte oder Chipkarte als Zahlungsmittel im öffentlichen Nahverkehr, zum Einsatz kommen.

Die besondere Aufmerksamkeit der Datenschützer gilt Kartenanwendungen, auf denen so sensible Daten gespeichert werden sollen, wie es bei verschiedenen freiwilligen Gesundheitskarten geplant ist. Die Speicherung des gesamten medizinischen Lebenslaufes mit allen Gesundheitsdaten, Krankheiten, Diagnosen, Therapien und Verschreibungen sowie Notfalldaten auf der Karte wäre beispielsweise möglich.

Unklar wäre dann, wem der Kartenbesitzer diese Daten offenbaren muß. Muß jeder Arzt, von dem er einen unvoreingenommenen Rat einholen möchte, alle Daten kennen? Kann der Bewerber um eine Arbeitsstelle dem Arbeitgeber vor der Einstellung den Einblick in die Gesundheitsdaten verwehren, ohne seine Chancen auf diese Stelle zunichte zu machen? Es zeichnet sich ab, daß hier im Interesse des Bürgers noch ein erheblicher Regelungsbedarf besteht.

Die Konferenz der Datenschutzbeauftragten hat zum Thema „Chipkarten im Gesundheitswesen“ zwei Entschließungen verabschiedet (siehe Anlagen 1 und 24).

2.19.4. Patientendaten - optisch speichern?

Einige Krankenhäuser und öffentliche Stellen des Gesundheitsdienstes wollen ihr bisheriges Archivierungssystem umstellen. Dabei soll unter anderem aus Platzmangel auf die Aufbewahrung von Schriftstücken möglichst ganz verzichtet werden. Daher stellte sich die Frage, ob zum Speichern von Patientendaten optische Datenspeicher geeignet sind und verwendet werden dürfen.

Weder das Landesdatenschutzgesetz noch die datenschutzrechtlichen Bestimmungen in den bereichsspezifischen Gesetzen schreiben bestimmte Speichertechnologien vor oder schließen die Anwendung bestimmter Technologien aus. Allerdings sind Verarbeitungsfunktionen wie Sperren, Anonymisieren und Löschen bei jeder automatisierten Datenverarbeitung zu realisieren. Deshalb ist grundsätzlich zu prüfen, ob diese Funktionen gewährleistet sind, bevor man sich für eine bestimmte Speichertechnologie entscheidet. Bei der Speicherung von Patientendaten auf optischen Datenträgern ist insbesondere zu beachten, daß sich die Sperr- und Löschvorschriften des LKHG M-V realisieren lassen (§ 19 LKHG M-V).

Der Begriff der „optischen Datenspeicherung“ ist abgeleitet vom zugrunde liegenden Aufzeichnungsverfahren mit Hilfe eines Laserstrahls. Man unterscheidet zwischen Datenträgern, die nur einmal beschreibbar sind, aber beliebig oft gelesen werden können, und solchen, die mehrfach beschreib- und lesbar sind. Zu den nur einmal beschreibbaren Speichern gehören die verschiedenen CD-ähnlichen Datenträger, wie die bekannte CD-ROM, die als Audio-CD sehr verbreitet ist, und die auf dem Markt schon länger verfügbare WORM, die vom Nutzer nur einmal beschrieben, aber beliebig oft gelesen werden kann.

Bei CD-ROM und WORM kann die Löschung von Daten nur durch Löschen von Verweisdaten erfolgen. Diese werden im Datenverwaltungssystem eines separat betriebenen EDV-Systems vorgehalten, das den Zugriff zu den Nutzdaten steuert. Im Datenverwaltungssystem sind nach diesem Löschvorgang die alten Verweise auf die zu löschende Information nicht mehr enthalten (logische Löschung), obwohl die Nutzdaten auf dem optischen Speichersystem physikalisch noch im Volltext vorhanden sind. Dieser logische Löschvorgang genügt nicht den Anforderungen des Datenschutzes. Löschen ist im Landesdatenschutzgesetz als "dauerhaftes Unkenntlichmachen gespeicherter Daten" definiert (§ 3 Abs. 7 Nr. 6 DSG MV). Von einem solchen dauerhaften Unkenntlichmachen kann man aber hier nicht sprechen, weil beispielsweise die Anbieter der CD-ROM- bzw. WORM-Platte und des Laufwerks über das Wissen und die Möglichkeit verfügen, wie man auf derart „logisch“ gelöschte Daten zugreifen kann.

Die datenschutzgerechte Löschung von Daten auf einmal beschreibbaren optischen Speichern läßt sich somit nur erreichen, indem nach dem Löschen des entsprechenden Eintrags in der Verweisdatei die übrigen Daten vom alten Träger auf eine neue optische Speicherplatte kopiert werden und danach der alte Datenträger physisch zerstört wird. Auch die Berichtigung falsch gespeicherter Daten kann nur auf diese oder vergleichbare Art und Weise erfolgen.

Seit kurzem gibt es jedoch Alternativen zu den nur einmal beschreibbaren optischen Datenspeichern. Ein Beispiel hierfür ist die ROD-MO (Rewritable Optical Disc) als eine Form der magneto-optischen (MO) Disc. Es handelt sich um eine mehrfach wiederbeschreibbare optische Disk. Sie erscheint allerdings aufgrund der Möglichkeit zur Veränderung der Daten für eine gesicherte Langzeitarchivierung nicht geeignet und dürfte eher als Alternative zu herkömmlichen magnetischen Laufwerken anzusehen sein.

Wegen der vielen Anfragen bei den Datenschutzbeauftragten des Bundes und der Länder zu diesem Thema hat der AK Technik unter Federführung des Saarländischen Landesdatenschutzbeauftragten eine Orientierungshilfe erarbeitet, die über den datenschutzgerechten Umgang mit optischen Speichermedien informiert (siehe Abschnitt 2.21). Sie gibt unter anderem konkrete Empfehlungen zu Einsatzmöglichkeiten der verschiedenen Technologien.

Den Krankenhäusern und öffentlichen Stellen des Gesundheitswesens habe ich mitgeteilt, daß aus datenschutzrechtlicher Sicht gegen den Einsatz der WORM-Technologie zur Archivierung von Patientendaten prinzipiell nichts einzuwenden ist, wenn die oben genannten Hinweise beachtet und die im LKHG M-V genannten technisch-organisatorischen Maßnahmen realisiert werden. Da die Anfragen sich häuften, habe ich auch dem Sozialminister meine Empfehlungen zur WORM-Technologie übersandt, damit sie von dort aus bei Beratungen weiteren Bedarfsträgern zur Kenntnis gegeben werden kann.

2.20. Datenverarbeitung im Auftrag

2.20.1. Wie die Treuhand Daten auffrischt

Im März 1995 informierte mich der Kollege eines anderen Bundeslandes darüber, daß in Mecklenburg-Vorpommern ein Pilotversuch zur "Totalerfassung aller Treuhandliegenschaften" durchgeführt wird und die Treuhand Liegenschaftsgesellschaft mbH (TLG) bereits einen Abgleich zwischen Daten des ehemaligen DDR-Liegenschaftskatasters "COLIDO" und den jetzt aktuellen Liegenschaftsdaten vorgenommen hat.

Ein Anruf bei der TLG in Berlin ergab, daß mit einem solchen Pilotprojekt tatsächlich bereits in Greifswald begonnen worden und der Innenminister Mecklenburg-Vorpommerns darüber informiert war. Ziel des Projektes sei es, alle noch im Besitz der Treuhand befindlichen Liegenschaften zu erfassen und Unregelmäßigkeiten bei bereits erfolgten Verkäufen aufzudecken. Der Pilotversuch wäre notwendig, um das Verfahren zu testen, das dann in allen neuen Bundesländern angewendet werden solle.

Der Innenminister bestätigte, daß ein solches Projekt bereits angelaufen sei. Eine Beteiligung des Landesbeauftragten für den Datenschutz gemäß § 29 Abs. 5 DSG MV wäre allerdings erst in der letzten Phase des Pilotprojektes vorgesehen, da vorher nicht mit personenbezogenen Daten umgegangen würde. Trotzdem hat der Innenminister das Pilotprojekt aufgrund meiner Anfrage sofort gestoppt. Auf meine Anforderung hin erhielt ich Anfang April 1995 die ersten detaillierten schriftlichen Informationen zur "Totalerfassung aller Treuhandliegenschaften".

Bei der Durchsicht der Unterlagen stellte sich folgendes heraus:
Die Treuhand hatte zwei Privatfirmen mit der Durchführung des Pilotprojektes beauftragt. Bereits seit Januar 1995 bestanden intensive Kontakte zwischen der TLG, den beauftragten Privatfirmen, dem Innenministerium und dem Kataster- und Vermessungsamt (KVA) der Hansestadt Greifswald. Im Februar 1995 hatte eine der Firmen von sich aus "datenschutzrechtliche Bedenken" gegenüber dem Innenministerium angemeldet. Meine Beteiligung gemäß § 29 Abs. 5 DSG MV wurde zu diesem Zeitpunkt jedoch als nicht notwendig erachtet.

Um mir selbst ein Bild vom Stand des Projektes zu verschaffen, stattete ich Anfang April 1995 dem KVA einen Kontrollbesuch ab. Die Mitarbeiter des KVA bestätigten, daß bereits Ende März 1995 ein Datenabgleich in Greifswald stattgefunden hatte. Dieser Abgleich wurde ohne Wissen des Innenministers und auf Initiative der Firmen durchgeführt, von denen die eine zuvor selbst datenschutzrechtliche Bedenken angemeldet hatte. Während der Kontrolle wurde ich von einem Mitarbeiter des KVA darüber informiert, daß der gesamte Datenbestand der Datenbank mit Eigentümerangaben (Eigentümerdatei) durch eine Hardwarekopplung auf einen Laptop der Privatfirmen überspielt wurde. Zwei Wochen später wurde mir allerdings mitgeteilt, der Datenbestand sei durch Überspielen mit Hilfe von Disketten erfolgt. Aus datenschutzrechtlicher Sicht ist das jedoch von untergeordneter Bedeutung. Entscheidend ist lediglich, daß keine Protokollierung der Datenübermittlung stattgefunden hatte und dadurch im nachhinein der Datentransfer nicht überprüfbar war.

Für die Selektion bestimmter Datensätze wurde ein von einer der Firmen zur Verfügung gestelltes Programm genutzt. Zu diesem Programm existierte keine Dokumentation, und es war weder hinsichtlich seiner Funktionalität von Mitarbeitern des KVA bzw. des Innenministeriums überprüft worden noch existierte eine Freigabe zur Nutzung dieser Software im KVA. Mit der sofort nach der Selektion erfolgten manuellen Überprüfung der Datensätze war angeblich festgestellt worden, daß das Programm ordnungsgemäß gearbeitet hatte. Eine spätere Prüfung der an die TLG übermittelten 2147 Datensätze ergab jedoch, daß tatsächlich 35 Datensätze unrechtmäßig selektiert und übermittelt worden waren, die Software also nicht für den angegebenen Zweck geeignet war.

Aufgrund der bei der Kontrolle festgestellten gravierenden Verstöße gegen das DSG MV habe ich dem Landrat des Landkreises Ostvorpommern eine förmliche Beanstandung gemäß § 28 Abs. 1 Nr. 2 DSG MV ausgesprochen. Insbesondere kritisierte ich die vollkommen unzureichenden technisch-organisatorischen Maßnahmen bei der Übermittlung und Selektion der Daten, die nicht rechtzeitige Information über das Projekt und das Fehlen von Dateibeschreibung und Geräteverzeichnis für die Eigentümerdatei, aus der die übermittelten Daten stammten.

In einer daraufhin veröffentlichten Presseinformation erklärte die TLG, daß wegen datenschutzrechtlicher Bedenken "die ins Auge gefaßte Vorgehensweise sofort verworfen" wird.

Um das Verfahren "Totalerfassung aller Treuhandliegenschaften" datenschutzgerecht auszugestalten, fand im Juni 1995 eine Beratung in Schwerin statt. Ich hatte Vertreter der beteiligten Firmen, der Innenministerien der neuen Länder und Datenschutzbeauftragte des Bundes und der Länder eingeladen.

Die Datenschutzbeauftragten erläuterten ihre Auffassung zu den Rechtsvorschriften, die dem Verfahren zugrunde liegen. Sie gaben Empfehlungen zum datenschutzgerechten Ablauf des Verfahrens und zu erforderlichen vertraglichen Regelungen, die vor Beginn des Pilotprojektes getroffen werden müssen. Da in den beteiligten Bundesländern die Liegenschaftsbücher auf unterschiedliche Art und Weise geführt werden, unterscheidet sich der Umfang dieser Regelungen. In Mecklenburg-Vorpommern wird das Automatisierte Liegenschaftsbuch vom DVZ geführt. Da die umfangreichen Auskunftsersuchen der TLG dort mit vorhandener Recherchesoftware auf der Basis schon existierender Verträge bearbeitet werden können, erübrigt sich eine vertragliche Vereinbarung zwischen dem Innenminister und der TLG. Ich habe jedoch empfohlen, eine Datenschutzvereinbarung zwischen der TLG bzw. der von ihr beauftragten Firmen und dem Innenminister abzuschließen. Darin sollte auch festgelegt werden, wie mit den Daten verfahren wird, die zur Erfüllung der Aufgaben der TLG nicht mehr erforderlich sind. Auch die Aufnahme der Forderung nach Prüfung und Freigabe der im Verfahren verwendeten Software, die von externen Dienstleistern bereitgestellt wird, war notwendig. Weiterhin sollte eine detaillierte Beschreibung der erforderlichen und geeigneten technisch-organisatorischen Maßnahmen in die Datenschutzvereinbarung aufgenommen werden.

Im Juli 1995 informierte mich der Innenminister, daß meine Empfehlungen die Grundlage für den Neubeginn des Pilotprojektes in Greifswald sein werden. Die Datenschutzvereinbarung zwischen den beiden Privatfirmen als Bevollmächtigte der TLG und dem Innenminister wurde unter Berücksichtigung meiner Empfehlungen im Oktober 1995 abgeschlossen.

Im November 1995 waren jedoch immer noch nicht alle Voraussetzungen für den erneuten Start des Pilotprojektes gegeben. Der Innenminister teilte mir mit, daß die Software nunmehr vom Landesvermessungsamt Mecklenburg-Vorpommern geprüft worden sei, aber nicht freigegeben werden könne, da noch immer unzulässige Datensätze selektiert wurden. Darüber hinaus wurden vom Programm durch Verknüpfung verschiedener Daten neue, nicht zulässige Dateien erstellt. Nach der Beseitigung der festgestellten Mängel wurde die Software im Dezember 1995 vom Landesvermessungsamt nach nochmaliger Prüfung zur Nutzung in den Kataster- und Vermessungsämtern freigegeben.

Die im § 16 DSG MV geforderte Dateibeschreibung der Eigentümerdatei des KVA und das entsprechende Geräteverzeichnis, um deren Zusendung ich bereits im Mai 1995 gebeten hatte, liegen mir bis heute nicht vor.

2.20.2. Wahrung des Steuer- und Meldegeheimnisses trotz Outsourcing?

Aus öffentlichen Stellen des kommunalen Bereiches wurde ich darüber informiert, daß sie einen externen Dienstleister mit der Verarbeitung personenbezogener Daten beauftragt haben. In einem Fall werden beispielsweise Lohnsteuerkarten durch eine private Firma kuvertiert und versandfertig vorbereitet. Andere Aufträge betreffen die Betreuung von Hard- und Software einschließlich der Pflege und Sicherung von Datenbeständen des Finanz- und Meldewesens. Ich hatte zu prüfen, ob eine solche Auftragsdatenverarbeitung mit den datenschutzrechtlichen Vorschriften vereinbar ist.

Grundsätzlich läßt § 4 des DSG MV den Umgang mit personenbezogenen Daten im Auftrag zu. Dabei sind jedoch einige Grundsätze zu beachten. Für die Einhaltung der Datenschutzvorschriften und die Kontrolle der technisch-organisatorischen Maßnahmen bleibt der Auftraggeber verantwortlich. Deshalb ist der Auftragnehmer sorgfältig auszuwählen. Die Beauftragung muß schriftlich erfolgen und der Landesbeauftragte für den Datenschutz ist darüber zu informieren. Der Auftragnehmer hat sich der Kontrolle des Landesdatenschutzbeauftragten zu unterwerfen und ist verpflichtet, gemäß § 32 Abs. 1 Nr. 3 BDSG der zuständigen Aufsichtsbehörde die Aufnahme und Beendigung der Auftragsdatenverarbeitung mitzuteilen.

Sollen personenbezogene Daten, die einer besonderen Amtsverschwiegenheit unterliegen, im Auftrag verarbeitet werden, sind auch datenschutzrechtliche Vorschriften anderer Gesetze zu beachten. Mit der Auslagerung der automatisierten Verarbeitung dieser Daten in eine private Firma ist verbunden, daß Arbeitnehmern dieser Firma Daten offenbart werden können, die z. B. dem Steuergeheimnis (§ 30 Abgabenordnung) oder den Vorschriften des Landesmeldegesetzes unterliegen.

Bei der automatisierten Verarbeitung von Einwohnermeldedaten im Auftrag müssen insbesondere die Vorschriften des § 38 Landesmeldegesetz beachtet werden. Den Meldebehörden wird hier das Recht eingeräumt, geeignete privatrechtliche Einrichtungen Mecklenburg-Vorpommerns zu beauftragen. Die Wahrung des Meldegeheimnisses ist vor allem durch die sorgfältige Auswahl von technisch-organisatorischen Maßnahmen sicherzustellen.

Fraglich ist, ob personenbezogene Daten, die dem Steuergeheimnis nach § 30 Abgabenordnung unterliegen, auch von Privaten verarbeitet werden dürfen, da diese Daten eine besondere Sensibilität aufweisen. Im Gegensatz zum Einwohnermeldewesen gibt es keine Vorschrift, welche die automatisierte Verarbeitung von Steuerdaten durch Private ausdrücklich erlaubt oder verbietet.

Nur wenn eine öffentliche Stelle weder fachlich noch personell in der Lage ist, die Aufgaben selbst wahrzunehmen, und kein öffentlicher Auftragnehmer zur Verfügung steht, darf sie Private mit der Verarbeitung von Steuerdaten beauftragen. Dann müssen Sicherungsmaßnahmen in personeller, organisatorischer und technischer Hinsicht vorgesehen werden, die der besonderen Sensibilität der Daten angepaßt und deshalb umfassender als die sonst im Rahmen der Auftragsdatenverarbeitung getroffenen Vorkehrungen sind. Zu den erforderlichen Maßnahmen gehören vor allem eine wirksame Abschottung der Datenbestände beim Auftragnehmer mit differenzierten Zugriffsrechten der Bearbeiter und die förmliche Verpflichtung auf die Einhaltung des Steuergeheimnisses aller beim Auftragnehmer beschäftigten Personen.

2.20.3. "Das sind Daten meiner Kunden!"

Ein kommunaler Zweckverband zur Wasserversorgung und Abwasserbehandlung informierte mich darüber, daß er mit der Inbetriebnahme eines neuen EDV-Systems nunmehr in der Lage sei, die Abrechnung aller Geschäftsvorgänge selbständig durchzuführen. Bisher war eine Firma mit diesen Abrechnungsaufgaben beauftragt und erhielt so die Stammdaten der Geschäftspartner des Zweckverbandes.

Für die selbständige Abrechnung der Geschäftsvorgänge benötigte der Zweckverband nun selbst die Daten seiner Kunden. Um datenschutzrechtliche Vorbehalte des bisherigen Auftragnehmers auszuräumen, wurde ich gebeten, meine Auffassung zur Weitergabe der Stammdaten mitzuteilen. Insbesondere bestanden Bedenken, daß der bisherige Auftragnehmer nicht in der Lage sein könnte, die Kundendaten seiner verschiedenen Auftraggeber vor der Datenweitergabe voneinander zu trennen.

Der Zweckverband hat als Auftraggeber gemäß § 4 DSG MV das Recht, den Auftragnehmer anzuweisen, seine Kundendaten zurückzugeben. Die Übermittlung der Kundendaten anderer Auftraggeber an den Zweckverband ist jedoch unzulässig. Der Auftragnehmer ist darüber hinaus verpflichtet, bei Beendigung des Auftragsverhältnisses die dann noch bei ihm befindlichen Daten des Auftraggebers zu löschen (§ 11 Abs. 2 Nr. 4 DSG MV).

Meine Nachfrage beim Auftragnehmer ergab, daß die Vorschriften des DSG MV im Rahmen der Datenverarbeitung im Auftrag des Zweckverbandes beachtet worden waren. Die Weitergabe der separierten Kundendaten des Zweckverbandes war ohne weiteres möglich.

Der kommunale Zweckverband erhielt nur die Daten seiner Kunden. Lediglich für einen Übergangszeitraum, dessen Dauer mit dem Zweckverband vereinbart wurde, blieben die Daten noch beim Auftragnehmer gespeichert.

2.21. Arbeitskreis "Technische und organisatorische Datenschutzfragen"

Im Berichtszeitraum wurden fünf Sitzungen des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ (AK Technik) in Schwerin, Kiel, Rostock, Hannover und Karlsruhe durchgeführt. Die Auswahl der Tagungsorte stand im Zusammenhang mit den Themen, die in den jeweiligen Sitzungen behandelt wurden. In Kiel stand beispielsweise ein Besuch bei der Datenzentrale Schleswig-Holstein auf dem Programm, weil Fragen der Sicherheit von PC und Netzen dort mit besonderem Engagement bearbeitet werden. In Karlsruhe tagte der AK Technik auf Einladung des Fraunhofer-Instituts für Informations- und Datenverarbeitung (IITB) und des Europäischen Instituts für Systemsicherheit (E.I.S.S.). Schwerpunkt dieser Sitzung waren Fragen der IT-Sicherheit bei der Nutzung von Internet-Diensten durch öffentliche Stellen.

Es hat sich bewährt, zu den Sitzungen des Arbeitskreises Spezialisten aus verschiedenen Bereichen von Industrie, Wissenschaft und Verwaltung einzuladen, um deren Fachwissen in die Beratungen einfließen zu lassen.

Neben den turnusmäßigen Sitzungen wurden unter Federführung des AK Technik zu den Themen "Automatische Autobahngebührenerhebung" (siehe Punkt 2.19.1) und "Kryptografie" (siehe Punkt 2.16.4) Workshops in Berlin und Wiesbaden veranstaltet. Ziel dieser Workshops war es, sich mit neuen Technologien vertraut zu machen und den Herstellern bereits im Stadium der Entwicklung datenschutzrechtliche Empfehlungen für neue Produkte und Verfahren zu geben. Ein konstruktiver Meinungsaustausch zwischen Datenschutzbeauftragten, Vertretern von Wissenschaft und Forschung, zukünftigen Anwendern neuer Verfahren und Anbietern von Hard- und Software wurde so ermöglicht.

Die Arbeitsergebnisse des AK Technik werden auf unterschiedliche Art und Weise publiziert. So werden Entschließungen der Konferenz der Datenschutzbeauftragten, die den technisch-organisatorischen Bereich betreffen, im Arbeitskreis vorbereitet. Beispiele hierfür sind die Entschließungen zu den Themen "Elektronische Mitteilungssysteme (X.400)" (siehe Anlage 15) oder "Automatische Erhebung von Straßennutzungsgebühren" (siehe Anlage 16). In Form von schriftlichen Berichten informiert der Arbeitskreis die Konferenz zu aktuellen technisch-organisatorischen Fragen. Als geeignetes Mittel zur Information von Bürgern und Mitarbeitern der öffentlichen Stellen hat sich die sogenannte Orientierungshilfe bewährt. In diesen Orientierungshilfen berichtet der Arbeitskreis einerseits umfassend über neue technische Entwicklungen, andererseits werden aber auch ganz konkrete Empfehlungen für den datenschutzgerechten Einsatz bestimmter neuer Techniken oder automatisierter Verfahren gegeben. Alle im Berichtszeitraum vom AK Technik ausgearbeiteten Orientierungshilfen sind in meiner Dienststelle kostenlos erhältlich:

- Datenschutzrechtliche Protokollierung beim Betrieb informationstechnischer Systeme (siehe Punkt 2.16.3)
- Datenschutzrechtliche Aspekte beim Einsatz optischer Datenspeicherung (siehe Punkt 2.19.4)
- Anschluß von öffentlichen Netzen an das Internet (siehe Punkt 2.18.3).

Ich möchte die Gelegenheit nutzen, um mich an dieser Stelle für die Einsatzbereitschaft meiner Kollegen bei der Mitarbeit im AK Technik zu bedanken. Sowohl an den Sitzungen des Arbeitskreises als auch an der selbständigen Tätigkeit der Arbeitsgruppen beteiligen sich alle Kollegen mit viel Engagement und Kompetenz.

In Zukunft werden die verschiedenen Arbeitskreise verstärkt zusammenarbeiten. Schon jetzt beraten beispielsweise Mitglieder des AK Sicherheit und des AK Technik gemeinsam datenschutzrechtlichen Fragen bei der Einführung von INPOL-Neu (siehe Punkt 2.3.2).

3. Öffentlichkeitsarbeit und Beratungstätigkeit

3.1. Beratungs- und Kontrollbesuche

Aufgrund steigender Beratungsersuchen öffentlicher Stellen habe ich meine Kontrollen in zunehmendem Maße auf anlaßbezogene Sachverhalte reduzieren müssen. Die Zahl der Routinekontrollen ist dadurch zurückgegangen. Während im ersten Berichtszeitraum vor allem datenschutzrechtliche Fragen grundsätzlicher Art im Mittelpunkt standen, wurden nunmehr einzelne Fachbereiche der öffentlichen Verwaltung im Hinblick auf die konkrete Aufgabenerfüllung kontrolliert.

Ich begrüße es, daß die öffentlichen Stellen des Landes meine Dienststelle zunehmend einbeziehen, um datenschutzrechtliche Erfordernisse bei der Einführung neuer Verfahren bereits im Planungsstadium zu berücksichtigen. So werden Verstöße gegen datenschutzrechtliche Bestimmungen vermieden und Kosten reduziert, denn die Umsetzung der Anforderungen in laufenden Verfahren wird in der Regel kostenintensiver.

3.2. Vorträge

Meine Mitarbeiter und ich haben Vorträge zu unterschiedlichen Themen des Datenschutzes gehalten. Aus personellen Gründen konnten leider nicht alle Vortragswünsche erfüllt werden. Die Vorträge wurden im Rahmen von Seminaren, Schulungen, Work-shops, Vorlesungen, Informationsveranstaltungen und Treffen zum Erfahrungsaustausch auf verschiedenen Ebenen gehalten. Themen waren beispielsweise:

- Grundsätze des Datenschutzes in der Landesverwaltung
- Stellung und Aufgaben des behördlichen Datenschutzbeauftragten
- Technische und organisatorische Aspekte des Datenschutzes
- Datenschutzrechtliche Anforderungen an die Datenverarbeitung im Auftrag
- Probleme des Datenschutzes bei Systemen zur automatischen Gebührenerhebung auf Autobahnen
- Datenschutz beim Einsatz digitaler Telekommunikationsanlagen
- Datenschutz im Krankenhaus
- Datenschutz in der Kinder- und Jugendhilfe
- Umgang mit Personalakten
- Datenschutz und Umweltschutz
- Zukunftsaspekte des Datenschutzes

3.3. Info-Blätter

Das Interesse der Bürger unseres Landes an Informationen zum Datenschutz hat weiter zugenommen. In den letzten zwei Jahren habe ich zehn neue Informationsblätter herausgegeben, die einen Überblick über grundsätzliche sowie aktuelle datenschutzrechtliche Themen geben sollen. Sie erheben nicht den Anspruch, umfassend oder auf konkrete Fragestellungen im Einzelfall Antworten zu geben, sondern dienen dem Verständnis des Datenschutzrechts in seiner praktischen Anwendung an Beispielen. Neben vielen Einzelpersonen haben auch öffentliche Stellen und Unternehmen diese Informationen angefordert. Neu sind im Berichtszeitraum erschienen: Autobahngebühren im Blickfeld, Das ISDN-Netz, Freiwillige Patienten-Chipkarten, Datenschutz in der Schule, Umgang mit Sozialdaten, Personenbezogene Daten in der Forschung, Technikfolgenabschätzung, Sicherheit der Informationstechnik, Personalakten und Personalaktendaten sowie Statistische Erhebungen.

3.4. Beratungen mit den behördlichen Datenschutzbeauftragten

Beratungen mit den Datenschutzbeauftragten der obersten Landesbehörden fanden in den vergangenen zwei Jahren regelmäßig statt. Dabei hat sich jedoch gezeigt, daß in den verschiedenen Ressorts sehr unterschiedliche datenschutzrechtliche Fragestellungen von Interesse sind. Zur Lösung dieser Einzelprobleme sind gemeinsame Beratungen in der bisher geführten Form nicht besonders geeignet. Ich habe deshalb vorgeschlagen, den Erfahrungsaustausch mit den obersten Landesbehörden in Zukunft erst dann fortzuführen, wenn genügend Themen zur Beratung vorliegen, die alle Ressorts betreffen.

Im Mai 1995 habe ich erstmals die behördlichen Datenschutzbeauftragten der Landkreise und kreisfreien Städte zu einem Erfahrungsaustausch eingeladen. Im Mittelpunkt dieses Gesprächs standen vor allem datenschutzrechtliche Fragen grundsätzlicher Art, wie das Berufsbild, die Qualifikation und die Aufgaben eines behördlichen Datenschutzbeauftragten, die Realisierung von technischen und organisatorischen Maßnahmen sowie Datenübermittlungen innerhalb von Behörden. Darüber hinaus trugen die Teilnehmer Fälle aus der Praxis vor, die von den Anwesenden erörtert wurden. Im Bedarfsfall kann die nächste gemeinsame Beratung in der ersten Hälfte des Jahres 1996 von mir durchgeführt werden.

4. Novellierungsvorschläge zum Landesdatenschutzgesetz

4.1. Novellierungsvorschläge

Schon in meinem Ersten Tätigkeitsbericht hatte ich einige Vorschläge zur Änderung des Landesdatenschutzgesetzes von Mecklenburg-Vorpommern gemacht. Die Erfahrungen der vergangenen zwei Jahre haben gezeigt, daß unser Landesdatenschutzgesetz verbesserungsbedürftig ist.

Erweiterung des Anwendungsbereichs bei Gerichten und Staatsanwaltschaften

Das Landesdatenschutzgesetz gilt nach der gegenwärtigen Rechtslage für die Staatsanwaltschaften und Gerichte nur, soweit sie Verwaltungsaufgaben ausführen. In ihrer Eigenschaft als Rechtsprechungsorgane unterliegen die Gerichte jedoch dem Bundesdatenschutzgesetz. Um eine einheitliche Regelung aller datenschutzrelevanten Vorgänge bei den Gerichten und Staatsanwaltschaften zu ermöglichen, sollte das Landesdatenschutzgesetz generell für alle Organe der Rechtspflege gelten, unabhängig davon, welche Tätigkeiten sie ausführen. Als notwendige Folge dieser Ausdehnung muß wegen der grundgesetzlich garantierten richterlichen Unabhängigkeit die Kontrolle des Landesbeauftragten für den Datenschutz bei Gerichten jedoch weiterhin auf deren Tätigkeiten in Verwaltungsangelegenheiten beschränkt bleiben. Um bei der datenschutzrechtlichen Kontrolle der von den Gerichten eingesetzten automatischen Datenverarbeitungssysteme die Abgrenzungsschwierigkeiten zu vermeiden - in Punkt 2.17.4 wird dieses Problem an einem konkreten Beispiel deutlich -, sollte in § 26 - Kontrolle - folgender Satz eingefügt werden: "Setzen Gerichte zur Erfüllung ihrer gesetzlichen Aufgaben automatische Datenverarbeitungsanlagen ein, so unterliegt unbeschadet der richterlichen Unabhängigkeit die Ordnungs- und Rechtmäßigkeit der Verfahren der Kontrolle des Landesbeauftragten für den Datenschutz."

Vorrang des Datenschutzgesetzes vor dem Verwaltungsverfahrensgesetz

Es sollte eine Vorschrift aufgenommen werden, wonach das Landesdatenschutzgesetz dem Landesverwaltungsverfahrensgesetz vorgeht, soweit bei der Ermittlung eines Sachverhalts personenbezogene Daten verarbeitet werden. Dies wäre eine Ausnahme von dem Grundsatz der Nachrangigkeit des Landesdatenschutzgesetzes gegenüber anderen anzuwendenden Rechtsvorschriften. Sie ist in diesem Fall jedoch angebracht, da das Landesverwaltungsverfahrensgesetz selbst ein Auffanggesetz darstellt und das Landesdatenschutzgesetz bezüglich des Umgangs mit personenbezogenen Daten sachgemäßere Regelungen enthält.

Zweckbindung der sogenannten Protokolldateien

Zur Datenschutzkontrolle, zur Datensicherung und zum Erreichen einer fehlerfreien automatischen Datenverarbeitung sind verschiedene Protokollierungen erforderlich. Sowohl Veränderungen an Hard- und Softwarekomponenten als auch die Verarbeitung personenbezogener Daten sind zu protokollieren, damit jederzeit nachvollzogen werden kann, wer wann mit welchen Mitteln Daten verändert hat. Da Protokolle eine Vielzahl personenbezogener Daten enthalten, ist dem Mißbrauch vorzubeugen. Deshalb sollte eine Vorschrift aufgenommen werden, die die Nutzung der Protokolldaten für andere Zwecke ausdrücklich verbietet (siehe auch Punkt 2.16.3).

Pflicht zur Führung eines Aktenverzeichnisses

Es sollte eine Vorschrift eingefügt werden, die die öffentlichen Stellen und ihre Auftragnehmer verpflichtet, ein Verzeichnis derjenigen Akten zu führen, in denen personenbezogene Daten gespeichert sind. Dies würde dem Auskunftsrecht des Betroffenen dienen und die Kontrolle durch den Datenschutzbeauftragten erleichtern.

Technische und organisatorische Maßnahmen - Stand der Technik

Nach § 17 Abs. 1 DSG MV sind "...die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich und angemessen sind, um die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz sicherzustellen...". Hier sollte ergänzt werden, daß sich die Art und Weise der Maßnahmen nach dem jeweiligen Stand der Technik zu richten hat. Zur Umsetzung dieser allgemein gehaltenen Forderung sollte bestimmt werden, daß die Landesregierung unter Beteiligung des Landesbeauftragten für den Datenschutz durch Rechtsverordnung die Anforderungen an die einzelnen Maßnahmen nach dem jeweiligen Stand der Technik festsetzt und fortschreibt. Eine Rechtsverordnung ist wie ein Gesetz allgemein verbindlich, ihr Erlaß sowie ihre Änderung sind aber wesentlich einfacher als bei einem Gesetz, so daß eine rasche Anpassung an den sich gerade in diesem Bereich rasant verändernden Stand der Technik erreichbar ist.

Beanstandungen gegenüber Hochschulen

Hochschulen haben eine besondere Stellung unter den juristischen Personen des öffentlichen Rechts. Beispielsweise steht ihnen die Selbstverwaltung im Rahmen der Gesetze zu. Trotz ihrer Autonomie können aber auch gegenüber diesen Institutionen Beanstandungen ausgesprochen werden. Um diesem Sachverhalt Rechnung zu tragen, sollten im § 28 DSG MV - Beanstandungen - die Hochschulen in der Aufzählung der möglichen Adressaten von Beanstandungen des Landesbeauftragten für den Datenschutz ausdrücklich erwähnt werden.

Der Datenschutzbeauftragte als oberste Landesbehörde

Die Landesverfassung verleiht dem Landesbeauftragten für den Datenschutz die Stellung eines unabhängigen, allein den Gesetzen unterworfenen Kontrollorganes. Es sollte daher im Wortlaut des Landesdatenschutzgesetzes zum Ausdruck kommen, daß das Amt des Landesbeauftragten für den Datenschutz als oberste Landesbehörde beim Präsidenten des Landtages eingerichtet wird. Diese Klarstellung ist angesichts der verfassungsrechtlichen Bedeutung sowie der sich aus dem Datenschutzgesetz ergebenden Rechtsstellung und Aufgaben des Landesbeauftragten für den Datenschutz geboten, insbesondere da er auch das Recht zur Kontrolle anderer oberster Landesbehörden hat.

4.2. Entwurf eines Änderungsgesetzes

Der Innenminister übersandte mir den Referentenentwurf eines Ersten Gesetzes zur Änderung des Landesdatenschutzgesetzes mit der Bitte um Stellungnahme. Dieser Entwurf sieht unter anderem vor, § 27 Abs. 2 um einen zweiten Satz zu ergänzen.

Der bisherige § 27 Abs. 2 lautet:

"Die Rechte nach Absatz 1[Auskunfts- und Zutrittsrechte] dürfen nur vom Landesbeauftragten für den Datenschutz persönlich ausgeübt werden, wenn die zuständige oberste Landesbehörde im Einzelfall feststellt, daß die Sicherheit des Bundes oder eines Landes dies gebietet."

Als zweiter Satz soll hinzugefügt werden:

"In diesem Fall müssen personenbezogene Daten eines Betroffenen, dem von der datenverarbeitenden Stelle Vertraulichkeit besonders zugesichert worden ist, auch dem Landesbeauftragten für den Datenschutz gegenüber nicht offenbart werden."

In meiner Stellungnahme habe ich diese Ergänzung abgelehnt.

Die geplante Ergänzung würde dazu führen, daß zum Beispiel Daten, die von Mitarbeitern der Verfassungsschutzbehörde bei und über Referenzpersonen erhoben wurden, keiner externen Kontrolle mehr unterliegen. Die besondere Zusicherung der Vertraulichkeit schwächt somit die Rechtsstellung desjenigen, gegenüber dem sie erfolgte. Kontrollen insbesondere im Bereich des Verfassungsschutzes haben unter anderem ergeben, daß weit mehr Daten als erforderlich gespeichert wurden. Ohne die Kontrollbefugnis des Landesbeauftragten für den Datenschutz, die ihm nach dem Willen des Innenministers möglichst entzogen werden soll, wäre diese für den Betroffenen nachteilige Situation wahrscheinlich nicht bekannt geworden.

Insgesamt stellt die vorgeschlagene Ergänzung die Schaffung eines kontrollfreien Bereichs dar, verbunden mit einer erheblichen Einschränkung der Rechte des Bürgers.

Der Stellungnahme habe ich als Anlage meine Novellierungsvorschläge beigefügt. Außerdem habe ich auf den Änderungsbedarf hingewiesen, der sich aus der inzwischen verabschiedeten EU-Datenschutzrichtlinie ergibt (siehe Abschnitt 2.1).

5. Anlagen

Anlage 1

Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1994

Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten von Bund und Länder verfolgen die zunehmende Verwendung von Chipkarten im Gesundheits- und Sozialwesen mit kritischer Aufmerksamkeit.

Chipkarte als gesetzliche Krankenversicherungskarte

Die Krankenversicherungskarte, die bis Ende des Jahres in allen Bundesländern eingeführt sein wird, darf nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten. Die Datenschutzbeauftragten überprüfen, ob

- die Krankenkassen nur die gesetzlich zulässigen Daten auf den Chipkarten speichern und
- die Kassenärztlichen Vereinigungen dafür sorgen, daß nur vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte Lesegeräte und vom Bundesverband der Kassenärztlichen Vereinigungen geprüfte Programme eingesetzt werden.

Chipkarte als freiwillige Gesundheitskarte

Sogenannte "Gesundheitskarten", etwa "Service-Karten" von Krankenversicherungen und privaten Anbietern, "Notfall-Karten", "Apo(theken)-Cards" und "Röntgen-Karten" werden neben der Krankenversicherungskarte als freiwillige Patienten-Chipkarte angeboten und empfohlen. Während die Krankenversicherungskarte nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten darf, kann mit diesen "Gesundheitskarten" über viele medizinische und andere persönliche Daten schnell und umfassend verfügt werden.

Gegenüber der konventionellen Ausweiskarte oder einer Karte mit einem Magnetstreifen ist die Chipkarten-Technik ungleich komplexer und vielfältig nutzbar. Damit steigen auch die Mißbrauchsgefahren bei Verlust, Diebstahl oder unbemerktem Ablesen der Daten durch Dritte. Anders als bei Ausweiskarten mit Klartext können Chipkarten nur mit technischen Hilfsmitteln gelesen werden, die der Betroffene in der Regel nicht besitzt. So kann er kaum kontrollieren, sondern muß weitgehend darauf vertrauen, daß der Aussteller der Karte und sein Arzt nur die mit ihm vereinbarten Daten im Chip speichern, das Lesegerät auch wirklich alle gespeicherten Daten anzeigt und der Chip keine oder nur eindeutig vereinbarte Verarbeitungsprogramme enthält.

Die Freiwilligkeit der Entscheidung für oder gegen die Gesundheitskarte mit Chipkarten-Technik ist in der Praxis bisweilen nicht gewährleistet. So wird ein faktischer Zwang auf die Entscheidungsfreiheit des Betroffenen ausgeübt, wenn der Aussteller - etwa ein Krankenversicherungsunternehmen oder eine Krankenkasse - mit der Einführung der Chipkarte das bisherige konventionelle Verfahren erheblich ändert, z. B. den Schriftwechsel erschwert oder den Zugang zu Leistungen Karten-Inhabern vorbehält bzw. erleichert.

So stellt beispielsweise eine Kasse ihren Mitgliedern Bonuspunkte in Aussicht, wenn sie auf sog. Aktionstagen der Kasse Werte wie Blutzucker, Sauerstoffdynamik, Cholesterol sowie weitere spezielle medizinische Daten ohne ärztliche Konsultation messen und auf der Karte speichern und aktualisieren lassen. In Abhängigkeit von der Veränderung dieser Werte wird von der Kasse gegebenenfalls ein Arztbesuch empfohlen. Die Vergabe solcher Bonuspunkte widerspricht dem Prinzip der Freiwilligkeit bei der Erhebung der Daten für die PatientenChipkarte. Der Effekt wird noch verstärkt, indem die Kasse die "Möglichkeit einer Beitragsrückerstattung" in Aussicht stellt. Die Datenschutzbeauftragten des Bundes und der Länder sehen in dieser Art der Anwendung der Chipkarten-Technik das Risiko eines Mißbrauchs, solange der Inhalt und die Nutzung der Daten nicht mit den zuständigen Fachleuten - wie den Medizinern - und den Krankenkassen abgestimmt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält für den Einsatz und die Nutzung freiwilliger Patienten-Chipkarten zumindest - vorbehaltlich weiterer Punkte die Gewährleistung folgender Voraussetzungen für erforderlich:

- Die Zuteilung einer Gesundheitskarte und die damit verbundene Speicherung von Gesundheitsdaten bedarf der schriftlichen Einwilligung des Betroffenen. Er ist vor der Erteilung der Einwilligung umfassend über Zweck, Inhalt und Verwendung der angebotenen Gesundheitskarte zu informieren.

- Die freiwillige Gesundheitskarte darf nicht - etwa durch Integration auf einem Chip - die Krankenversichertenkarte nach dem Sozialgesetzbuch verdrängen oder ersetzen.

- Die Karte ist technisch so zu gestalten, daß für die einzelnen Nutzungsarten nur die jeweils erforderlichen Daten zur Verfügung gestellt werden.

- Der Betroffene muß von Fall zu Fall frei und ohne Benachteiligung - z. B. gegenüber dem Arzt, der Krankenkasse oder der Versicherung - entscheiden können, die Gesundheitskarte zum Lesen der Gesundheitsdaten vorzulegen und ggf. den Zugriff auf bestimmte Daten zu beschränken. Er muß ferner frei entscheiden können, wer welche Daten in seinen Datenbestand übernehmen darf. Der Umfang der Daten, die gelesen oder übernommen werden dürfen, ist außerdem durch die gesetzliche Aufgabenstellung bzw. den Vertragszweck der Nutzer beschränkt.

- Der Kartenaussteller muß sicherstellen, daß der Betroffene jederzeit vom Inhalt der Gesundheitskarte unentgeltlich Kenntnis nehmen kann.

- Der Betroffene muß jederzeit Änderungen und Löschungen der gespeicherten Daten veranlassen können.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dafür aus, daß der Gesetzgeber dies durch bereichsspezifische Rechtsgrundlagen sicherstellt.

Anlage 2

Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 09./10. März 1994
(bei Stimmenthaltung Bayerns)

Informationsverarbeitung im Strafverfahren

Die Datenschutzbeauftragten des Bundes und der Länder erinnern an ihre Vorschläge zu gesetzlichen Regelungen der Informationsverarbeitung im Strafverfahren, die sie seit 1981 unterbreitet haben.

Während die Befugnisse von Polizei und Staatsanwaltschaft zur Datenerhebung bei Ermittlungen mittlerweile in weitreichender Form gesetzlich abgesichert wurden, fehlen weiterhin Regelungen in der Strafprozeßordnung, wie die erhobenen Daten in Akten und Dateien weiter verarbeitet werden dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder halten die Beachtung folgender Grundsätze für notwendig, die in den Entwürfen des Bundes (Art. 4 §§ 474 ff. StPO des Entwurfs für ein Verbrechensbekämpfungsgesetz - BT-Drucksache 12/6853) und der Länder (Entwurf eines Strafverfahrensänderungsgesetzes 1994 des Strafrechtsausschusses der Justizministerkonferenz) nicht ausreichend berücksichtigt sind:

1. Strafrechtliche Ermittungsakten enthalten eine Vielzahl höchstsensibler Daten insbesondere auch über Opfer von Straftaten und Zeugen, die deshalb eines wirksamen Schutzes bedürfen. Es würde den Besonderheiten der im Strafverfahren - auch mit Zwangsmitteln - erhobenen Daten nicht entsprechen, wenn Strafakten als Informationsquelle für jegliche Zwecke anderer Behörden oder von nicht am Strafverfahren Beteiligten dienten. Die einzelnen Zwecke und die zugriffsberechtigten Stellen sind daher abschließend normenklar festzulegen.

1.1 Ingesamt ist sicherzustellen, daß der in anderen Zweigen der öffentlichen Verwaltung verbindlich geltende Standard des Datenschutzes für Übermittlungen keinesfalls unterschritten wird.

1.2 Soweit ein unabweisbarer Bedarf anderer Stellen an Informationen aus Strafverfahren besteht, ist er in erster Linie durch Erteilung von Auskünften zu befriedigen. Akteneinsichtnahmen oder Aktenübersendungen können erst dann zugelassen werden, wenn eine Auskunftserteilung nicht ausreicht. Nicht erforderliche Aktenteile müssen ausgesondert werden. An Privatpersonen dürfen Informationen aus strafrechtlichen Ermittlungen nur weitergegeben werden, wenn deren rechtliche Interessen davon abhängen.

2. Bei Regelungen zur dateimäßigen Speicherung ist zu unterscheiden zwischen Systemen zur Vorgangsverwaltung (wie z. B. zentrale Namensdateien) und Dateien, die der Unterstützung strafprozessualer Ermittlungen dienen (z. B. Spurendokumentations- und Recherchesysteme).

2.1 Der Datensatz zur Vorgangsverwaltung ist auf die Angaben zu beschränken, die zum Auffinden der Akten und zur Information über den Verfahrensstand erforderlich sind. Daten über Personen, die keine Beschuldigten sind, dürfen nur dann erfaßt werden, wenn dies zur Vorgangsverwaltung zwingend erforderlich ist. In diesen Fällen bedarf es besonderer Zugriffs- und Verwendungsbeschränkungen.

In jedem Fall sind die Daten entsprechend dem Verfahrensstand zu aktualisieren. Vom Gesetzgeber sind konkrete Löschungsfristen vorzusehen. Die Speicherung ist längstens auf den Zeitpunkt zu begrenzen, für den die Akte aufbewahrtwird. Vorgangsverwaltungssysteme können so auch für eine wirksame Kontrolle der Aufbewahrungsfristen genutzt werden.

2.2 Die Staatsanwaltschaft kann sich zur Verwaltung ihres konventionell gespeicherten Datenmaterials grundsätzlich eines behördeninternen, automatisierten Nachweissystems bedienen. Länderübergreifende automatisierte Informationssysteme dürfen in Beachtung des Erforderlichkeitsprinzips demgegenüber allenfalls für solche Vorgänge errichtet werden, bei denen bestimmte Tatsachen die Prognose begründen, daß auf die erfaßten Daten zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben (erneut) zugegegriffen werden muß.

Eine solche Prognose wird in der Regel dann nicht gerechtfertigt sein, wenn das zugrundeliegende Verfahren mit einer Einstellung nach § 170 Abs. 2 StPO oder einem rechtskräftigen Freispruch abgeschlossen worden ist, sofern nicht auch nach Abschluß des Verfahrens noch tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte eine strafbare Handlung begangen hat. Eine Bereitstellung von Daten jedenfalls zu Zwecken der Strafverfolgung wird ferner grundsätzlich dann nicht in Betracht kommen, wenn die Ermittlungen konkrete Anhaltspunkte dafür bieten, daß der Beschuldigte nicht erneut strafbare Handlungen begehen wird. Dies kann z. B. bei Fahrlässigkeitstaten der Fall sein. Bei laufenden Verfahren kann die Zulässigkeit der Aufnahme von Daten im Hinblick auf die Möglichkeiten einer Verbindung von Verfahren, die Einstellung nach § 154 StPO oder die Gesamtstrafenbildung gegeben sein.

2.3 Für einen Informationsverbund zwischen verschiedenen speichernden Staatsanwaltschaften mit der Möglichkeit eines Direktzugriffs auf die Daten der jeweils anderen Behörden ergibt sich als Voraussetzung, daß die Weitergabe aller dem Zugriff unterliegenden Daten zumindest bei abstrakter Betrachtung zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben der übermittelnden oder der zugriffsberechtigten Stellen geeignet und angemessen sein muß.

Für den Bereich der Strafverfolgung gilt ein umfassendes Aufklärungsgebot (§§ 152 Abs. 2, 160 StPO). Die Staatsanwaltschaft kann im Rahmen ihrer Ermittlungen grundsätzlich ohne Rücksicht auf das Gewicht des Tatvorwurfs von allen öffentlichen Behörden - also auch von anderen Staatsanwaltschaften - Auskunft verlangen (§ 161 Satz 1 StPO). Diese Auskunftspflicht besteht über das Ermittlungsverfahren hinaus bis zum Abschluß des Strafverfahrens. Daten, die im Falle einer entsprechenden Anfrage zu mit einem Strafverfahren zusammenhängenden Zwecken offenbart werden müßten, können damit - ungeachtet der besonderen Voraussetzungen für die Errichtung eines Direktabrufverfahrens - von jeder Staatsanwaltschaft für andere Staatsanwaltschaften grundsätzlich auch in einem Informationssystem mit Direktabrufmöglichkeit bereitgestellt werden, sofern nur bestimmte Tatsachen die Annahme rechtfertigen, daß die Daten in einem Verfahren einer anderen Behörde verwertet werden müssen. Eine solche Annahme wird regelmäßig wiederum in den unter 2.2 dargestellten Fällen nicht zu begründen sein.

Eine Bereitstellung von Daten wird darüber hinaus auch dann nicht erfolgen können, wenn diese einem besonderen Amtsgeheimnis unterliegen und deshalb auch auf Anforderung nicht ohne weiteres übermittelt werden dürften. Auf § 78 SGB X ist in diesem Zusammenhang hinzuweisen. Ein Direktabruf durch andere Stellen als Staatsanwaltschaften ist schon nach der Zweckbestimmung des Systems ausgeschlossen.

2.4 In der Praxis dienen derzeit die bestehenden polizeilichen Informationssysteme auch den Zwecken der Strafverfolgung. Eine Abstimmung der polizeilichen und der staatsanwaltschaftlichen Informationssysteme ist geboten. Eine weitere Abstimmung wird im Hinblick auf das Bundeszentralregister zu erfolgen haben, das ebenfalls Daten zu Zwecken der Strafverfolgung, aber auch der Strafvollstreckung speichert.

Die Datenschutzbeauftragten halten daher eine grundlegende Überarbeitung dieser Entwürfe für notwendig und bieten hierfür ihre Unterstützung an (vgl. Beschlüsse der Datenschutzkonferenzen vom 28./29. September 1981 zu "Mindestanforderungen für den Datenschutz bei den Zentralen Namenskarteien der Staatsanwaltschaften", vom 24./25. November 1986 "Überlegungen zu Regelungen der Informationsverarbeitung im Strafverfahren" und vom 05./06. April 1989 zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts vom 03. November 1988).

Anlage 3

Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1994
(gegen die Stimme Bayerns)

Abbau des Sozialdatenschutzes

Der Gesetzgeber hat in den vergangenen Monaten die Möglichkeit der Überprüfung von Sozialleistungsempfängern ohne deren vorherige Befragung oder Kenntnis in drastischem Umfang vermehrt. Insbesondere durch das seit dem 1. Juli 1993 geltende Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms ist das Kontrollinstrumentarium von Sozialund Arbeitsämtern noch einmal erheblich erweitert worden. Ohne Rücksicht auf konkrete Anhaltspunkte für einen unberechtigten Leistungsbezug im Einzelfall sind künftig automatisierte Datenabgleiche zwischen Sozialhilfeträgern sowie zwischen diesen und der Arbeitsverwaltung bzw. der Kranken-, Unfall- und Rentenversicherung gestattet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist sehr besorgt über diese Entwicklung, die zu einem immer dichteren Datenverbundsystem im Sozialleistungsbereich und zu immer nachhaltigeren Eingriffen in das Recht auf informationelle Selbstbestimmung aller Betroffenen, d. h. auch und gerade der großen Mehrheit rechtstreuer Antragsteller und Leistungsbezieher, führt.

Mit Nachdruck wenden sich die Datenschutzbeauftragten gegen Versuche von Sozialverwaltungen, bei der Umsetzung der neuen Kontrollregelungen durch extensive Interpretation über den gesetzlich vorgegebenen Rahmen hinauszugehen. So erlaubt beispielsweise der neu gefaßte § 117 Abs. 3 des Bundessozialhilfegesetzes entgegen der Handhabung einzelner Kommunen keinen automatisierten Datenabgleich zwischen Sozialhilfedatei und Kraftfahrzeug-Register, sondern nur den Vergleich von Angaben in Verdachtsfällen.

Die dargestellte Entwicklung macht es erneut notwendig, auf die verfassungsrechtliche Qualität des Grundsatzes der Datenerhebung beim Betroffenen hinzuweisen. An dem Prinzip, daß bei der Überprüfung der Leistungsberechtigung und der Nachweise Auskünfte zunächst beim Antragsteller anzufordern sind und nur aufgrund konkreter Verdachtsmomente Nachfragen bei dritten Stellen oder Datenabgleiche erfolgen dürfen, muß für den Regelfall festgehalten werden, soll der Einzelne mündiger Bürger bleiben und nicht zum bloßen Objekt staatlicher Verhaltenskontrolle werden.

Sorge äußert die Konferenz auch über die hartnäckigen Bestrebungen, Datenbestände der Sozialverwaltung für immer neue Zwecke und Adressaten zu öffnen. Beispiele dafür sind die im Gesetzgebungsverfahren zum 2. SGB-Änderungsgesetz im letzten Augenblick gescheiterten Anträge, Polizei und Staatsschutz in unvertretbarem Umfang Zugriff auf Daten Arbeitsloser und sonstiger Sozialleistungsempfänger zu geben. Das Sozialgeheimnis muß ein wirksamer Sonderschutz für die besonders sensiblen Daten in der Sozialverwaltung bleiben. Nur dies entspricht der Abhängigkeit des Einzelnen von staatlichen Leistungen und der sich daraus ergebenden speziellen Verletzlichkeit seines Rechts auf informationelle Selbstbestimmung.

Anlage 4

Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 09./10. März 1994

Gesetzentwurf der Bundesregierung zur Neuordnung des Postwesens und der Telekommunikation

(Postneuordnungsgesetz - PTNeuOG, BR-Drs. 115/94 = BT-Drs. 12/6718) und zu der dafür erforderlichen Änderung des Grundgesetzes (BR-Drs. 114/94 = BT-Drs. 12/6717)

I.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, daß mit der Umwandlung der Deutschen Bundespost POSTDIENST in die Deutsche Post AG und der Deutschen Bundespost TELEKOM in die Deutsche Telekom AG zwei staatliche Einrichtungen aufhören zu existieren, gegenüber denen sich der Bürger bisher unmittelbar auf das Post- und Fernmeldegeheimnis berufen kann. Sie treten deshalb dafür ein, in der Verfassung sicherzustellen, daß jeder, der Post- und Fernmeldedienstleistungen erbringt, das Post- und Fernmeldegeheimnis zu wahren hat.

II.

Im Gesetz zur Neuordnung des Postwesens und der Telekommunikation ist ein den Vorgaben des Bundesverfassungsgerichts in seinem Volkszählungsurteil vom 15. Dezember 1983 und in seinem Fangschaltungsbeschluß vom 25. März 1992 entsprechender Schutz von Individualrechten zu gewährleisten.

Die Datenschutzbeauftragten halten inbesondere folgende Änderungen des Gesetzentwurfs für erforderlich:

a) Der Umfang der zulässigen Verarbeitung personenbezogener Daten im Post- und Telekommunikationswesen ist im Gesetz selbst festzulegen; lediglich deren konkrete Ausgestaltung kann der Regelung durch Rechtsverordnungen überlassen bleiben.

b) Die Gewährleistung des Datenschutzes und des Post- und Fernmeldegeheimnisses muß in den Katalog der Ziele der Regulierung aufgenommen werden.

c) Das Post- und Telekommunikationswesen muß auf Dauer - auch nach dem Wegfall der Monopole - einer effektiven, unabhängigen datenschutzrechtlichen Kontrolle von Amts wegen nach bundesweit einheitlichen Kritierien unterworfen bleiben, auch soweit personenbezogene Daten nicht in Dateien verarbeitet werden.

d) Die Frist für die Speicherung von Verbindungsdaten zur Ermittlung und zum Nachweis der Entgelte ist präzise festzulegen.

e) Die vorgesehene Vorschrift zum Einzelentgeltnachweis schränkt den Kreis der Einrichtungen, die Telefonberatung durchführen und die nicht auf Einzelentgeltnachweisen erscheinen sollen, in unakzeptabler Weise ein. Dem Schutz des informationellen Selbstbestimmungsrechtes und des Fernmeldegeheimnisses der Angerufenen würde es dagegen am ehesten entsprechen, wenn jeder inländische Anschlußinhaber selbst entscheiden kann, ob und gegebenenfalls wie seine Rufnummer auf Einzelentgeltnachweisen erscheinen soll. Damit wäre auch die Anonymität von Anrufen bei Beratungseinrichtungen unbürokratisch sicherzustellen. Ein entsprechendes Verfahren wird in den Niederlanden bereits praktiziert.

f) Es wäre völlig unangemessen, wenn in Zukunft erlaubt würde, daß die Telekommunikationsunternehmen Nachrichteninhalte über die Befugnisse des § 14 a Fernmeldeanlagengesetz hinaus auch für die Unterbindung von Leistungserschleichungen und sonstiger rechtswidriger Inanspruchnahme des Telekommunikationsnetzes und seiner Einrichtungen sowie von Telekommunikations- und Informationsdienstleistungen erheben, verarbeiten und nutzen dürften.

III.

Die Datenschutzbeauftragten betonen, daß angesichts der neuen technischen Möglichkeiten digitaler Kommunikations- und Informationsdienste und der mit ihrer Nutzung zwangsläufig verbundenen Datenverarbeitung eine grundlegende Überarbeitung des § 12 Fernmeldeanlagengesetz, der die Weitergabe vorhandener Telekommunikationsdaten in Strafverfahren erlaubt, überfällig ist. Sie erinnern an die Umsetzung der entsprechenden Entschließung des Bundesrates vom 27. August 1991 (BR-Drs. 416/91).

Anlage 5

Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 09./10. März 1994
(gegen die Stimme Bayerns)

Ausländerzentralregistergesetz

Das Ausländerzentralregister beim Bundesverwaltungsamt in Köln existiert seit 40 Jahren ohne gesetzliche Grundlage. Derzeit stehen den verschiedenen Benutzern des Registers Daten zu mindestens 8 Millionen Ausländern, die sich in der Bundesrepublik aufhalten oder aufgehalten haben, zur Verfügung. Gespeichert sind neben Daten zur Identifizierung und weiteren Beschreibung der Person insbesondere Angaben zum Meldestatus, Aufenthaltsrecht und Asylverfahren.

Die Datenschutzbeauftragten des Bundes und der Länder haben immer wieder darauf hingewiesen, daß die Führung eines derartigen Registers ohne gesetzliche Regelung mit dem vom Grundgesetz Deutschen wie Ausländern gleichermaßen garantierten Recht auf informationelle Selbstbestimmung unvereinbar ist. Sie begrüßen daher, daß mit dem am 02. März 1994 vom Bundeskabinett beschlossenen Entwurf für ein Ausländerzentralregistergesetz eine gesetzliche Grundlage geschaffen werden soll.

Zwar enthält dieser Gesetzentwurf gegenüber früheren Entwürfen eine Reihe datenschutzrechtlicher Verbesserungen, Bedenken bestehen jedoch weiterhin: Die Datenschutzbeauftragten wenden sich insbesondere dagegen, daß das Ausländerzentralregister nicht nur als Informations- und Kommunikationssystem für die mit der Durchführung ausländer- und asylrechtlicher Vorschriften betrauten Behörden dienen, sondern darüber hinaus als Informationsverbund für Aufgaben der Polizei, Strafverfolgungsorgane und Nachrichtendienste zur Verfügung stehen soll.

Die Funktionserweiterung wird deutlich durch die Speicherung von Erkenntnissen der Sicherheitsbehörden zu Ausländern in das Register. So soll der INPOL-Fahndungsbestand des BKA, soweit er Ausschreibungen zur Festnahme und zur Aufenthaltsermittlung von Ausländern enthält, in das Ausländerzentralregister übernommen werden. Gleiches gilt für die vorgesehene Speicherung von Angaben zu Personen, bei denen Anhaltspunkte für den Verdacht bestehten, daß sie im einzelnen bezeichnete Straftaten planen, begehen oder begangen haben. Diese Informationen dienen nicht einem Informationsbedarf zur Erfüllung ausländerbehördlicher Aufgaben, sondern - worauf die Entwurfsbegründung hinweist - der Kriminalitätsbekämpfung. Für diese Zwecke stehen den Sicherheitsbehörden aber eigene Informationssysteme zur Verfügung. Nach Auffassung der Datenschutzbeauftragten dürfen deshalb derartige Erkenntnisse nicht in das Register aufgenommen werden.

Die im Entwurf vorgesehenen Voraussetzungen unter denen u. a. für Polizeibehörden, Staatsanwaltschaften und Nachrichtendienste automatisierte Abrufverfahren eingerichtet werden können, stellen keine wirksamen Vorkehrungen für eine Begrenzung der Abrufe dar. Besonders problematisch ist der geplante automatisierte Zugriff durch die Nachrichtendienste auf einen - wenn auch reduzierten - Datensatz. Für die Dienste ist in den jeweiligen bereichsspezifischen Gesetzen der automatisierte Abruf aus anderen Datenbeständen ausgeschlossen. Die Erforderlichkeit derartiger Abrufe ist in keiner Weise belegt. Die Datenschutzbeauftragten

sprechen sich deshalb dafür aus, zumindest auf den automatisierten Abruf durch Nachrichtendienste zu verzichten.

Anlage 6

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 02. Mai 1994
(bei Stimmenthaltung der Landesbeauftragten Thüringens und Bayerns)

Entwurf der NADIS-Richtlinien vom 02. Mai 1994

Das von den Verfassungsschutzbehörden des Bundes und der Länder betriebene Verbundsystem NADIS-PZD (Nachrichtendienstliches Informationssystem/Personenzentraldatei) ist nach den Vorgaben der in Überarbeitung befindlichen NADIS-Richtlinien und der nunmehr erstellten Dateianordnung als Aktenhinweissystem zu qualifizieren. Die NADIS-Richtlinien und die Dateianordnung haben sich hinsichtlich ihres Regelungsgehaltes an den Bestimmungen der Verfassungsschutzgesetze zu orientieren.

Die Datenschutzbeauftragten des Bundes und der Länder halten den Entwurf der NADIS-Richtlinien und der Dateianordnung für die Personenzentraldatei für zu weitgehend und fordern deshalb:

- Die in der Personenzentraldatei gespeicherten personenbezogenen Daten sind auf das unerläßlich notwendige Maß zu reduzieren. Eine solche automatisierte Datei darf nach den bindenden Vorgaben des Bundesverfassungsschutzgesetzes nur die Daten enthalten, die für das Auffinden der Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind. Eine Erweiterung für andere Identifizierungszwecke scheidet somit aus.

  Die Dateianordnung enthält darüber hinaus Arten von Daten, die über den Zweck einer Aktenhinweisdatei hinausgehen.

- Alle Rechtsvorschriften, die für die an dem zu übermittelnden Datensatz beteiligten Verfassungsschutzbehörden maßgeblich sind, sind zu beachten. Die in dem Entwurf der NADIS-Richtlinien enthaltenen Regelungen für die Übermittlung personenbezogener Daten sehen hingegen vor, daß hierfür ausschließlich das Recht der übermittelnden Stelle gelten soll.

- Die Dauer der Speicherung von Protokolldatenbeständen ist einheitlich zu regeln. Eine Differenzierung, ob die ursprünglich in der Personenzentraldatei erfaßte Information infolge Fristablaufs oder aufgrund einer Einzelfallentscheidung gelöscht wurde, erscheint nicht sachgerecht. Außerdem muß sichergestellt sein, daß Protokolldaten, so wie es die Verfassungsschutzgesetze vorsehen, nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage verwendet werden.

- Die Datenschutzbeauftragten sind im Rahmen der Durchführung und Fortentwicklung des Nachrichtendienstlichen Informationssystems frühzeitig zu unterrichten und zu beteiligen. Dies muß insbesondere bei der Vorbereitung von datenschutzrechtlichen Regelungen gelten.

Anlage 7

Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. August 1994

Vorschlag der Kommission der Europäischen Union für eine Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik (EG-Statistikverordnung)

(KOM(94) 78 endg.; Ratsdok. 5615/94 = BR-Drs. 283/94)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, daß die Europäische Union eine allgemeine Regelung für die Gemeinschaftsstatistik trifft, weisen allerdings darauf-hin, daß die datenschutzrechtliche Entwicklung bei der Europäischen Union mit dem Aufbau der europäischen Statistik keineswegs Schritt gehalten hat.

Sie stellen mit Besorgnis fest, daß der vorliegende Vorschlag einer EG-Statistikverordnung die nationalen datenschutzrechtlichen Grundsätze und wesentliche Standards des Statistikrechts weitgehend nicht berücksichtigt. Sie fordern daher zur Wahrung des Rechts der Betroffenen auf informationelle Selbstbestimmung mit Nachdruck, daß die Bundesregierung ihre Bedenken gegen diesen Vorschlag geltend macht und diese bei den Beratungen auf europäischer Ebene zum Tragen bringt.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen ausdrücklich den Beschluß des Deutschen Bundesrates vom 8. Juli 1994 (BR-Drs. 283/94 - Beschluß -).

Gegen den vorgelegten Vorschlag einer Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik (EG-Statistikverordnung) erheben sie insbesondere die folgenden datenschutzrechtlichen Bedenken:

1. In Art. 1 sollte als die zuständige Gemeinschaftsdienststelle unmißverständlich das Statistische Amt der Europäischen Gemeinschaften (EUROSTAT) bestimmt werden, weil die erforderlichen rechtlichen, administrativen, technischen und organisatorischen Maßnahmen - insbesondere zur Sicherung der Zweckbindung der zu statistischen Zwecken erhobenen Daten sowie zur Wahrung der statistischen Geheimhaltung - bei dieser Stelle bereits aufgrund der EG-Übermittlungsverordnung 1588/90 vom 11. Juni 1990 getroffen werden können. Eine jederzeit revidierbare Organisationsentscheidung der Kommission darüber, welche Dienststelle der Europäischen Union für statistische Aufgaben zuständig ist, birgt dagegen die Gefahr, daß Daten an unterschiedliche Stellen der Kommission zu unterschiedlichen Zwecken übermittelt werden.
   Zugleich sollte EUROSTAT zumindestens einen der Selbständigkeit der Statistischen Ämter in der Bundesrepublik Deutschland vergleichbaren organisationsrechtlichen Status erhalten, der die unter dem Gesichtspunkt der Objektivität und Neutralität gebotenen Eigenständigkeit bei der Aufgabenerfüllung garantiert. Dies könnte anläßlich der für 1996 vorgesehenen Revision des Vertrages über die Europäische Union geschehen.

2. Das mehrjährige statistische Programm sollte nicht wie in Art. 3 vorgesehen von der Kommission beschlossen werden. Die grundlegenden Entscheidungen über die Bürger belastende Datenerhebungen sollten dem Rat mit Zustimmung des Europäischen Parlaments vorbehalten bleiben. Dabei sollte der Planungscharakter des Programms in den Vordergrund gestellt werden.

3. Art. 5 sollte festlegen, daß statistische Einzelmaßnahmen durch einen Rechtsakt gemäß dem Verfahren nach Art. 189 b EG-Vertrag angeordnet werden. Dies gilt auch für die statistische Auswertung von Daten, die bei den administrativen Stellen bereits vorliegen (sog. Sekundärstatistik). Die im Vorschlag vorgesehene generelle Befugnis der Kommission, statistische Einzelmaßnahmen zu regeln, ist viel zu weitgehend.

4. Die in Art. 12 vorgesehene Übertragung der Befugnis zur Organisation der Verbreitung der statistischen Daten auf die Kommission widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag, aus dem folgt, daß grundsätzlich die Mitgliedstaaten nach ihrem nationalen Recht zur Verbreitung der statistischen Daten zuständig sind. Ferner sollte in Art. 12 festgelegt werden, daß an Stellen außerhalb der statistischen Gemeinschaftsdienststelle nur nicht-vertrauliche statistische Daten übermittelt werden dürfen.

5. Der in Art. 13 gegenüber der Definition in der EG-Übermittlungsverordnung 1588/90 neu definierte Begriff "statistische Geheimhaltung" muß präzisiert werden. Dazu gehört insbesondere, daß festgelegt wird, unter welchen Voraussetzungen statistische Daten vertraulich sind und nicht nur als vertraulich gelten. Dies gilt um so mehr, als im Verordnungsvorschlag dieser Begriff nicht nur in Art. 13, sondern auch in Art. 9 Abs. 2 - allerdings mit einem anderen Begriffsinhalt - definiert wird. Der Begriff "statistische Geheimhaltung" sollte an einer Stelle in der Verordnung und so definiert werden, daß er Art. 2 Nr. 1 der EG-Übermittlungsverordnung 1588/90 und damit den derzeit geltenden nationalen Begriffsbestimmungen entspricht. Dies stände auch im Einklang mit dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag.
6. Gemäß dem Grundsatz der Subsidiarität sollte - ebenso wie die Befugnis zur Verbreitung statistischer Ergebnisse (Art. 11 Abs. 1) - auch die Festlegung der Zuständigkeit für die Durchführung der statistischen Einzelmaßnahmen (Art. 7) den Mitgliedstaaten überlassen bleiben.

7. Auch die in Art. 16 vorgesehene generelle Zugangsregelung einzelstaatlicher Stellen und der Gemeinschaftsdienststelle zu Registern der Verwaltung widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag. Dieser gebietet hier, daß - jedenfalls grundsätzlich - die Mitgliedstaaten zu bestimmen haben, in welcher Weise sich die für die Erstellung der Gemeinschaftsstatistiken zuständigen nationalen Stellen Daten beschaffen. Damit ist aber nicht zu vereinbaren, daß auch Stellen der Kommission unmittelbar Zugang zu nationalen Verwaltungsregistern haben sollen.

   Ferner bleibt unklar, ob die nach Art. 16 erhobenen Daten Erhebungs- oder Hilfsmerkmale sein sollen. Im übrigen darf über Art. 16 ein Zugang zu solchen personenbezogenen Daten, die nach nationalem Recht einer besonderen Geheimhaltung, z. B. dem Steuer- oder auch dem Sozialgeheimnis unterliegen, nicht eröffnet werden.

8. Die Regelung des Art. 17 ist mißglückt. Allem Anschein nach soll hier eine weitgehende Ausnahmeregelung von der statistischen Geheimhaltung zugunsten von Forschungsinstituten, einzelner Forscher und von für die Erstellung von Nicht-Gemeinschaftsstatistiken zuständigen Stellen vorgesehen werden, die die Möglichkeit eröffnet, die in diesem Bereich geltenden strengeren nationalen Regelungen zu umgehen. Außerdem würde von der für EUROSTAT geltenden EG-Übermittlungsverordnung 1588/90 abgewichen werden. Art. 17 sollte deshalb so gefaßt werden, daß die nationalen Zugangsregelungen für Einrichtungen mit der Aufgabe der unabhängigen wissenschaftlichen Forschung nicht umgangen werden können.

9. Der Vorschlag der Kommission sieht weder eine alsbaldige Trennung und Aufbewahrung von Erhebungs- und Hilfsmerkmalen noch eine alsbaldige Löschung personenbezogener Hilfsmerkmale vor. In der Bundesrepublik Deutschland dagegen gehören entsprechende Regelungen (vgl. § 12 BStatG) zum Kernbereich des Statistikrechts. Im Volkszählungsurteil hat das Bundesverfassungsgericht ihnen grundrechtssichernde Bedeutung beigemessen.

10. Schließlich fehlt es für die Organe der Europäischen Union noch immer an einer unabhängigen und effektiven Datenschutzkontrollinstanz, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der Europäischen Union in seinen Rechten verletzt zu sein.

Anlage 8

Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27.09.1994

Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen

Angesichts der aktuellen Diskussion über die innere Sicherheit weisen die Datenschutzbeauftragten des Bundes und der Länder darauf hin, daß umfangreiche polizeiliche Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten, insbesondere im technischen Bereich, gesetzlich verankert worden sind.

Zum Kreis der Betroffenen zählen dabei nicht nur Personen, gegen die Verdachtsgründe vorliegen, sondern auch nichtverdächtige Kontakt- und Begleitpersonen und Unbeteiligte, deren Schutz nach Auffassung der Datenschutzbeauftragten besonders wichtig ist.

Vor diesem Hintergrund schlagen die Datenschutzbeauftragten vor, den derzeitigen Erkenntnisstand über die Erforderlichkeit polizeilicher Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten sowie ihre Auswirkungen auf die Rechte der Betroffenen durch folgende Maßnahmen zu verbessern:

1. Die Datenschutzbeauftragten teilen die von einigen Innenministern vertretene Auffassung, daß bloße Angaben über Einsatzzahlen der besonderen Befugnisse zur Datenerhebung nur einen begrenzten Aussagewert haben. Aufschluß über die tatsächliche Praxis, ihre Erforderlichkeit und Verhältnismäßigkeit läßt sich nur durch Überprüfung und Auswertung der einzelnen Einsätze gewinnen. Hierzu müssen unter Beteiligung der Datenschutzbeauftragten und der Wissenschaft, insbesondere der Kriminologie und des Polizeirechts, objektive und nachprüfbare Auswertungskriterien entwickelt werden.

   Die Datenschutzbeauftragten begrüßen daher die Initiative für eine sog. Rechtstatsachensammlung, die Erhebungen zu polizeilichen Ermittlungsmethoden und Eingriffsbefugnissen durchführen soll. Sie schlagen vor, in diese Rechtstatsachensammlung insbesondere Angaben über den Anlaß einer Datenerhebung mit besonderen Mitteln, die Örtlichkeit und die Dauer der Maßnahme, den Umfang der überwachten Gespräche, den betroffenen Personenkreis sowie die Anzahl der ermittelten, verurteilten, aber auch der entlasteten Personen einzubeziehen. Derartige Aufstellungen wären nicht nur für elektronische Überwachungsmethoden, sondern auch für Observationen, den Einsatz verdeckter Ermittler und V-Personen sowie für Rasterfahndungen denkbar.

2. Einige Polizeigesetze verpflichten dazu zu überprüfen, ob es notwendig ist, bestehende Dateien weiterzuführen oder zu ändern. Dabei soll nicht nur darauf eingegangen werden, ob die Anwendungen, d. h. die Dateien, weiterhin erforderlich sind, sondern auch auf ihren Nutzen sowie auf ihre Schwachstellen und Mängel. Ferner sind Vorschläge zu machen, wie festgestellte Defizite beseitigt oder minimiert werden können.

3. Die Datenschutzbeauftragten gehen davon aus, daß sie bei den Überlegungen zur Rechtstatsachensammlung rechtzeitig beteiligt und die jeweiligen Materialien und Zwischenergebnisse mit ihnen erörtert werden.

Anlage 9

Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27.09.1994

Fehlende bereichsspezifische gesetzliche Regelungen bei der Justiz

Obwohl seit dem Volkszählungsurteil des Bundesverfassungsgerichts mehr als 10 Jahre vergangen sind, werden im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet. Stattdessen sind in den letzten Jahren in zunehmendem Maße automatisierte Verfahren neu eingesetzt worden. Die Eingriffe in das Recht auf informationelle Selbstbestimmung stützen die Justizverwaltungen auf die Rechtsprechung des Bundesverfassungsgerichts zum sog. Übergangsbonus.

Die Datenschutzbeauftragten des Bundes und der Länder weisen im Hinblick auf die kommende Legislaturperiode den Bundesgesetzgeber erneut darauf hin, daß gesetzliche Regelungen im Bereich der Justiz überfällig sind. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Der zur Zeit dem Bundesrat vorliegende Entwurf eines Strafverfahrensänderungsgesetzes beispielsweise wird datenschutzrechtlichen Anforderungen in keiner Weise gerecht.

Im Bereich der Justiz fehlen ausreichende gesetzliche Regelungen für die

- Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien,
- Datenerhebung, -verarbeitung und -nutzung im Strafvollzug,
- Übermittlung von Daten aus den bei Gerichten geführten Registern (z.B. Grundbuch) und deren Nutzung durch die Empfänger,
- Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen (Justizmitteilungsgesetz),
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien.

Eine Berufung auf den sog. Übergangsbonus auf unbegrenzte Zeit steht nicht in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts. Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe in der neuen Legislaturperiode unverzüglich bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes des Bürgers entgegenwirken.

Anlage 10

Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28.09.1994

Datenschutzrechtliche Anforderungen an ein Übereinkommen der Mitgliedstaaten der Europäischen Union über die Errichtung eines europäischen Polizeiamtes (Europol)

Die Datenschutzbeauftragten der Länder gehen gemeinsam mit dem Bundesdatenschutzbeauftragten davon aus, daß bei den Verhandlungen mindestens folgende Punkte berücksichtigt werden:

- Das Übereinkommen muß der verfassungsrechtlichen Kompetenzverteilung in Bund und Ländern für die Polizei entsprechen. Die materielle Verantwortung für die Datenverarbeitung muß, soweit die Daten von Landesbehörden erhoben worden sind, weiterhin bei den Ländern liegen. Davon bleiben die Zuständigkeiten und die dazugehörigen Befugnisse des BKA als nationale Stelle für den Informationsverkehr mit EUROPOL unberührt.

- Die Regelungen zur Verarbeitung personenbezogener Daten müssen präzise sein und dem Grundsatz der Verhältnismäßigkeit entsprechen. Beispielsweise erfüllen die in den bisherigen Entwürfen vorgesehenen Befugnisse zur europaweiten Speicherung von Daten unbeteiligter Personen diese Voraussetzungen nicht.

Die Datenschutzbeauftragten erwarten, daß die deutsche Seite eine Klarstellung über die Verantwortung der Länder, zum Beispiel durch eine Protokollerklärung zum EUROPOL-Übereinkommen, trifft.

Anlage 11

Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27.09.1994

Art. 12 Verbrechensbekämpfungsgesetz zur Trennung von Polizei und Nachrichtendiensten

Geheimdienstliche Informationsmacht und polizeiliche Exekutivbefugnisse müssen strikt getrennt bleiben. Die Datenschutzbeauftragten des Bundes und der Länder stellen mit Besorgnis Entwicklungen fest, die die klare Trennungslinie zwischen Nachrichtendiensten und Polizeibehörden weiter zu verwischen drohen. Dies betrifft vor allem den Einsatz des Bundesnachrichtendienstes nach dem Verbrechensbekämpfungsgesetz:

- Der BND erhält danach bei der Fernmeldeaufklärung auch Befugnisse, die auf eine gezielte Erhebung von Daten für polizeiliche Zwecke hinauslaufen können. Deshalb ist bei dem Vollzug des Gesetzes darauf zu achten, daß nicht gezielt Informationen gesammelt werden, die vom Auftrag des BND nicht umfaßt werden.

- Zwischen nachrichtendienstlichen Vorfelderkenntnissen und polizeilichen Zwangsmaßnahmen ist ein Filter erforderlich, der vor allem Unbeteiligte vor überzogenen Belastungen schützt.

Die Datenschutzbeauftragten fordern, für die Zusammenarbeit von Nachrichtendiensten und Polizei in der Durchführung und Gesetzgebung das Trennungsgebot strikt zu beachten. Dies gilt auch bei der Fernmeldeaufklärung des BND. Eine wirksame Kontrolle durch den Datenschutzbeauftragten in diesem sensiblen Bereich ist auch nach der Rechtssprechung des Bundesverfassungsgerichts sicherzustellen.

Anlage 12

Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27.09.1994

Geänderter Vorschlag für eine Europäische Richtlinie zum Datenschutz im ISDN und in Mobilfunknetzen vom 13. Juni 1994 (KOM (94) 128 endg. - COD 288)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, daß die Europäische Kommission mit der Vorlage des geänderten Vorschlags für eine Richtlinie zum Datenschutz im ISDN ihre Absicht bekräftigt hat, unionsweit bereichsspezifische Regelungen für den Datenschutz in Telekommunikationsnetzen zu schaffen. Es kann kein Zweifel daran bestehen, daß die digitalen Telekommunikationsnetze in der Europäischen Union zunehmend zur wichtigsten Infrastruktur für die Verarbeitung personenbezogener Daten werden. Der Regelungsdruck wird erhöht durch die Tatsache, daß die Europäische Union die rechtlichen und technischen Voraussetzungen für die Liberalisierung der Telekommunikationsmärkte in weiten Bereichen bereits geschaffen hat und mehrere Mitgliedsstaaten, darunter Deutschland, derzeit ihr nationales Telekommunikationsrecht auf die Vorgaben der EU umstellen.

Aus diesem Grund sollte der geänderte Vorschlag für eine ISDN-Richtlinie so bald wie möglich vom Ministerrat und vom Europäischen Parlament abschließend beraten werden. Die Bundesregierung sollte die deutsche Ratspräsidentschaft dazu nutzen, den geänderten Vorschlag für eine ISDN-Richtlinie im Rat behandeln zu lassen.

Dabei sollte sich die Bundesregierung insbesondere für folgende Verbesserungen des Richtlinienvorschlags aus datenschutzrechtlicher Sicht einsetzen:

1. Für Telekommunikationsorganisationen und Diensteanbieter müssen die gleichen gemeinschaftsrechtlichen Regelungen zum Datenschutz gelten. Die Verarbeitung personenbezogener Daten durch Diensteanbieter darf nicht privilegiert werden.

2. Die Beschränkung der Datenverarbeitung auf Zwecke der Telekommunikation sollte wieder in die Richtlinie aufgenommen werden. Der allgemeine Zweckbindungsgrundsatz der Datenschutzrichtlinie läßt die Zweckentfremdung schon bei "berechtigten Interessen" der Verarbeiter zu. Das ist angesichts zunehmender Diversifizierung der Aktivitäten von Netzbetreibern und Diensteanbietern eine zu weitgehende Lockerung der Zweckbindung im Telekommunikationsbereich.
3. Das ursprünglich vorgesehene Verbot, personenbezogene Daten zur Erstellung von elektronischen Profilen der Teilnehmer zu nutzen, sollte wieder in die Richtlinie aufgenommen werden.

4. Die Speicherung von Inhaltsdaten nach Beendigung der Übertragung sollte - wie im ursprünglichen Richtlinienentwurf vorgesehen - untersagt werden.

5. Die Vertraulichkeit der Kommunikationsbeziehungen und -inhalte (Fernmeldegeheimnis) sollte - wie es der ursprüngliche Richtlinienvorschlag ebenfalls vorsah - auf Unionsebene garantiert werden.

6. Um eine Harmonisierung des Gemeinschaftsrechts beim Einzelgebührennachweis zu erreichen, sollten konkrete Vorgaben in die Richtlinie aufgenommen werden, z.B. indem den angerufenen Teilnehmern die Aufnahme ihrer Rufnummer in Einzelgebührennachweise freigestellt wird.

7. Im Fall der Anrufweiterschaltung sollte die automatische Information des anrufenden Teilnehmers darüber, daß sein Anruf (z.B. bei einem Arzt) an einen Dritten weitergeschaltet wird, gewährleistet sein.

Die Konferenz begrüßt die im geänderten Vorschlag vorgesehene Kostenfreiheit für die verschiedenen Optionen der Anzeige der Rufnummer des Anrufers und für die Nichtaufnahme von Daten in das Teilnehmerverzeichnis (Telefonbuch).

Diese Vorschläge berücksichtigen das Subsidiaritätsprinzip und beschränken sich auf Änderungen, die zur Gewährleistung der Vertraulichkeit der Kommunikation in der Europäischen Union realisiert werden müssen. Zudem wird die Europäische Union insoweit im Rahmen ihrer ausschließlichen Zuständigkeit tätig. Die Konferenz bittet auch die Entscheidungsträger auf Unionsebene sowie die Datenschutzbehörden der anderen Mitgliedsstaaten, diese Anregungen zu unterstützen.

Anlage 13

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995

Eingeschränkter Zugriff auf Versichertendaten bei landesweiten oder überregionalen gesetzlichen Krankenkassen

Die gesetzlichen Krankenkassen schließen sich zunehmend zu landesweiten oder überregionalen gesetzlichen Krankenkassen zusammen. Es stellt sich daher verstärkt die Frage, welche bzw. wieviele Geschäftsstellen solcher Krankenkassen umfassend auf alle gespeicherten Daten eines Versicherten zugreifen können.

Die Datenschutzbeauftragten halten nur folgendes für vertretbar:

1. Geschäftsstellen einer Krankenkasse können ohne schriftliches Einverständnis des Versicherten nur auf einen "Stammdatensatz" zugreifen. Dieser "Stammdatensatz" darf nur den Namen, das Geburtsdatum, die Anschrift, die Krankenversichertennummer und die betreuende Geschäftsstelle des Versicherten umfassen.

2. Lediglich eine Geschäftsstelle kann umfassend auf den Datensatz eines Versicherten zugreifen, sofern der Versicherte nicht ausdrücklich und eindeutig schriftlich in derartige Zugriffsmöglichkeiten durch weitere Geschäftsstellen eingewilligt hat.

3. Vor der Einwilligung ist der Betroffene umfassend aufzuklären. Die Daten dürfen nur zweckgebunden verwendet werden

Anlage 14

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995

Sozialgesetzbuch VII

Verfassungsgemäßer Datenschutz für Unfallversicherte erforderlich
Durch die Träger der gesetzlichen Unfallversicherung werden oft Daten der Versicherten hinter deren Rücken oder zumindest ohne deren konkrete Kenntnis erhoben und weitergegeben. Der vorliegende Referentenentwurf des Bundesministeriums für Arbeit und Sozialordnung zum Unfallversicherungs-Einordnungsgesetz - SGB VII - sieht dazu keine Änderungen vor.

Aus dem Recht auf informationelle Selbstbestimmung der Versicherten, insbesondere auf Transparenz der einzelnen Verfahrensschritte, ergeben sich mehrere grundlegende Forderungen, die bei einer Überarbeitung des Referentenentwurfes berücksichtigt werden müssen:

1. Auskunftspflicht behandelnder Ärzte gegenüber Unfallversicherungsträgern

Für behandelnde Ärzte sollte eine gesetzliche Auskunftspflicht gegenüber Unfallversicherungsträgern nur festgelegt werden, soweit dies erforderlich ist für eine sachgerechte und schnelle Heilung (§§ 557 Abs. 2 RVO - § 34 Referentenentwurf SGB VII). Die gesetzliche Auskunftspflicht ist daher auf Angaben über die Behandlung und den Zustand des Verletzten zu beschränken. Danach dürfen Vorerkrankungen, die aus Sicht des Arztes mit dem aktuellen Status in keinem Zusammenhang stehen oder keine Bedeutung im Zusammenhang mit dem Arbeitsunfall oder der Berufskrankheit haben, nicht übermittelt werden (Beispiel: Handverletzung und Salmonellenvergiftung).

2. Datenerhebung, -verarbeitung und -nutzung durch Durchgangsärzte und Berufskrankheitenärzte

Soweit von den Unfallversicherungsträgern bestellte Durchgangsärzte personenbezogene Daten über den Unfallverletzten erheben und Unfallversicherungsträgern und anderen Stellen mitteilen, muß dies auf eine normenklare gesetzliche Grundlage gestellt werden; die bisherige Regelung in dem zwischen den Verbänden der Kassenärzte und der Unfallversicherungsträger geschlossenen "Ärzteabkommen" reicht für die damit verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen nicht aus. Entsprechendes gilt für die geplante Einführung eines Berufskrankheitenarztes.

3. Mitteilung personenbezogener Patientendaten durch Unfallversicherungsträger an ärztliche Gutachter

Im Hinblick auf das Recht der Betroffenen, der Bestellung eines bestimmten Gutachters im Einzelfall aus wichtigem Grund - z. B. wegen möglicher Befangenheit - zu widersprechen, haben die Betroffenen ein besonderes berechtigtes Interesse an der Transparenz dieser Datenübermittlungen.

Gesetzlich festzulegen ist daher, daß dem Betroffenen vor Übermittlung seiner Daten an einen Gutachter der Zweck des Gutachtens und die Person des Gutachters unter Hinweis auf sein Widerspruchsrecht nach § 76 Abs. 2 SGB X mitzuteilen sind.

4. Eingriffe der Unfallversicherungsträger und ihrer Verbände in das Recht auf informationelle Selbstbestimmung

Aufgaben der Unfallversicherungsträger und ihrer Verbände und ihre Befugnisse zur Datenerhebung, -verarbeitung und nutzung - einschließlich der Aufbewahrungsfristen - sind differenziert in der verfassungsrechtlich gebotenen Klarheit gesetzlich zu regeln. Der vorliegende Referentenentwurf erscheint in diesem Punkt weitgehend unzureichend. So werden undifferenziert Unfallversicherungsträger und ihre Verbände behandelt, die Fachaufgaben dieser Stellen nicht oder nicht hinreichend deutlich genannt, und andererseits Selbstverständlichkeiten wie das Führen von Dateien über erforderliche Daten aufgeführt. Außerdem beschränkt sich die Regelung auf die Datenverarbeitung in Dateien und übergeht die gerade im Bereich der Berufsgenossenschaften mit Gutachten und ähnlichen Unterlagen stark ausgeprägte Datenverarbeitung in Akten.

Die Zuweisung von Aufgaben und Befugnissen an Verbände der gesetzlichen Unfallversicherung muß zudem wie bei allen anderen Verbänden von Leistungsträgern durch die Einrichtung einer staatlichen Aufsicht ergänzt werden.

Soweit Vorschriften der Unfallversicherungsträger und ihrer Verbände (z. B. Unfallverhütungsvorschriften) durch Regelungen über die Erhebung, Verarbeitung und Nutzung sensibler medizinischer Daten in das Recht auf informationelle Selbstbestimmung eingreifen, sind diese Eingriffe gesetzlich zu regeln.

5. Anzeige eines Berufsunfalls und einer Berufskrankheit

Bei Datenschutzkontrollen der bisherigen Anzeigen von Berufsunfällen und -krankheiten hat sich gezeigt, daß der Umfang der an die verschiedenen Stellen übermittelten Daten zum Teil dem Grundsatz der Verhältnismäßigkeit, insbesondere der Erforderlichkeit nicht Rechnung trägt. Der Inhalt dieser Anzeigen muß an diesen Grundsätzen gemessen neu festgelegt werden.

6. Zentraldateien mehrerer Unfallversicherungsträger oder ihrer Verbände

Zweck und Inhalt zentral geführter Dateien sind in angemessenem Umfang gesetzlich präzise zu regeln. Dasselbe gilt für die Datenverarbeitung und -nutzung sowie die Festlegung der jeweils speichernden Stelle.

Die rechtzeitige Beteiligung des jeweils zuständigen Bundes- oder Landesbeauftragten für den Datenschutz vor Einrichtung einer Zentraldatei ist vorzusehen.

7. Anforderung medizinischer Unterlagen bei anderen Sozialleistungsträgern

Der in § 76 Abs. 2 SGB X vorgesehene Hinweis auf das Widerspruchsrecht gegen die Übermittlung medizinischer Daten geht stets dann ins Leere, wenn bei der speichernden bzw. übermittelnden Stelle kein Verwaltungsverfahren läuft.

Es ist daher festzulegen, daß ein Unfallversicherungsträger vor der Anforderung von Sozialdaten im Sinne des § 76 SGB X bei anderen Sozialleistungsträgern den Versicherten auf dessen Widerspruchsrecht nach § 76 Abs. 2 SGB X gegenüber der übermittelnden Stelle hinzuweisen hat.

8. Akteneinsichtsrecht der Versicherten

Hinsichtlich des gesetzlichen Akteneinsichtsrechts nach § 25 SGB X treten in der Praxis seitens der Unfallversicherungsträger Unsicherheiten auf, ob zum Schutz von Betriebs- und Geschäftsgeheimnissen oder Urheberrechten das Einsichtsrecht beschränkt werden muß. Hierzu ist eine gesetzliche Klarstellung geboten, daß diese Rechte dem Akteneinsichtsrecht nicht entgegenstehen.

Anlage 15

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995

Datenschutz bei elektronischen Mitteilungssystemen

Es ist damit zu rechnen, daß in Zukunft mit Hilfe elektronischer Mitteilungssysteme rechtsverbindliche bedeutsame Informationen und insbesondere personenbezogene Daten über Netze ausgetauscht werden.

Die zunehmende Nutzung von elektronischen Mitteilungssystemen (Electronic-Mail, Dokumentenaustausch über Datenfernübertragung, Message Handling Systems MHS/X.400) hat zur Folge, daß Bedrohungen wie Verlust von Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit verschärft werden, weil Unbefugte Zugriffe auf Daten und Programme erhalten können und die Übertragungswege vom Kommunikationspartner nicht sicher zu kontrollieren sind. Deshalb ist beim Einsatz solcher Systeme das Risikobewußtsein bei den Verantwortlichen sowie den Anwendern zu schärfen. In diesem Zusammenhang gewinnt der Schutz der elektronisch gespeicherten, verarbeiteten und übertragenen Information durch eine Vielzahl umfassender aufeinander abgestimmter Sicherheitsmaßnahmen an Bedeutung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, daß den folgenden Sicherheitsaspekten beim Einsatz von elektronischen Mitteilungssystemen Rechnung getragen wird:

1. Authentizität von Benutzern, Nachrichten und Systemmeldungen

Für den Empfänger einer Nachricht muß jederzeit die Möglichkeit bestehen, anhand bestimmter Kriterien die Authentizität des Absenders, der Nachricht sowie der an ihn gerichteten Systemmeldungen (z. B. Empfangs- und Weiterleitungsbestätigungen, Sendeanforderungen, Teilnehmerkennungen, Teilnehmereinstufungen) zu überprüfen.

2. Vertraulichkeit von übertragenen Daten

Für alle Arten von Daten in elektronischen Mitteilungssystemen - Nachrichten sowie Verkehrs- und Verbindungsdaten - muß die Vertraulichkeit gewahrt bleiben. Sie ist durch geeignete Maßnahmen, z.B. kryptografische Verfahren, sicherzustellen.

3. Integrität von Nachrichten und Meldungen

Es ist zu gewährleisten, daß bei Speicherung und Weiterleitung von Daten keine unbefugte, unerkannte Veränderung erfolgen kann.

4. Fälschungssichere Kommunikationsnachweise

Die für die Anerkennung einer elektronischen Kommunikation erforderlichen fälschungssicheren Sende-, Empfangs- und Übertragungsnachweise müssen dem Anwender auf Wunsch zur Verfügung stehen.

5. Ausschluß von Kommunikationsprofilen

Die Erstellung von Kommunikationsprofilen muß verhindert werden. Gespeicherte Protokollierungsdaten dürfen nur zu Zwecken des Datenschutzes und der Datensicherung (§§ 14 Abs. 4, 31 BDSG bzw. landesgesetzliche Regelungen) verwendet werden.

Empfehlungen zum Einsatz von elektronischen Mitteilungssystemen:

Zum sicheren Einsatz von elektronischen Mitteilungssystemen sind als Grundschutzmaßnahmen folgende Empfehlungen zu beachten.

1. Grundsätzlich sind nur solche Produkte einzusetzen, die die Sicherheitsfunktionen der X.400-Empfehlung aus dem Jahre 1988 erfüllen. Vorhandene Systeme - insbesondere solche, die noch auf Empfehlungen von 1984 basieren -, sollen künftig durch geeignete Zusatzprodukte hinsichtlich ihrer Sicherheit verbessert oder durch neuere Softwareversionen ersetzt werden.

2. Bei Übertragung von personenbezogenen Daten ist eine Verschlüsselung vorzusehen. Die Verschlüsselung der Daten muß mit einem hinreichend sicheren Verschlüsselungsverfahren erfolgen. Neben der Auswahl eines effektiven Verschlüsselungsalgorithmus (z. B. DES, IDEA) muß dabei insbesondere eine ordnungsgemäße Schlüsselerzeugung, -verwaltung und -verteilung gewährleistet sein. Verschlüsselungskomponenten sind durch technische, bauliche und organisatorische Maßnahmen vor dem Zugriff Unbefugter zu schützen.

3. Zur Absicherung der Integrität der Daten sollte auf Verfahren der "elektronischen Unterschrift" zurückgegriffen werden.

4. Nach Möglichkeit ist die Funktion des Systemverwalters von der des Netzwerkverwalters - insbesondere der Verwaltung des elektronischen Mitteilungssystems - aus Sicherheitsgründen zu trennen.

5. Es ist grundsätzlich separat administrierbare Hard- oder Software - z. B. in Form eines Kommunikationsservers - für das elektronische Mitteilungssystem vorzusehen.

6. Bei Verwendungen von öffentlichen Übertragungswegen, sind die vorhandenen Sicherheitsmechanismen dieser Netze z. B. geschlossene Benutzergruppen, Rufnummernidentifikation, Teilnehmerzeichengabe und automatische Rückruffunktion zur Abwehr des Zugriffs durch externe zu nutzen.

7. Zur Beweissicherung einer stattgefunden Kommunikation sollte die eingesetzte Software folgende Funktionen beinhalten:
   - Zustellung/Empfangsnachweise

- Sende/Empfangsübergabenachweise

Anlage 16

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995

Automatische Erhebung von Straßennutzungsgebühren

Gegenwärtig werden Systeme zur automatischen Erhebung von Straßenbenutzungsgebühren in mehreren Versuchsfeldern erprobt. Sie können im Rahmen der weiteren Entwicklung zu zentralen Komponenten umfassender Verkehrstelematiksysteme (z.B. Verkehrsinformation und -leitung) werden.

Mit der Einführung derartiger Verkehrstelematiksysteme besteht die Gefahr, daß personenbezogene Daten über den Aufenthaltsort von Millionen Verkehrsteilnehmern, erhoben und verarbeitet werden. Exakte Bewegungsprofile können dadurch erstellt werden. Damit wären technische Voraussetzungen geschaffen, daß Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Derartige Datensammlungen wären aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil das Grundrecht auf freie Entfaltung der Persönlichkeit auch das Recht umfaßt, sich möglichst frei und unbeobachtet zu bewegen. Vor diesem Hintergrund ist es besonders wichtig, elektronische Mautsysteme datenschutzgerecht auszugestalten. Bei den anstehenden Entscheidungen sind andere Verfahren, wie z. B. die Vignette, einzubeziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, daß der Grundsatz der datenschutzgerechten Ausgestaltung von Systemen zur automatischen Erhebung von Straßenbenutzungsgebühren von allen Beteiligten am Feldversuch auf der BAB A 555 akzeptiert wird. Zur Umsetzung dieses Grundsatzes fordern die Datenschutzbeauftragten:

- Der Grundsatz der "datenfreien Fahrt" muß auch künftig gewährleistet sein. Über Verkehrsteilnehmer, die ordnungsgemäß bezahlen, dürfen keine Daten erhoben oder verarbeitet werden, die die Herstellung eines Personenbezugs ermöglichen. Es sind ausschließlich solche Zahlungsverfahren anzuwenden, bei denen die Abrechnungsdaten nur dezentral beim Verkehrsteilnehmer gespeichert werden. Die Verkehrsteilnehmer dürfen jedoch nicht gezwungen werden, einen lückenlosen Nachweis über ihre Bewegungen zu führen.

- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Möglichkeit einer flächendeckenden Kontrolle ist von vornherein technisch und rechtlich auszuschließen. Die Gebührenkontrolle ist so zu gestalten, daß die Identität des Verkehrsteilnehmers nur dann aufgedeckt wird, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Gebühren nicht entrichtet worden sind.

- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Verkehrsteilnehmer durchschaubar sein. Der Verkehrsteilnehmer muß jederzeit über sein Guthaben, die Abbuchung und den eventuellen Kontrollvorgang informiert sein.

- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, daß sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.

Die hierbei anzuwendenden Verfahren wären gesetzlich abschließend vorzugeben. Dabei ist sicherzustellen, daß anfallende personenbezogene Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen. Ferner ist zu gewährleisten, daß Betreiber derartiger Systeme - unabhängig von ihrer Rechtsform - einer Datenschutzkontrolle nach einheitlichen Kriterien unterliegen. Die Bundesregierung wird aufgefordert, bei der anstehenden internationalen Normierung elektronischer Mautsysteme die datenschutzrechtlichen Anforderungen durchzusetzen.

Anlage 17

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995

Datenschutz bei Wahlen

Bei der Durchführung von Wahlen haben sich Probleme bei der Verarbeitung personenbezogener Daten ergeben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu die folgende Entschließung (bei Gegenstimme von Baden-Württemberg zu Nr. 4.) gefaßt:

1. Durchführung von Wahlstatistiken

Diejenigen Wahlberechtigten, in deren Wahlbezirk eine repräsentative Wahlstatistik durchgeführt werden soll, sind bereits mit der Wahlbenachrichtigung hierüber zu informieren. In allgemeiner Form ist auch im Wahllokal ein gut sichtbarer Hinweis auf die Einbeziehung in die Wahlstatistik anzubringen.

Die Statistik sollte nur in solchen Wahlbezirken durchgeführt werden, in denen jede Geschlechts- und Altersgruppe wenigstens so viele Wahlberechtigte aufweist, daß das Wahlgeheimnis mit Sicherheit gewahrt bleibt. Das Kriterium ist vom Landeswahlleiter vor der Festlegung der Auswahlbezirke zu prüfen. Gegebenenfalls sind ungeeignete Wahlbezirke auszutauschen.

Die Auszählung der Wahlberechtigten und der Wahlbeteiligung auf der Grundlage der Wählerverzeichnisse sollte durch den Wahlvorstand erfolgen, während die statistische Auszählung der Stimmzettel durch die jeweils für die Durchführung der Statistik zuständige Stelle vorzunehmen ist.

Untersuchungen, bei denen Angaben über die Wahlbeteiligung oder die Stimmabgabe aus verschiedenen Wahlen einzelfall- und personenbezogen zusammengeführt werden, gefährden das Wahlgeheimnis und sind daher unzulässig.

2. Auslegung von Wählerverzeichnissen

Durch die Einsicht in das Wählerverzeichnis besteht nach der jetzigen Rechtslage die Gefahr, daß Daten sowohl von Bürgern, über die in Melderegistern eine Auskunftssperre eingetragen ist, als auch von Bürgern, die in einer speziellen sozialen Situation leben (z. B. Justizvollzugsanstalten, Frauenhäuser, psychiatrische Kliniken, Obdachlose), offenbart werden.

Um einerseits die Kontrollmöglichkeit durch die Öffentlichkeit im Vorfeld einer Wahl weiterhin zu gewährleisten, andererseits die datenschutzrechtlichen Belange der genannten Betroffenen zu wahren und dem Mißbrauch einer Adreßrecherche vorzubeugen, fordern die Datenschutzbeauftragten des Bundes und der Länder, daß bei allen Wahlen

- entweder in den öffentlich ausliegenden Wählerverzeichnissen nur Name, Vorname und Geburtsdatum der Wahlberechtigten aufgeführt werden

- oder aber bei Wiedergabe der Adressen im Wählerverzeichnis nur Auskünfte zu bestimmten Personen an den Auskunftssuchenden erteilt werden, wenn er vorher die Adresse dieser Person aufgegeben hat.

Im übrigen sind Daten von Bürgern, für die in Melderegistern eine Auskunftssperre eingetragen ist, im Wählerverzeichnis nicht zu veröffentlichen.

3. Gewinnung von Wahlhelfern

Bei der Gewinnung von Wahlhelfern sind folgende Grundsätze zu beachten:

Es dürfen nur die zur Bestellung erforderlichen Daten, wie Name, Vorname und Wohnanschrift, erhoben werden. Die Betroffenen sind über den Zweck der Datenerhebung und die weitere Datenverarbeitung umfassend zu unterrichten.

Über die Abwicklung der jeweiligen Wahl hinaus dürfen die Daten der Wahlhelfer, soweit sie nicht ausdrücklich widersprochen haben, in einer Wahlhelferdatei nur gespeichert werden, wenn sie dieser Speicherung nicht widersprochen haben. Die Wahlhelfer sind auf ihr Widerspruchsrecht hinzuweisen.

Beschäftigtendaten dürfen nur auf freiwilliger Basis übermittelt werden, sofern nicht eine besondere Rechtsvorschrift die Übermittlung zuläßt. Im Falle der Freiwilligkeit muß es den Beschäftigten möglich sein, selbst die Meldung unmittelbar gegenüber der Wahlbehörde abzugeben. Nach Gründen, die einer Übernahme des Ehrenamtes entgegenstehen, darf erst im förmlichen Verfahren durch die Wahlbehörde gefragt werden.

4. Erteilung von Wahlscheinen

Die in den Wahlordnungen des Bundes und der Länder enthaltene Regelung, nach der die Antragstellung für die Erteilung eines Wahlscheines auf einem Vordruck zu begründen ist und der Grund gegenüber der Gemeinde glaubhaft gemacht werden muß, ist aus datenschutzrechtlicher Sicht unverhältnismäßig. Da sich aus der geforderten Differenzierung der Begründung keine unterschiedlichen Rechtsfolgen ableiten, ist diese entbehrlich. Es genügt in der Antragstellung

eine Erklärung des Wahlberechtigten, daß er am Tag der Wahl aus wichtigem Grund das für ihn zuständige Wahllokal nicht aufsuchen kann.

Anlage 18

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995

Maßhalten beim vorbeugenden personellen Sabotageschutz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, bei Sicherheitsüberprüfungen zum personellen Sabotageschutz Augenmaß zu bewahren. Bei diesen Sicherheitsüberprüfungen werden sensible Daten, z. B. über politische Anschauungen oder Alkoholkonsum, vorbeugend erhoben, also ohne daß der Betroffene dazu Anlaß geboten hätte. Polizei und Verfassungsschutz sind routinemäßig beteiligt. Schon wenn der Betroffene im Verlauf der Überprüfung auch nur in den Verdacht der Unzuverlässigkeit gerät, kann dies bereits erheblichen Einfluß zumindest auf das berufliche Fortkommen nehmen.

Gegenwärtig sind solche Überprüfungen spezialgesetzlich für den Atombereich und für Flughäfen vorgesehen. Das Bundesministerium des Innern will jetzt klären, inwieweit Beschäftigte in anderen Einrichtungen überprüft werden sollen.

Unstreitig können solche Überprüfungen unbescholtener Bürger nur zum Schutz von "lebens- und verteidigungswichtigen Einrichtungen" angemessen sein und nur Personen betreffen, die dort an "sicherheitsempfindlichen Stellen" tätig sind. Als "lebenswichtig" sehen die Innenminister und -senatoren aber bereits Stellen an, "die für das Funktionieren des Gemeinwesens unverzichtbar sind". Damit könnten Beschäftigte in weiten Bereichen des öffentlichen Dienstes und der Wirtschaft mit Sicherheitsüberprüfungen überzogen werden.

Die Datenschutzbeauftragten meinen, daß das Persönlichkeitsrecht hier größere Zurückhaltung gebietet. Die Sicherheitsüberprüfungen müssen auf Bereiche beschränkt bleiben, in denen einer erheblichen Bedrohung für das Leben zahlreicher Menschen vorgebeugt werden muß.

Soweit in solchen Bereichen Sicherheitsüberprüfungen durchgeführt werden sollen, bedarf es einer ebenso klaren gesetzlichen Grundlage, wie bisher im Atomgesetz und im Luftverkehrsgesetz. Die zu schützenden Arten lebens- und verteidigungswichtiger Einrichtungen müssen durch Rechtsvorschrift abschließend festgelegt sein. Dabei sind für die jeweiligen Bereiche angemessene Regelungen zu treffen, die mit Rücksicht auf die Interessen Betroffener folgende allgemeine Grundsätze beachten:

- möglichst klare Vorgaben zur "Sicherheitsempfindlichkeit" in der Vorschrift und exakte Festlegung dieser Stellen durch die zuständige Behörde nach Anhörung der Personalvertretung der einzelnen Einrichtung,
- Zustimmung des Betroffenen als Verfahrensvoraussetzung,
- abschließender Katalog der regelmäßig durchzuführenden Maßnahmen, dabei Beschränkung auf vorhandene Erkenntnisse, keine Ausforschungsermittlungen,
- strenge Zweckbindung und angemessene organisatorische Vorkehrungen zu deren Gewährleistung, insbesondere Trennung von Personalakte,
  eigene Verfahrensrechte des Betroffenen, insbesondere rechtliches Gehör vor ablehnender Entscheidung und aktenkundige Gegendarstellung,
  angemessener Auskunftsanspruch, einschließlich Akteneinsicht,

effektive Datenschutzkontrolle, auch zur Datenverarbeitung in Akten bei nicht-öffentlichen Stellen.

Im Regelfall muß zusätzlich gelten:

> Überprüfung durch die zuständige Aufsichtsbehörde selbst, nicht durch Verfassungsschutzbehörden,
> keine Einbeziehung weiterer Personen (wie Ehegatten usw.).

Ausnahmetatbestände wären - auch zum Verfahren - präzise zu fassen.
Die Praxis der Sicherheitsüberprüfungen zum personellen Sabotageschutz steht in Bund und Ländern vor einer wichtigen Weichenstellung. Sie muß klar und angemessen sein.

Anlage 19

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995

Entwurf eines Gesetzes über das Bundeskriminalamt (BKA-Gesetz) Bundesrats-Drucksache 94/95

Zu den Beratungen des Entwurfs für ein Gesetz über das Bundeskriminalamt erklären die Datenschutzbeauftragten des Bundes und der Länder:

Auch aus Sicht des Datenschutzes ist es zu begrüßen, daß die seit langem überfälligen bereichspezifischen Regelungen zur bundesweiten polizeilichen Datenverarbeitung insbesondere im polizeilichen Informationssystem (INPOL) nunmehr in das Gesetzgebungsverfahren eingebracht werden. Der Gesetzentwurf enthält im Vergleich zu den Vorentwürfen eine Reihe von Vorschriften, die datenschutzrechtlich positiv zu werten sind. Hierzu gehören:

- der Verzicht auf die im Vorentwurf vorgesehenen Befugnisse zur sog. "Feststellung des Anfangsverdachts";

- das Erfordernis der Einwilligung für die Speicherung von Daten über Zeugen und mögliche Opfer;

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

- die Beachtung landesgesetzlicher Löschungsfristen.

  Andererseits begegnet der Gesetzentwurf jedoch nach wie vor gewichtigen Bedenken, da er tiefe Eingriffe in die Rechte von Betroffenen ermöglicht, deren Voraussetzungen und Reichweite unklar oder nicht durch überwiegende Interessen der Allgemeinheit gerechtfertigt sind. Dies gilt insbesondere für

- die Verwendung des Begriffs der Straftaten von erheblicher Bedeutung ohne Definition, um welche Tatbestände es sich handelt, weil damit nicht mehr voraussehbar ist, wann die an diesen Begriff anknüpfenden Eingriffsbefugnisse zur Datenverarbeitung eröffnet sind;

- die Befugnisse der Zentralstelle zu selbständigen Datenerhebungen und Übermittlungen bis hin zum automatisierten Datenverbund mit ausländischen und zwischenstaatlichen Stellen ohne Einvernehmen mit den jeweils verantwortlichen Länderpolizeien;

- die unklare Abgrenzung der Datenverarbeitungsbefugnisse im Hinblick auf die unterschiedlichen Befugnisse zur Strafverfolgung, Gefahrenabwehr, Verhütung von Straftaten und Vorsorge für künftige Strafverfolgung sowie die fehlende klare Zweckbindungs- und Zweckänderungsregelung;

- die Befugnis zur verdeckten Datenerhebung aus Wohnungen ohne eindeutige Begrenzung auf den Schutz gefährdeter Ermittler.

Die Datenschutzbeauftragten fordern den Gesetzgeber auf, die Schwachstellen des Entwurfs auszuräumen. Insbesondere fordern sie klare verfassungskonforme Regelungen zur Auskunftserteilung an Betroffene und der Prüfrechte für INPOL-Daten dahingehend, daß die Datenschutzkontrollrechte bei der datenschutzrechtlichen Verantwortung der Stellen anknüpfen, die die Speicherung im INPOL-System selbst vornehmen oder veranlassen.

Anlage 20

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995

Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich

Bisher ist der Gesetzgeber im Bereich der Justiz den verfassungsrechtlichen Forderungen nach ausreichenden normenklaren Regelungen über die Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien nicht nachgekommen. So enthalten z.B. die bislang bekannt gewordenen Entwürfe zu einem Strafverfahrensänderungsgesetz nur unzureichende Generalklauseln. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erklärt (bei Stimmenthaltung von Hamburg) deshalb:

1. Aufbewahrung, Aussonderung und Vernichtung der Akten und die Speicherung personenbezogener Daten in Dateien im Bereich der Justiz müssen nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil für die Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden gesetzlich geregelt werden, wobei sich die Aufbewahrungsdauer am Recht auf informationelle Selbstbestimmung und am Zweck der Speicherung zu orientieren hat.

   Hierbei hat der Gesetzgeber die grundlegenden Entscheidungen zur Aufbewahrungsdauer selbst zu treffen. Aufgrund einer hinreichend konkreten Verordnungsermächtigung können die Einzelheiten durch Rechtsverordnung bestimmt werden.

2. Die derzeit bestehenden Aufbewahrungsfristen sind konsequent zu vereinfachen und zu verkürzen. Soweit geboten, sind Verkürzungen vorzunehmen.

3. Die derzeit geltende generelle 30jährige Aufbewahrungsfrist für Strafurteile und Strafbefehle mit der Folge der umfassenden Verfügbarkeit der darin enthaltenen Informationen ist nicht angemessen. Bei der Bemessung der Aufbewahrungsfrist von Strafurteilen und Strafbefehlen sowie für die Bestimmung des Zeitpunkts der Einschränkung der Verfügbarkeit ist vielmehr nach Art und Maß der verhängten Sanktionen zu differenzieren.

   Bei der Festlegung des Beginns der Aufbewahrungsfrist sollte - abweichend von der bisherigen Praxis, nach der es auf die Weglegung der Akte ankommt - regelmäßig auf den Zeitpunkt des Eintritts der Rechtskraft der ergangenen gerichtlichen Entscheidung abgestellt werden.

   Ergeht keine rechtskraftfähige Entscheidung, so sollte die Aufbewahrungsfrist mit dem Erlaß der Abschlußverfügung beginnen.

4. Wird der Akteninhalt auf Bild- oder Datenträgern, die an die Stelle der Urschrift treten, aufbewahrt, so sind gleichwohl unterschiedliche Löschungsfristen für einzelne Aktenteile zu beachten. Aus datenschutzrechtlicher Sicht sind Datenträger zu wählen, die eine differenzierte Löschung gewährleisten. Ist bei Altbeständen eine teilweise Aussonderung technisch nicht möglich oder nur mit unverhältnismäßigem Aufwand zu bewerkstelligen, so hat eine Sperrung der an sich auszusondernden Teile zu erfolgen.

5. Sind in einer Akte Daten mehrerer beteiligter Personen gespeichert, so ist eine Sperre hinsichtlich solcher Aktenteile, die einzelne beteiligte Personen betreffen, vorzusehen, wenn diese Aktenteile eigentlich ausgesondert werden müßten, aus praktischen Gründen aber keine Vernichtung erfolgen kann.

6. Bei Freisprüchen und Einstellungen des Verfahrens wegen Wegfalls des Tatverdachts ist dafür Sorge zu tragen, daß ein Zugriff auf die automatisiert gespeicherten Daten nur noch zu Zwecken der Aktenverwaltung erfolgen kann.

7. Für die Daten von Nebenbeteiligten (z. B. Anzeigeerstatter, Geschädigte) ist eine vorzeitige Löschung vorzusehen. Hinsichtlich der Hauptbeteiligten sollte eine Teillöschung der Personen- und Verfahrensdaten stattfinden, sobald die vollständigen Daten zur Durchführung des Verfahrens nicht mehr erforderlich sind.

8. Soweit Daten verschiedener Gerichtszweige oder verschiedener speichernder Stellen in gemeinsamen Systemen verarbeitet werden, ist durch rechtliche, technische und organisatorische Maßnahmen sicherzustellen, daß die Zweckbindung der gespeicherten Daten beachtet wird.

Anlage 21

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995

Anforderungen an den Persönlichkeitsschutz im Medienbereich

Die unabhängige und unzensierte Berichterstattung durch Presse, Rundfunk und Film (Art. 5 Abs. 1 Satz 2 GG) dient der freien individuellen und öffentlichen Meinungsbildung. Das Bundesverfassungsgericht hat die freie Meinungsbildung als Voraussetzung sowohl der Persönlichkeitsentfaltung als auch der demokratischen Ordnung bezeichnet. Insofern besteht ein enger Zusammenhang zwischen der Selbstbestimmung des Einzelnen und der Medienfreiheit.

Die rasante Entwicklung der Medientechnik, die Zunahme interaktiver Teledienste und die verstärkte kommerzielle Nutzung von Pressedatenbanken eröffnen einerseits neue Informationsmöglichkeiten für den Bürger, verschärfen aber die Gefährdungen des Rechts auf informationelle Selbstbestimmung. Diesen Gefährdungen muß der Datenschutz auf rechtlicher und technisch-organisatorischer Ebene angemessen begegnen.

Electronic Publishing und Medienarchive

Neue Formen der Verbreitung von Informationen über Netze und auf elektronischen Datenträgern führen in bisher unbekanntem Maß zu großen Informationsbeständen, in denen potentiell jedermann gezielt auf personenbezogene Daten zugreifen kann. Zudem öffnen Medienarchive, die bislang ausschließlich für journalistische Zwecke genutzt wurden, riesige Datensammlungen für medienfremde Nutzer. In Persönlichkeitsrechte wird dann besonders tief eingegriffen, wenn auch lange zurückliegende Publikationen praktisch von jedermann recherchiert werden können. Damit droht das in verschiedenen Rechtsbereichen vorgesehene "Recht auf Vergessen" wirkungslos zu werden, das z.B. durch die Löschungsvorschriften für das Bundeszentralregister gewährleistet werden soll.

Angesichts dieser Entwicklungen muß die Reichweite der datenschutzrechtlichen Sonderstellung der Medien ("Medienprivileg") neu bestimmt werden. Es ist zumindest gesetzlich klarzustellen, daß die geschäftsmäßige Verwendung personenbezogener Daten außerhalb des eigenen Medienbereichs, insbesondere durch kommerzielle Pressedatenbanken, nicht unter das "Medienprivileg" fällt.

Interaktive Dienste und Mediennutzungsprofile

Auch beim Ausbau neuer digitaler Kommunikationsformen (interaktive Dienste wie z.B. Video on Demand) müssen die Persönlichkeitsrechte der Nutzer gewahrt werden. Dabei ist stärker als bisher von vornherein Wert darauf zu legen, daß datenschutzfreundliche Techniken entwickelt werden und zum Einsatz kommen, bei denen personenbezogene Verbindungs- und Nutzungsdaten erst gar nicht entstehen. Von besonderer Bedeutung sind hier anonyme Zahlverfahren, z.B. Prepaid-Karten, auf denen Informationen über die Nutzung ausschließlich dezentral gespeichert werden.

Entsprechend den Bestimmungen im Bildschirmtextstaatsvertrag und in den neueren Mediengesetzen ist sicherzustellen, daß sich die Erhebung und die Aufzeichnung von Verbindungs- und Abrechnungsdaten auf das erforderliche Maß beschränken. Dieser strikte Verarbeitungsrahmen darf auch nicht dadurch ausgeweitet werden, daß die Nutzung eines Dienstes von der Einwilligung in eine zweckfremde Verwendung der Daten abhängig gemacht wird. Die Länder sollten entsprechende einheitliche Regelungen für alle interaktiven Dienste treffen.

Da es sich bei den angesprochenen Diensten um Bestandteile einer entstehenden globalen Informationsinfrastruktur handelt, wird die Bundesregierung aufgefordert, sich auf internationaler Ebene für entsprechende Regelungen einzusetzen.

Rechte der Betroffenen gegenüber den Medien

Während die von der Berichterstattung Betroffenen - neben dem für alle Bereiche geltenden Gegendarstellungsrecht - gegenüber den öffentlich-rechtlichen und privaten Rundfunkveranstaltern inzwischen weitere elementare Datenschutzrechte besitzen, gibt es gegenüber der Presse keine vergleichbaren Regelungen.

So kann derjenige, der durch die Berichterstattung der Rundfunkveranstalter in seinem Persönlichkeitsrecht beeinträchtigt wird, in den meisten Fällen nach der Publikation Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Gegenüber der Presse hat er kein entsprechendes Auskunftsrecht. Die meisten Rundfunkveranstalter sind - anders als die Presse - zudem verpflichtet, etwaige Gegendarstellungen zu den gespeicherten Daten zu nehmen, auf die sie sich beziehen (Mitspeicherungspflicht). Ein sachlicher Grund für diese Unterscheidungen ist nicht erkennbar.

Das Presserecht sollte insofern der Rechtslage nach dem Rundfunkrecht (z.B. § 41 Abs. 3 BDSG und Art. 17 Abs. 2 ZDF-Staatsvertrag) angeglichen werden.

Gegenüber Pressedatenbanken, die nicht nur dem eigenen internen Gebrauch dienen, sollte der Betroffene darüber hinaus ein Auskunftsrecht bezüglich des zu seiner Person gespeicherten veröffentlichen Materials haben.

Öffentlichkeitsarbeit der Behörden

Personenbezogene Veröffentlichungen von Behörden können das Recht auf informationelle Selbstbestimmung erheblich beeinträchtigen. Das gilt für die Personen, auf die die Aktivitäten der Behörde unmittelbar gerichtet sind, wie auch für andere Verfahrensbeteiligte (wie z. B. Einwender, Opfer von Straftaten, Zeugen) und im besonderen Maße für unbeteiligte Personen aus dem sozialen Umfeld des Betroffenen. Deshalb ist bei der Weitergabe von Daten aus Strafermittlungsverfahren an die Medien besonders zurückhaltend zu verfahren.

Für den Umfang des Anspruchs der Medien auf Weitergabe personenbezogener Daten in Form von Presseerklärungen und Auskünften gibt es keine konkreten gesetzlichen Festlegungen. Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für geboten, daß der Gesetzgeber Kriterien für die Abwägung zwischen dem Persönlichkeitsrecht des Betroffenen und der Freiheit der Berichterstattung durch Rundfunk und Presse deutlicher als bisher festlegt. Dafür kommen die Vorschriften des Landespresserechts, in besonders sensiblen Bereichen aber auch spezialgesetzliche Regelungen wie etwa die Strafprozeßordnung in Betracht.

Gerichtsfernsehen

Die Datenschutzbeauftragten des Bundes und der Länder treten den in jüngster Zeit zunehmend erhobenen Forderungen nach einer Aufhebung des Verbots der Hörfunk- und Fernsehberichterstattung aus Gerichtsverhandlungen entgegen. Insbesondere bei Strafprozessen vor laufenden Mikrofonen und Kameras würde es unweigerlich zu einer gravierenden Beeinträchtigung des Persönlichkeitsrechts der Angeklagten, der Opfer, der Zeugen und ihrer Angehörigen kommen. Selbst mit Einwilligung aller Prozeßbeteiligten darf die Hörfunk- und Fernsehberichterstattung nicht zugelassen werden. Die Gerichtsverhandlung darf nicht zu einem massenmedial vermittelten "modernen Pranger" werden.

Anlage 22

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995

Planungen eines Korruptionsbekämpfungsgesetzes

Derzeit gibt es Vorschläge, die Bekämpfung der Korruption durch Verschärfungen des Strafrechts und des Strafprozeßrechts mit weiteren Eingriffen in das Grundrecht auf informationelle Selbstbestimmung zu organisieren. Ein Beispiel dafür ist der Beschluß des Bundesrates vom 3. November 1995 zur Einbringung eines Korruptionsbekämpfungsgesetzes.

Nach dem vom Bundesrat beschlossenen Gesetzentwurf sollen Bestechlichkeit und Bestechung in den Kreis derjenigen Tatbestände aufgenommen werden, bei deren Verdacht die Überwachung des Fernmeldeverkehrs und der Einsatz technischer Mittel ohne Wissen des Betroffenen (§§ 100a, 100c StPO) angeordnet werden dürfen.

Die Datenschutzbeauftragten weisen demgegenüber darauf hin, daß es vorrangig um Prävention, nicht um Repression geht. Die Datenschutzbeauftragten treten für eine entschlossene und wirksame Bekämpfung der Korruption mit rechtsstaatlichen Mitteln unter strikter Beachtung der Freiheitsrechte ein.

Sie wenden sich zugleich gegen eine Rechtspolitik, welche - noch bevor sie sich darüber im klaren ist, was die bisherigen Verschärfungen und Eingriffe an Vorteilen und an Nachteilen gebracht haben - auf weitere Verschärfungen und Eingriffe setzt.

Gerade gegenüber der Korruption gibt es Möglichkeiten, welche Effektivität versprechen und gleichwohl die Privatsphäre der unbeteiligten und unschuldigen Bürgerinnen und Bürger nicht antasten:

- Rotation derjenigen Mitarbeiterinnen und Mitarbeiter einer Behörde, deren Position und Aufgaben erfahrungsgemäß für Bestechungsversuche in Betracht kommen;
- Vier- und Sechsaugenprinzip bei bestimmten Entscheidungen;
- Trennung von Planung, Überwachung und Ausführung, von Ausschreibung und Vergabe;
- Prüfverfahren und Innenrevision;
- Codes of Conduct (formalisierte "Ethikprogramme") im Bereich der Wirtschaft;
- verbesserte Transparenz von Entscheidungsprozessen in der Verwaltung.

Die in den Gesetzentwürfen vorgesehene weitere Einschränkung von Grundrechten, die mit einer abermaligen Erweiterung der Telefonüberwachung verbunden wäre, ist nur vertretbar, wenn sie nach einer sorgfältigen Güter- und Risikoabwägung zusätzlich zu den oben genannten Verfahrens- und Verhaltensmaßregeln als geeignet und unbedingt erforderlich anzusehen wäre.

Die Datenschutzbeauftragten verlangen, daß vor einer zusätzlichen Aufnahme von Straftatbeständen in den Katalog der Abhörvorschrift des § 100a StPO diese Abwägung durchgeführt wird.

Die Datenschutzbeauftragten fordern weiterhin, daß eine Erweiterung des genannten Straftatenkataloges nur befristet vorgenommen wird, damit sich vor einer Verlängerung die Notwendigkeit stellt, auf der Grundlage einer sorgfältigen Erfolgs- und Effektivitätskontrolle erneut die Erforderlichkeit und Verhältnismäßigkeit einer solchen Erweiterung des Grundrechtseingriffs zu überprüfen.

Die Datenschutzbeauftragten verlangen, daß der Gesetzgeber vor weiteren Eingriffen in Freiheitsrechte eine sorgfältige Güter- und Risikoabwägung vornimmt und dabei insbesondere verantwortlich prüft, ob sich die innenpolitischen Ziele mit Mitteln erreichen lassen, welche die informationelle Selbstbestimmung der Bürgerinnen und Bürger schonen.

Schließlich gibt die anstehende erneute Erweiterung des Katalogs von § 100a StPO Veranlassung, den Umfang der darin genannten Straftaten sobald wie möglich grundlegend zu überprüfen.

Anlage 23

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995

Forderungen an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien (außerhalb der Öffentlichkeitsfahndung der Ermittlungsbehörden)

1. Für die Übermittlung von personenbezogenen Daten durch Justiz und Polizei an die Medien sollte eine bereichsspezifische Rechtsgrundlage geschaffen werden. Die Regelung sollte für den betroffenen Bürger den Umfang des Eingriffs in sein Recht auf informationelle Selbstbestimmung erkennbar machen.

2. Die Übermittlung personenbezogener Daten an die Medien ist nur ausnahmsweise gerechtfertigt, wenn das Verfahren gerade im Hinblick auf die Person des Betroffenen oder die besonderen Umstände der Tat für die Öffentlichkeit von überwiegendem Interesse ist.

3. Bei der Entscheidung, ob und in welchem Umfang personenbezogene Daten an die Medien übermittelt werden, sind die schutzwürdigen Belange der Betroffenen zu berücksichtigen. Dazu zählen insbesondere die privaten und beruflichen Folgen für das Opfer, den Beschuldigten/Angeklagten und deren Angehörige sowie die Schwere, die Umstände und die Folgen des Delikts.

   Bei der Übermittlung von personenbezogenen Daten über Beschuldigte/Angeklagte sind auch der Grad des Tatverdachts und der Stand des Verfahrens zu berücksichtigen. Vor Beginn der öffentlichen Hauptverhandlung ist ein besonders strenger Maßstab an das Vorliegen eines "überwiegenden Interesses" der Öffentlichkeit anzulegen.

   Bis zur rechtskräftigen Verurteilung ist die Unschuldsvermutung zugunsten des Beschuldigten oder Angeklagten zu beachten. Zu unterlassen sind alle Auskünfte oder Erklärungen, die geeignet sind, die Unbefangenheit der Verfahrensbeteiligten zu beeinträchtigen. Akteneinsicht durch Medienvertreter kommt nicht in Betracht.

4. Grundsätzlich sind in Auskünfte und Erklärungen über das Ermittlungs- und Strafverfahren keine Namen und sonstige personenbezogene Angaben, die Opfer von Straftaten, Zeugen, Beschuldigte und Angeklagte bestimmbar machen, aufzunehmen. Vor allem bei Hinweisen auf den Wohnort, das Alter, den Beruf und die familiären Verhältnisse oder sonstigen sozialen Bindungen (z.B. Partei- oder Vereinsmitgliedschaft) ist zu prüfen, inwieweit dadurch eine Identifizierung des Betroffenen möglich wird.

5. Personenbezogene Daten dürfen nicht übermittelt werden, wenn besondere bundesgesetzliche oder landesgesetzliche Verwendungsregelungen entgegenstehen.

6. Ist die Bekanntgabe der Person des Beschuldigten oder Angeklagten wegen des überwiegenden öffentlichen Interesses gerechtfertigt, muß auch bei der Übermittlung sonstiger personenbezogener Daten abgewogen werden, ob diese Informationen für die Berichterstattung über die Tat selbst oder die Hintergründe, die zu der Tat geführt haben, erforderlich sind,

und in welchem Umfang der Betroffene dadurch in seinem Persönlichkeitsrecht beeinträchtigt wird.

7. Die Bekanntgabe von Vorstrafen ist nur ausnahmsweise zulässig. Sie setzt voraus, daß die frühere Verurteilung im Bundeszentralregister noch nicht getilgt und ihre Kenntnis für eine nachvollziehbare Berichterstattung über eine schwerwiegende Straftat - auch unter Berücksichtigung des Persönlichkeitsrechts des Betroffenen und des Resozialisierungsgedankens - erforderlich ist. Besondere Zurückhaltung ist bei Auskünften und Erklärungen über Sachverhalte geboten, die der früheren Verurteilung zugrunde liegen.

8. Wegen des überragenden Schutzes von Minderjährigen und Heranwachsenden ist bei Auskünften und Erklärungen über Verfahren gegen diesen Personenkreis besondere Zurückhaltung hinsichtlich der Bekanntgabe personenbezogener Daten zu wahren.

9. Opfer, Zeugen und Familienangehörige haben in der Regel keine Veranlassung gegeben, daß ihre persönlichen Lebensumstände in der Öffentlichkeit bekannt gemacht werden. Die Übermittlung personenbezogener Daten über diesen Personenkreis an die Medien kommt deshalb grundsätzlich nicht in Betracht.

10. Bildveröffentlichungen greifen wegen der damit verbundenen sozialen Prangerwirkung besonders tief in das Persönlichkeitsrecht des Betroffenen ein. Eine Bildherausgabe kommt daher für Zwecke der Medienberichterstattung nicht in Betracht.

Anlage 24

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995

Datenschutzrechtliche Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 47. Konferenz am 09./10. März 1994 kritisch zum Einsatz von Chipkarten im Gesundheitswesen Stellung genommen. In dem Beschluß wird die Nutzung von Patientenkarten von mehreren Voraussetzungen zur Sicherung des Persönlichkeitsrechts abhängig gemacht.

Seitdem werden in mehreren Ländern Modellversuche und Pilotprojekte durchgeführt. Die Bandbreite reicht

- von allgemeinen Patientenkarten, die an möglichst viele Patienten/Versicherte ausgegeben werden, eine Vielzahl von Krankheitsdaten enthalten und von einem unbestimmten Kreis von Personen und Institutionen des Gesundheitswesens zu vielfältigen Zwecken verwendet werden können (z.B. Vital-Card der AOK Leipzig, Persönliche Patientenkarte Neuwied, BKK-Patientenkarte Berlin)

- bis zu krankheitsspezifischen Karten für bestimmte Patientengruppen mit reduziertem Datensatz und einer Definition der Verwendung (z.B. Dialyse-Card, Diab-Card, Krebsnachsorgekarte, Defi-Card).

Datenschutzrechtlich stellen sich vor allem folgende Probleme:

- Die massenhafte Einführung der Karten erzeugt einen sozialen Druck auf die Betroffenen, sie mitzuführen und vorzuzeigen. Diesen Erwartungen wird sich der Betroffene vielfach nur unter Befremden des Arztes oder sogar der Gefahr, daß dieser die Behandlung ablehnt, verweigern können.

- Die Verwendung von allgemeinen Patientenkarten bringt die Gefahr einer pauschalen Offenbarung von medizinischen Daten mit sich.

- Dem Patienten wird die Last aufgebürdet, für die Sicherheit seiner medizinischen Daten selbst zu sorgen.

Die Datenschutzbeauftragten fordern alle für Kartenprojekte im Gesundheitswesen Verantwortlichen in Politik, Industrie, Ärzteschaft, Wissenschaft und in den Krankenversicherungen auf, das Recht auf informationelle Selbstbestimmung der betroffenen Patienten bzw. Versicherten zu gewährleisten. Die 50. Konferenz hält folgende Voraussetzungen für elementar:

1. Besondere Schutzwürdigkeit medizinischer Daten

Medizinische Daten sind besonders schutzwürdig, unabhängig davon, welche Technologien eingesetzt werden, ob die Patientendaten beim Arzt gespeichert und versandt oder über ein Netz abgerufen werden oder ob der Patient die Daten auf einer Chipkarte bei sich hat. Es handelt sich oftmals um belastende, schicksalhafte Daten. Zudem geht es nicht nur um Daten des Patienten, sondern auch um fremde Einblicke in die ärztliche Tätigkeit.

2. Wirksame Entscheidung der Betroffenen über die Verwendung einer Karte

Die freie Entscheidung der Betroffenen (Patienten/Versicherten), eine Chipkarte zu verwenden, muß gewährleistet sein. Dies umfaßt die Entscheidung,

- ob Daten auf einer Chipkarte gespeichert werden,
- welche der Gesundheitsdaten auf die Karte aufgenommen werden,
- welche Daten auf der Karte wieder gelöscht werden,
- ob die Karte bei einem Arztbesuch bzw. einem Apothekenbesuch vorgelegt wird und
- welche Daten im Einzelfall zugänglich gemacht werden.

Ein Widerruf der Entscheidung muß ohne Nachteile für die Betroffenen möglich sein. Die gleiche Freiheit der Entscheidung für oder gegen die Verwendung der Chipkarte muß für Ärzte und Apotheker gewährleistet sein. Eine wirksame Entscheidung für oder gegen die Verwendung einer Chipkarte setzt eine schriftliche, objektive, vollständige und nachvollziehbare Information über Zweck, Art, Umfang und Beteiligte der Chipkarten-Kommunikation voraus. Das Gesamtkonzept des Chipkarteneinsatzes und der damit verbundenen Datenverarbeitung muß für die Betroffenen überschaubar sein.

Auf der Karte darf nicht der Datensatz der Krankenversichertenkarte nach § 291 Abs. 2 SGB V, insbesondere nicht die Krankenversicherung und die Krankenversicherungsnummer, gespeichert werden, da andernfalls - zumal bei allgemeinen Patientenkarten mit hohem Verbreitungsgrad - die Krankenversichertenkarte verdrängt und deren Nutzungsbeschränkungen umgangen werden.

3. Freiheit der Entscheidung

Die uneingeschränkte Freiheit der Entscheidung der Betroffenen für oder gegen die Verwendung einer Chipkarte muß gewährleistet sein, denn der Einsatz von Chipkarten im Gesundheitswesen führt keineswegs zwangsläufig zu größerer Autonomie der Patienten. Neue Technologien können sich auch als Verführung erweisen, deren Preis erst langfristig erkennbar wird. Die individuelle Entscheidung des Bürgers über die Verarbeitung seiner Daten war und bleibt ein zentrales Recht gegenüber Eingriffen in seine Freiheitssphäre. Mit der Chipkarte können sich jedoch Situationen ergeben, in denen wirkliche Freiheit, tatsächliche Wahlmöglichkeit der Betroffenen nicht mehr gewährleistet sind und durch technische und organisatorische, rechtliche und soziale Rahmenbedingungen wiederhergestellt werden müssen.

Dem Staat kommt hier eine veränderte Rolle zu: Freiheitsrechte nicht einzuschränken, sondern sie zu sichern, wo Entwicklungen des Marktes und der Technologien sowie Gruppeninteressen die Entscheidungsfreiheit des Bürgers bedrohen. Die Technologie selbst kann für die Sicherung der Freiheitsrechte ein wertvolles Hilfsmittel sein. Darüber hinaus kommt der Informiertheit der Betroffenen ein zentraler Stellenwert zu. Ihre Kompetenz zur Entscheidung und zum praktischen Umgang mit der Karte muß gestärkt werden, damit sie auch langfristig die größtmöglichen Chancen haben, ihre Interessen durchzusetzen.

Mit der Ausstellung der Karte dürfen nur die Vorteile verknüpft werden, die sich unmittelbar aus den Nutzungspraktiken der Karte selbst ergeben. Die freie Entscheidung der Betroffenen, eine Karte zu nutzen oder dies abzulehnen, darf nicht durch einen Nutzungszwang oder eine Bevorzugung von Karten-Nutzern (z.B. durch Bonuspunkte) bzw. von Karten-Verweigerern eingeschränkt werden.

4. Keine Verschlechterung der Situation der Betroffenen

Durch die Einführung von Kommunikationssystemen mit Chipkarten dürfen die Betroffenen nicht schlechter gestellt werden als im konventionellen Verfahren. Die medizinische Versorgung, der Schutz der Gesundheitsdaten und die Mitentscheidungsrechte der Betroffenen müssen in Umfang und Qualität erhalten bleiben.

Das therapeutische Verhältnis Arzt/Patient darf sich durch den Einsatz von Chipkarten nicht verschlechtern. Freiheit und Vertrauen innerhalb des Arzt-Patienten-Verhältnisses sowie der Grundsatz der Abschottung der dem Arzt anvertrauten Informationen und der ärztlichen Erkenntnisse nach außen, gegen die Kenntnisnahme durch Dritte, müssen erhalten bleiben. Insbesondere muß der Gesetzgeber sicherstellen, daß die auf der beim Patienten befindlichen Chipkarte gespeicherten medizinischen Daten ebenso gegen Beschlagnahme und unbefugte Kenntnisnahme geschützt sind wie die beim Arzt gespeicherten Daten. Eine Kommunikation unter Vorlage der Karte mit Personen oder Stellen außerhalb des Arzt-Patienten-Verhältnisses, z.B. Arbeitgebern oder Versicherungen, muß vom Gesetzgeber untersagt werden.

Das sich im Gespräch entwickelnde Vertrauensverhältnis zwischen Arzt und Patient darf nicht durch eine Chipkarten-vermittelte Kommunikation verdrängt werden. Verkürzte Darstellungen medizinischer Sachverhalte auf der Chipkarte - z.B. mit Hilfe von Schlüsselbegriffen - dürfen nicht zu einer Minderung der Qualität des therapeutischen Verhältnisses führen; das liegt auch im Interesse des Arztes. Der Patient muß auch weiterhin die Möglichkeit des individuellen Dialogs wählen können. Dies schließt insbesondere die Freiheit des Betroffenen ein, eine Chipkarte im Einzelfall nicht vorzulegen, auf der Chipkarte nur einen begrenzten Datensatz speichern zu lassen oder zu entscheiden, welchem Arzt welche Informationen oder Informationsbereiche offenbart werden. Der Patient darf durch die Ausgestaltung und den Verwendungszusammenhang der Chipkarte nicht zur pauschalen Offenbarung seiner Daten gezwungen sein. So sind Daten auf der Chipkarte so zu ordnen, daß z.B. beim Zahnarzt die gynäkologische Behandlung geheim bleiben kann.

Es darf keine "Einwilligung" in Chipkarten und Chipkartensysteme mit verminderter Datensicherheit geben. Der Gesetzgeber muß die Patienten vor "billigen Gesundheitskarten" ohne ausreichende Sicherung vor einer Nutzung durch Dritte schützen.

5. Sicherstellung der Integrität und Authentizität der Daten

Zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der Daten auf Chipkarten im Gesundheitswesen und zur Differenzierung der Zugriffsmöglichkeiten nach dem Grundsatz der Erforderlichkeit in unterschiedlichen Situationen sind kryptografische Verfahren sowie geeignete Betriebssysteme zur Abschottung unterschiedlicher Anwendungsbereiche nach dem Stand der Technik in Chipkarten und Schreib-/Lese-Terminals zu implementieren. Eine Protokollierung der Lösch- und Schreibvorgänge auf der Karte ist unverzichtbar.

Darüber hinaus ist für das infrastrukturelle Kartenumfeld (Herstellung, Verteilung, Personalisierung,..., Rücknahme) sicherzustellen, daß ausreichende technische und organisatorische Maßnahmen Berücksichtigung finden. Für die zur Erstellung und Personalisierung von Gesundheits-Chipkarten dienenden Systeme sowie die informationstechnischen Systeme und Verfahren, mit denen Daten auf der Chipkarte gelesen, eingetragen, verändert, gelöscht oder verarbeitet werden, muß der gleiche hohe Sicherheitsstandard erreicht werden.

6. Keine neuen zentralen medizinischen Datensammlungen

Der Einsatz von Chipkarten im Gesundheitswesen darf nicht zur Entstehung neuer zentraler Dateien von Patientendaten bei Kassenärztlicher Vereinigung, Krankenkassen, Kartenherstellern oder sonstigen Stellen führen. Dies gilt auch für das Hinterlegen von Sicherungskopien der auf der Karte gespeicherten medizinischen Daten. Es steht in der freien Entscheidung der Betroffenen, ob sie dem Arzt ihres Vertrauens eine umfassende Pflege aller Chipkarten-Daten - einschließlich der Sicherungskopien - übertragen oder nicht.

7. Leserecht des Karteninhabers

Der Karteninhaber muß das Recht und die Möglichkeit haben, seine auf der Chipkarte gespeicherten Daten vollständig zu lesen.

8. Suche nach datenschutzfreundlichen Alternativen

Angesichts der aufgezeigten Gefährdungen der informationellen Selbstbestimmung im Gesundheitswesen muß die Suche nach datenschutzfreundlichen Alternativen zur Chipkarte fortgesetzt werden.

Vorstehende Kriterien sind der Maßstab für die datenschutzrechtliche Bewertung von Projekten für die Einführung von Chipkarten im Gesundheitswesen.

Die Datenschutzbeauftragten von Bund und Ländern fordern die Gesetzgeber auf, die dringend notwendigen Regelungen zur Sicherung der Rechte von Patienten und Ärzten zu schaffen. Ebenso ist durch die Gesetzgeber den Besonderheiten der Datenverarbeitung auf Chipkarten durch bereichsspezifische Regelungen Rechnung zu tragen.

Anlage 25

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995

Weiterentwicklung des Datenschutzes in der Europäischen Union

Die Konferenz der Datenschutzbeauftragten der Europäischen Union hat am 08.09.1995 in Kopenhagen in einer Resolution im Hinblick auf die für 1996 geplante Regierungskonferenz dafür plädiert, anläßlich der Überarbeitung der Unions- und Gemeinschaftsverträge in einen verbindlichen Grundrechtskatalog ein einklagbares europäisches Grundrecht auf Datenschutz aufzunehmen. Die Schaffung rechtsverbindlicher Datenschutzregelungen für die Organe und Einrichtungen der Union sowie die Schaffung einer unabhängigen und effektiven Datenschutzkontrollinstanz der EU werden angemahnt. Dieser Resolution schließt sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an. Sie hält angesichts der fortschreitenden Integration und des zunehmenden Einsatzes von Informations- und Kommunikationstechnologien in der EU eine Weiterentwicklung des Datenschutzes im Rahmen der EU für geboten.

Sie fordert die zuständigen Politiker und insbesondere die Bundesregierung auf, dafür einzutreten, daß im EU-Vertragsrecht ein Grundrecht auf Datenschutz aufgenommen wird, die materiellen Datenschutzregelungen in der EU verbessert werden, das Amt eines Europäischen Datenschutzbeauftragten geschaffen wird sowie eine parlamentarische und richterliche Kontrolle der Datenverarbeitung der im EU-Vertrag vorgesehen Instanzen sichergestellt wird.

Grundrecht auf Datenschutz

Bei einer Weiterentwicklung der Europäischen Union ist es unabdingbar, daß dem Grundrechtsschutz eine angemessene Bedeutung beigemessen wird. Dies sollte dadurch geschehen, daß die Verträge zur Europäischen Union mit einem Grundrechtskatalog ergänzt werden. Mit einer Entschließung vom 10.02.1994 hat das Europäische Parlament einen Entwurf zur Verfassung der Europäischen Union zur Erörterung gestellt, der u.a. folgende Aussagen enthält: "Jeder hat das Recht auf Achtung und Schutz seiner Identität. Die Achtung der Privatsphäre und des Familienlebens, des Ansehens (...) wird gewährleistet".

Die Konferenz der Datenschutzbeauftragten ist mit ihrer Entschließung vom 28.04.1992 dafür eingetreten, daß in das Grundgesetz nach dem Vorbild anderer europäischer Verfassungen ein Grundrecht auf Datenschutz aufgenommen wird. Sie hat hierfür einen Formulierungsvorschlag gemacht. Auf ihren Konferenzen am 16./17.02.1993 und 9./10.03.1994 bekräftigten die Datenschutzbeauftragten des Bundes und der Länder ihre Position. Diese Forderung wurde aber wegen des Nichterreichens der notwendigen qualifizierten Mehrheit durch den Gesetzgeber nicht umgesetzt.

In Wirtschaft, Verwaltung und Gesellschaft der Staaten der EU erhält der Dienstleistungs- und Informationssektor eine zunehmende Bedeutung. Dies hat zur Folge, daß mit hochentwickelten Informationstechnologien von privaten wie von öffentlichen Stellen verstärkt personenbezogene Daten verarbeitet und auch grenzüberschreitend ausgetauscht werden. Diese Entwicklung wird gefördert durch die Privatisierung und den rasanten Ausbau transeuropäischer elektronischer Telekommunikations-Netze. Dadurch gerät das Grundrecht auf informationelle Selbstbestimmung in besonderem Maße auf der überstaatlichen Ebene in Gefahr. Dieser Gefahr kann dadurch entgegengetreten werden, daß in einen in den überarbeiteten EU-Vertrag aufzunehmenden Grundrechtskatalog das Grundrecht auf Datenschutz und zu dessen Konkretisierung ein Recht auf unbeobachtete Telekommunikation aufgenommen werden. Dies hätte folgende positive Auswirkungen:

- Anhand einer ausdrücklichen gemeinsamen Rechtsnorm kann sich eine einheitliche Rechtsprechung zum Datenschutz entwickeln, an die sowohl die EU-Organe wie auch die nationalen Stellen gebunden werden.

- Ein solches Grundrecht wäre die Basis für eine Vereinheitlichung des derzeit noch sehr unterschiedlichen nationalen Datenschutzrechts auf einem hohen Niveau.

- Den Bürgerinnen und Bürgern wird deutlich erkennbar, daß ihnen in einklagbarer Form der Datenschutz in gleicher Weise garantiert wird wie die traditionellen Grundrechte.

- Das grundlegende rechtsstaatliche Prinzip des Datenschutzes wird dauerhaft, auch bei Erweiterung der EU, gesichert.

- Mit der rechtlichen Konkretisierung eines Rechts auf unbeobachtete Telekommunikation würde der zunehmenden Registrierung des Verhaltens der Bürgerinnen und Bürger in der multimedialen Informationsgesellschaft entgegengewirkt und der Schutz des Fernmeldegeheimnisses auch nach dem Abbau der staatlichen Monopole im Sprachtelefondienst sichergestellt.

Materielle Datenschutzregelungen

Mit der kürzlich verabschiedeten EU-Datenschutzrichtlinie wird ein großer Fortschritt für den Datenschutz auf europäischer Ebene erreicht. Dies darf aber nicht den Blick dafür verstellen, daß in einzelnen Bereichen spezifische, dringend nötige Datenschutzregelungen fehlen. Insbesondere sind folgende Bereiche regelungsbedürftig:

- Es bedarf eines für die EU-Institutionen verbindlichen eigenen Datenschutzrechts. Die datenschutzrechtliche Verantwortung der Mitgliedstaaten einschließlich ihrer Datenschutzkontrolle der Übermittlung von Daten an EU-Institutionen bleibt dabei unberührt.

- Die geplante ISDN-Datenschutzrichtlinie darf weder einer völlig falsch verstandenen Subsidiarität zum Opfer fallen noch in unzureichender Form verabschiedet werden.

- Die im Bereich der Statistik bestehenden datenschutzrechtlichen Defizite sind abzubauen.

- Es soll eine Technikfolgenabschätzung bei der Förderung und Einführung neuer Informationstechniken mit Personenbezug durch die EU obligatorisch eingeführt werden.

- In den Bereichen Inneres und Justiz sind aufeinander abgestimmte verbindliche Regelungen mit hohem Datenschutzstandard, die die Datenverarbeitung in Akten und die Sicherung der Datenschutzkontrolle mit umfassen, zu schaffen.

- Es bedarf der Harmonisierung des Arbeitnehmerdatenschutzes auf hohem Niveau in den Staaten der EU.

- Für das Personal der EU-Organe ist der Arbeitnehmerdatenschutz sicherzustellen, was z.B. bei der Durchführung von Sicherheitsüberprüfungen insbesondere unter Beteiligung von Behörden der Heimatstaaten von großer Bedeutung ist.

Es ist zu prüfen, inwieweit Informationszugangsrechte in weiteren Bereichen eingeführt werden sollen.

Europäischer Datenschutzbeauftragter

Die Konferenz der EU-Datenschutzkontrollinstanzen (25./26.05.1994, 08.09.1995) und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (25.08.1994) haben darauf hingewiesen, daß es an einer unabhängigen und effektiven Datenschutzkontrollinstanz fehlt, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der EU in seinen Rechten verletzt zu sein. Aufgabe eines Europäischen Datenschutzbeauftragten sollte die Behandlung aller Datenschutzbelange der EU sein. Dazu gehört nicht nur die Bearbeitung von Betroffeneneingaben, sondern auch die datenschutzrechtliche Beratung der EU-Organe und -Einrichtungen sowie deren anlaßunabhängige Kontrolle, die Begleitung informationstechnischer EU-Projekte und der entsprechenden EU-Normsetzung sowie die Zusammenarbeit mit den nationalen Kontrollinstanzen. Wegen der teilweise anders gelagerten Aufgaben sollen die Funktionen des Europäischen Datenschutzbeauftragten und des Bürgerbeauftragten nach den EG-Verträgen nicht vermengt werden. Die Bundesregierung sollte im Rahmen der Vorbereitung der Regierungskonferenz 1996 darauf hinwirken, daß ein unabhängiger Europäischer Datenschutzbeauftragter in den Verträgen über die Europäische Union institutionell abgesichert wird.

Parlamentarische und richterliche Kontrolle

Bei der Zusammenarbeit der EU-Staaten in den Bereichen Justiz und Inneres muß mit Besorgnis festgestellt werden, daß eine ausreichende parlamentarische und richterliche Kontrolle im EUV derzeit nicht gewährleistet ist. Die geplante Europol-Konvention ist hierfür ein Beispiel. Mit unbestimmten Formulierungen werden einem fast völlig freischwebenden Europäischen Polizeiamt informationelle Befugnisse eingeräumt, einem Amt, das keiner parlamentarischen Verantwortlichkeit und nur einer unzureichenden (teils nur nationalen) Rechtskontrolle unterworfen wird. Zur Wahrung des Datenschutzes bei der Umsetzung gemeinsamer Maßnahmen in den Bereichen Justiz und Inneres muß daher - unbeschadet der Kontrolle durch die nationalen Datenschutzbehörden - auch eine im Rahmen ihrer jeweiligen Zuständigkeiten lückenlose Kontrolle durch die nationalen Parlamente und Gerichte sowie durch das Europäische Parlament und den Europäischen Gerichtshof sichergestellt werden.

Anlage 26

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995

Datenschutz bei der Neuordnung der Telekommunikation (Postreform III)

Mit der Postreform III soll die Neugestaltung des Telekommunikationssektors in Deutschland nach den Vorgaben des Liberalisierungskonzepts der Europäischen Union abgeschlossen werden. Entstehen wird ein riesiger Markt mit einer Vielzahl von großen und kleinen, teilweise auch grenzüberschreitend tätigen Netzbetreibern und Diensteanbietern. Die Akteure auf diesem Telekommunikationsmarkt werden zum größeren Teil als Privatunternehmen operieren, es werden aber auch öffentliche Stellen ihre Leistungen anbieten. Der gesetzgeberische Abschluß der Liberalisierung und der Privatisierung des TK-Sektors wird die rechtliche Grundlage bilden für den endgültigen Eintritt in das Zeitalter von weltweiter Vernetzung, Multimedia und interaktiven Diensten und damit für den rapiden Anstieg des Konsums von Angeboten der Telekommunikation, des interaktiven Rundfunks und der Datenverarbeitung.

Die Konsequenzen sind absehbar: Gegenüber der heutigen Situation werden unvergleichlich mehr personenbezogene Daten durch mehr Stellen registriert und ausgewertet werden. Betroffen sind alle, die fernsehen, telefonieren, fernkopieren, Texte und Dokumente über Datenleitung schicken oder Telebanking oder Teleshopping betreiben. Die Risiken für den Einzelnen durch die vermehrten Möglichkeiten der Verhaltens- und Umfeldkontrolle oder der Ausforschung persönlicher Lebensgewohnheiten und Eigenschaften vergrößern sich entsprechend.

Der vom Bundesministerium für Post und Telekommunikation vorgelegte Referentenentwurf für ein Telekommunikationsgesetz (TKG-E, Stand: 06.10.95) macht es erforderlich, erneut die Realisierung der grundlegenden Rahmenbedingungen für eine datenschutzgerechte Gestaltung der künftigen Telekommunikationslandschaft - soweit die Gesetzgebungskompetenz des Bundes betroffen ist - anzumahnen.

Ein wirksamer Datenschutz muß - wie bereits jetzt gesetzlich fixiert - auch künftig gleichberechtigtes Regulierungsziel neben z.B. der Sicherstellung der flächendeckenden Grundversorgung mit Telekommunikationsdienstleistungen bleiben.

Kundenwünsche nach variablerer und komfortablerer Nutzung der technischen Möglichkeiten werden zunehmen. Gerade deshalb müssen die Prinzipien der Datenvermeidung und der strikten Begrenzung der Datenverarbeitung auf das erforderliche Ausmaß ihren Vorrang bei der Ausgestaltung der kommunikationstechnischen Infrastruktur behalten. Netzbetreiber und Diensteanbieter sollten verpflichtet werden, überall dort, wo dies technisch möglich ist, auch anonyme Zugangs- und Nutzungsformen für ihre Leistungen bereitzustellen. Für eine sichere Datenübertragung sind ohne prohibitive Zusatzkosten wirksame Verschlüsselungsverfahren bereitzustellen.

Das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis müssen für alle Netzbetreiber und Diensteanbieter ungeachtet ihrer Rechtsform und ihrer Kundenstruktur (z.B. sog. Corporate Networks) einheitlich auf einem hohen Niveau gesichert werden. Der bisherige Schutzstandard darf keinesfalls unter den durch die Postreform II erreichten Stand gesenkt werden. Ein hohes Datenschutzniveau ist als Grundversorgung unabdingbar; seine Gewährleistung sollte deshalb Teil der Universaldienstleistung sein. Die in Grundrechte eingreifenden Regelungen sind im Telekommunikationsgesetz selbst und nicht in Verordnungen zu treffen. Die untergesetzlichen, den Datenschutz betreffenden Normen gehören in eine einzige, nicht verstreut in mehrere Verordnungen.

Entscheidend für die Wirksamkeit des Grundrechtsschutzes ist die strikte Einhaltung der Zweckbindung der Verbindungs- und Rechnungsdaten. Das "Feststellen mißbräuchlicher Inanspruchnahme" oder die "bedarfsgerechte Gestaltung" von TK-Leistungen dürfen nicht als Anlaß für eine umfassende Auswertung dieser Angaben oder sogar der Nachrichteninhalte herangezogen werden.

Für den Kunden bzw. Teilnehmer ist es von größter Bedeutung, die Verarbeitungsvorgänge im TK-Bereich überschauen zu können. Er muß auch künftig über die Nutzungsrisiken bestimmter Kommunikationstechniken (z.B. Mobilfunk) ebenso wie über seine Widerspruchsmöglichkeiten umfassend aufgeklärt werden. Keinesfalls darf die Einwilligung des Betroffenen mißbraucht werden um bereichsspezifischer Schutznormen oder effiziente Datensicherungsvorkehrungen zu umgehen.

Um auch und gerade für das besonders schutzwürdige Fernmeldegeheimnis einen durchgängig hohen Schutzstandard zu sichern, braucht es eine unabhängige Kontrolle nach bundesweit einheitlichen Kriterien. Die Zuweisung dieser Überwachungsaufgabe an die im TKG-Entwurf vorgesehene Regulierungsbehörde ist wegen deren mangelhafter Unabhängigkeit und der von ihr wahrzunehmenden Regulierungsaufgaben, die mit Interessenkonflikten verbunden sein werden, nicht akzeptabel.

Deshalb sollte aufgrund seiner langjährigen fachlichen Erfahrung bei der Kontrolle der TELEKOM und seiner umfassenden Querschnittskenntnisse im TK-Bereich der Bundesbeauftragte für den Datenschutz eine zentrale Funktion für die Kontrolle im Telekommunikationsbereich erhalten. Die Aufgaben, die die Landesbeauftragten für den Datenschutz und die Aufsichtsbehörden im Rahmen ihrer Zuständigkeiten erfüllen, sind gesetzlich klar zu regeln.

Die Akzeptanz der Informationsgesellschaft der Zukunft hängt wesentlich ab von der Sicherung des Grundrechts auf unbeobachtete Kommunikation. Das Telekommunikationsgesetz wird einen entscheidenden Baustein für die rechtliche Ausgestaltung der künftigen TK-Infrastruktur bilden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher dazu auf, die von ihr vorgeschlagenen Regelungen im weiteren Gesetzgebungsverfahren zu berücksichtigen und sich für ihre Umsetzung auch auf der europäischen Ebene (z.B. in der ISDN-Richtlinie) einzusetzen.

Anlage 27

Gemeinsame Presseerklärung der Datenschutzbeauftragten des Bundes und der Länder Baden-Württemberg, Berlin, Brandenburg, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen-Anhalt, Schleswig-Holstein

Datenschutz für Strafakten in Gefahr

Kritik von Datenschutzbeauftragten am Entwurf für ein Strafverfahrensänderungsgesetz (StVÄG)

Als unverhältnismäßige Ermächtigung zu Eingriffen in das Persönlichkeitsrecht kritisieren die Datenschutzbeauftragten des Bundes und von 13 Ländern (Baden-Württemberg, Berlin, Brandenburg, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen-Anhalt, Schleswig-Holstein) den Entwurf eines Strafverfahrensänderungsgesetzes 1994 (StVÄG 1994). Dieser von mehreren Landesregierungen (Bayern, Hessen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland und Thüringen) vorgelegte Entwurf soll am kommenden Freitag (14.10.) im Bundesrat beschlossen und dann in den neugewählten Bundestag eingebracht werden.

Der Gesetzentwurf (Bundesrats-Drucks. 620/94 vom 14.06.94) verfehlt seinen Anspruch, dem Volkszählungsurteil des Bundesverfassungsgerichts Rechnung zu tragen und den Schutz der Daten für die an Strafprozessen Beteiligten sicherzustellen; er fällt weit hinter den Standard der allgemeinen Datenschutzgesetze und der Polizeigesetze der Länder zurück. Er dient erkennbar nur dem Ziel, bestehende EDV-Systeme einzelner Bundesländer und überkommene Arbeitsweisen der Justiz formal abzusichern.

Wird der Entwurf unverändert Gesetz, müssen Verdächtige ebenso wie Verbrechensopfer, Tatzeugen und Unbeteiligte damit rechnen, daß Daten über ihre Person aus Strafakten nicht nur an andere Rechtspflegeorgane, sondern an viele andere Behörden weitergegeben werden können. Auch private Personen und Unternehmen, etwa Versicherungen, soll ein nicht näher definiertes "berechtigtes Interesse" zur Auskunft aus oder zur Einsicht in Strafakten legitimieren. Der Entwurf mißachtet die besondere Schutzwürdigkeit gerade des Inhalts von Strafakten; deren Informationen werden teilweise unter Zeugniszwang ermittelt und stammen vielfach aus der Intimsphäre der Betroffenen. Beispiele dafür sind medizinische und psychologische Gutachten oder vertrauliche Abhörprotokolle aus Telefonüberwachungen. Der Gesetzesantrag sieht auch vor, daß Angaben in Justizdateien abweichend vom allgemeinen Datenschutzrecht nur nach dem Zufallsprinzip aus Anlaß einer Einzelfallbearbeitung gelöscht werden sollen.

Die Datenschutzbeauftragten fordern die Landesregierungen auf, dem StVÄG 1994 am kommenden Freitag im Bundesrat nicht zuzustimmen und den Entwurf noch einmal gründlich zu überarbeiten. Die von ihnen wiederholt geäußerten gravierenden Datenschutzbedenken lassen sich nur ausräumen, wenn Verarbeitungsbedingungen und Datenflüsse präzise geregelt und strikt auf die Zwecke des Strafverfahrens begrenzt werden.

Anlage 28

Stellungnahme der Datenschutzbeauftragten der östlichen Bundesländer zu den Entwürfen der Länder-Krebsregisterausführungsgesetze (KrebsRAGe)

(aufgrund der Beratung in Kleinmachnow am 08.09.1995)

1. Die Datenschutzbeauftragten fordern einen Staatsvertrag über solche Regelungen betreffend die Einrichtung und den Betrieb des gemeinsamen großen Krebsregisters, die grundrechtsrelevante Wirkung entfalten. Vor allem ist zu regeln, welche Daten im einzelnen welchem Landesrecht unterliegen und wer für die datenschutzrechtliche Kontrolle zuständig ist.

2. Die Regelungslücke, die der Bundesgesetzgeber in § 8 Abs. 2 KRG hinsichtlich Verstorbener ohne Angehörige gelassen hat, muß geschlossen werden.

3. Hinsichtlich des vorhandenen Datenbestandes fordern die Datenschutzbeauftragten, daß die eine Schlechterstellung bedeutende Sonderregelung der Abs. 2 und 3 des § 5 KrebsRAG bzw. § 6 SächsKrebsRAG entfällt.

   Dies bedeutet, daß § 5 Abs. 2 und 3 (entsprechend für Sachsen § 6 Abs. 2 und 3) dahingehend geändert wird, daß die vorhandenen Datenbestände des ehemaligen Nationalen Krebsregisters der DDR und die weiteren zwischenzeitlichen Meldungen von der Vertrauensstelle zu übernehmen sind.

   Zumindest wäre es aus verfassungsrechtlichen Gründen unerläßlich, daß Abs. 3 folgender Satz angefügt wird:

   > "Vorher dürfen die Daten nach Abs. 1 nicht genutzt werden."

4. Einer rechtlichen Regelung bedürfen insbesondere auch Verfahrensfragen für Forschungsvorhaben. Hierzu kommen - gleichlautende - Rechtsverordnungen der Länder in Betracht.

   Regelungsbedarf besteht darüber hinaus für die organisatorische, räumliche und personelle Trennung der Registerstelle und der Vertrauensstelle sowie für die Dienst-, Rechts- und Fachaufsicht über das gemeinsame Krebsregister durch das Land Berlin.

5. Die Regelung des § 3 Abs. 5 KRG verletzt den Grundsatz der Erforderlichkeit insoweit, als sie eine Übermittlung von Daten vorsieht, die über den Datenkatalog in § 2 Abs. 1 und 2 KRG hinausgeht. Landesrechtlich muß geregelt werden, daß im Rahmen der Übermittlung von Ablichtungen von Leichenschauscheinen nach § 3 Abs. 5 KRG den Vertrauensstellen nur die Daten nach § 2 Abs. 1 und 2 KRG zur Verfügung gestellt werden dürfen.

6. Verfassungsrechtlich bedenklich ist die uneingeschränkte Übertragung der Landesbefugnisse nach § 8 Abs. 1 KRG auf die Senatsverwaltung des Landes Berlin.

7. § 4 KrebsRAG bzw. § 5 sächsische Fassung ist ersatzlos zu streichen, weil die Vorschrift eine Datenübermittlung erlaubt, die vom Gesetzeszweck des KRG nicht gedeckt ist.

8. Gemeldete Daten, die nicht unter das KRG fallen, sind vorbehaltlich archivrechtlicher Anbietungspflichten zu löschen.

6. Abkürzungsverzeichnis

AGE	Automatische Gebührenerhebung auf Autobahnen
AGMN	Arbeitsgemeinschaft in Mecklenburg-Vorpommern tätiger Notärzte e. V.
AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“
ARGUS	Allgemeines Register- und Informationssystem für Gerichte und Staatsanwaltschaften
ASYLON	Asyl Online Datei des Bundesamtes für die Anerkennung ausländischer Flüchtlinge
AZR	Ausländerzentralregister
BDSG	Bundesdatenschutzgesetz
BerRehaG	Berufliches Rehabilitierungsgesetz
BErzGG	Bundeserziehungsgeldgesetz
BfD	Bundesbeauftragter für den Datenschutz
BfV	Bundesamt für Verfassungsschutz
BGH	Bundesgerichtshof
BIOS	Basic Input/Output System
BKA	Bundeskriminalamt
BMJ	Bundesminister der Justiz
BND	Bundesnachrichtendienst
BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
Bundesbeauftragter	Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BVerfSchG	Bundesverfassungsschutzgesetz
BVG	Bundesversorgungsgesetz

BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
CD-ROM	Compact Disc Read Only Memory
DES	Data Encryption Standard
DSB	Datenschutzbeauftragter
DSG MV	Landesdatenschutzgesetz von Mecklenburg-Vorpommern
DV	Datenverarbeitung
DVZ MV GmbH	Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
E.I.S.S.	Europäisches Institut für Systemsicherheit
ED-Behandlung	erkennungsdienstliche Behandlung
EDE	EUROPOL Drogeneinheit
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUROPOL	Europäisches Polizeiamt
EUROPOL-Konvention	Entwurf eines Übereinkommens der Mitgliedstaaten der Europäischen Union über die Errichtung eines Europäischen Polizeiamtes
FH	Fachhochschule
G 10	Gesetz zu Artikel 10 Grundgesetz
GEZ	Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten
HKR	Haushalts-, Kassen- und Rechnungswesen
HR	Hessischer Rundfunk
IITB	Institut für Informationsverarbeitung in Technik und Biologie (jetzt: Fraunhofer-Institut für Informations- und Datenverarbeitung)
IKK	Innungskrankenkasse

IMA-IT	Interministerieller Ausschuß für Informations- und Telekommunikationstechnik
IMK	Innenministerkonferenz
IMPP	Institut für medizinische und pharmazeutische Prüfungsfragen
INPOL	Informationssystem der Polizei
InVeKoS	Integriertes Verwaltungs- und Kontrollsystem
ISDN	Integrated Services Digital Network (digitales diensteintegrierendes Netz)
IT	Informationstechnik
ITSR	IT-Strukturrahmen für die Landesverwaltung Mecklenburg-Vorpommern
IVBB	Informationsverbund Berlin-Bonn
KA-Richtlinien	Dienstanweisung für die Führung von Kriminalakten
KIZ	Kommunikations- und Informationszentrum
KRG	Krebsregistergesetz
KV M-V	Kommunalverfassung für das Land Mecklenburg-Vorpommern
KVA	Kataster- und Vermessungsamt
LAPIS	Landesweites Polizei Informationssystem
LAVINE	Landesdaten-Vermittlungs- und Informationsnetz
LBG M-V	Landesbeamtengesetz Mecklenburg-Vorpommern
LHG M-V	Landeshochschulgesetz Mecklenburg-Vorpommern
LKA	Landeskriminalamt Mecklenburg-Vorpommern
LKHG M-V	Landeskrankenhausgesetz Mecklenburg-Vorpommern
LMG	Landesmeldegesetz
LPrG M-V	Landespressegesetz Mecklenburg-Vorpommern

LStatG M-V	Landesstatistikgesetz Mecklenburg-Vorpommern
LVerfSchG	Landesverfassungsschutzgesetz
MO	Magneto-Optisch
NADIS	Nachrichtendienstliches Informationssystem
NDR	Norddeutscher Rundfunk
ÖGDG MV	Gesetz über den öffentlichen Gesundheitsdienst Mecklenburg-Vorpommern
PC	Personalcomputer
PCMCIA	Personal Computer Memory Card International Association
PED	Polizeiliche Erkenntnisdatei
PersVG	Personalvertretungsgesetz
PERSYS	Personal- und Stellenverwaltungssystem
PIN	Persönliche Identifikationsnummer
PKZ	Personenkennzahl
RKpS MV	Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen in Mecklenburg-Vorpommern
ROD-MO	Rewritable Optical Disc Magneto Optisch
RSA	Verschlüsselungsverfahren (benannt nach den Entwicklern Rivest, Shamir und Adleman)
SchwbG	Schwerbehindertengesetz
SED-UnBerG	SED-Unrechtsbereinigungsgesetz
SGB I	Sozialgesetzbuch Erstes Buch
SGB V	Sozialgesetzbuch Fünftes Buch
SGB VIII	Sozialgesetzbuch Achtes Buch
SGB X	Sozialgesetzbuch Zehntes Buch

SiR MV	Richtlinien für die Sicherheitsüberprüfung von Personen im Rahmen des Geheimnisschutzes
SOG MV	Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern
SPUDOK	Spurendokumentation
SQL	Structured Query Language (Datenbankabfragesprache)
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StrRehaG	Strafrechtliches Rehabilitierungsgesetz
StUG	Stasi-Unterlagen-Gesetz
StVÄG	Strafverfahrensänderungsgesetz
SÜG	Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes
TK-Anlagen	Telekommunikationsanlagen
TLG	Treuhand Liegenschaftsgesellschaft mbH
VEU	Verordnung über die elektronische Unterschrift
WDR	Westdeutscher Rundfunk
WORM	Write Once Read Many
WPflG	Wehrpflichtgesetz
ZEVIS	Zentrales Verkehrsinformationssystem

7. Stichwortverzeichnis

8. Publikationen

Kostenlos beim Landesbeauftragten für den Datenschutz erhältliche Informationsmaterialien:

Der Landesbeauftragte für den Datenschutz
(Faltblatt mit allgemeinen Informationen)

Datenschutz geht jeden an
(Faltblatt des Innenministers MV)

Gesetze und Verordnungen zum Datenschutz
(Gesetzessammlung in Broschürenform)

Informationen zum Datenschutz
(Faltblätter mit aktuellen Informationen)

1. Großer Lauschangriff
2. Datenschutz und Personalcomputer
3. Chipkarte
4. Patientenakte
5. Datenschutz und Verfassungsschutz
6. Datenschutz und Personen-Identifikation
7. Datenschutz und Telefax
8. Adreßbücher
9. Datenmißbrauch
10. Schutz persönlicher Daten
11. Autobahngebühren im Blickfeld
12. Das ISDN-Netz
13. Freiwillige Patienten-Chipkarten
14. Datenschutz in der Schule
15. Umgang mit Sozialdaten
16. Personenbezogene Daten in der Forschung
17. Technikfolgenabschätzung
18. Sicherheit der Informationstechnik
19. Personalakten und Personalaktendaten
20. Statistische Erhebungen

Tätigkeitsberichte *(in Broschürenform)*

1. Tätigkeitsbericht für den Zeitraum 1992/93

Informationen des Bundesbeauftragten für den Datenschutz
(in Broschürenform)

- BfD - INFO 1 - Bundesdatenschutzgesetz
- BfD - INFO 2 - Der Bürger und seine Daten
- BfD - INFO 3 - Schutz der Sozialdaten

Handreichungen *(in Form von Kopien)*

- Hinweise zu den Aufgaben eines internen Datenschutzbeauftragten öffentlicher Stellen
- Orientierungshilfe "Forderung an Wartung und Fernwartung von DV-Anlagen"
- Hinweise zur Führung von Dateibeschreibung und Geräteverzeichnis
- Organisationshilfe zur Vernichtung von Schriftgut
- Orientierungshilfe "Datenschutzrechtliche Protokollierung beim Betrieb informationstechnischer Systeme (IT-Systeme)"
- Orientierungshilfe "Datenschutzrechtliche Aspekte beim Einsatz optischer Datenspeicherung"
- Orientierungshilfe "Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet"