Der Landesbeauftragte für den Datenschutz
Mecklenburg-Vorpommern

Sechster Tätigkeitsbericht

2002/2003

Herausgeber: Der Landesbeauftragte für den Datenschutz
Mecklenburg-Vorpommern
Schloss Schwerin
19053 Schwerin
Telefon: (03 85) 5 94 94-0
Telefax: (03 85) 5 94 94-58
E-Mail: datenschutz@mvnet.de
Internet: http://www.lfd.m-v.de

Druck: cw Obotritendruck GmbH

Vorwort

Das Datenschutzgesetz von Mecklenburg-Vorpommern sieht vor, dass der Landesbeauftragte für den Datenschutz dem Landtag und der Landesregierung für jeweils zwei Kalenderjahre einen Bericht über seine Tätigkeit vorlegt. Dieser Sechste Tätigkeitsbericht umfasst den Zeitraum vom 1. Januar 2002 bis zum 31. Dezember 2003.

Wie in den Jahren zuvor habe ich Vorgänge ausgewählt, die einen Gesamteindruck von der vielseitigen Tätigkeit meiner Behörde vermitteln und deren Kenntnis bei der Umsetzung der Datenschutzvorschriften hilfreich sein kann. Einige Beiträge schließen an Sachverhalte aus den letzten Berichten an. Insofern könnte es nützlich sein, in dem einen oder anderen Fall noch einmal auf diese Berichte zurückzugreifen.

Mit Ablauf des Jahres 2004 geht meine zweite Amtszeit zu Ende. Eine nochmalige Wiederwahl sieht das Gesetz nicht vor. Demzufolge ist der vorliegende Sechste Tätigkeitsbericht gleichzeitig mein letzter.

Für die konstruktive und sachorientierte Zusammenarbeit danke ich den Abgeordneten unseres Landtages und den Beschäftigten in den öffentlichen Stellen unseres Landes. Ein weiterer Dank gilt meinen Amtskolleginnen und -kollegen im Bund und in den Ländern für ein hilfreiches, angenehmes und gemeinsames Handeln im Interesse des Datenschutzes. Insbesondere danke ich jedoch meinen Mitarbeiterinnen und Mitarbeitern für ihre engagierte, zuverlässige und sachkundige Arbeit in den vergangenen Jahren.

Dr. Werner Kessel
Landesbeauftragter für den Datenschutz
Mecklenburg-Vorpommern

INHALTSVERZEICHNIS

1. SITUATION DES DATENSCHUTZES

Im Datenschutz lassen sich zwei gegenläufige Trends erkennen: Einerseits sind die Bürger sensibler geworden, wenn sie persönliche Daten für verschiedene Zwecke zur Verfügung stellen sollen, und auch öffentliche Stellen gehen zunehmend sorgsamer mit personenbezogenen Daten um. Andererseits schränken die Gesetzgeber im Bund und in den Ländern das Grundrecht der Bürger auf informationelle Selbstbestimmung durch immer neue Rechtsvorschriften im Sicherheitsbereich ständig weiter ein. Bedenklich ist vor allem, mit welcher Leichtigkeit und Geschwindigkeit das geschieht. Oft reicht es schon aus zu argumentieren, dass die neue Vorschrift der Verbrechensbekämpfung dient und deshalb wohl niemand etwas dagegen einwenden könne – auch die Datenschützer nicht. Natürlich wissen auch Datenschützer, dass nicht nur sie, sondern auch die Sicherheitsbehörden letzten Endes dem Bürger dienen. Dabei darf aber nicht aus dem Blickfeld geraten, dass jede Erweiterung von Befugnissen der Sicherheitsbehörden die Freiheitsrechte des Individuums und damit auch das Grundrecht auf informationelle Selbstbestimmung einschränkt. Es ist die verfassungsrechtlich festgeschriebene Aufgabe der Datenschützer, dafür zu sorgen, dass dieses Grundrecht nicht irgendwann der Beliebigkeit anheim fällt und nur noch auf dem Papier steht.

In diesem Spannungsfeld hat der Gesetzgeber vor jedem geplanten Eingriff in das Grundrecht auf informationelle Selbstbestimmung gewissenhaft zu prüfen, ob die neuen Befugnisse überhaupt geeignet und tatsächlich erforderlich sind, um das gewünschte Ziel zu erreichen. Weiterhin muss er sorgfältig abwägen, ob die Einschränkungen der Rechte unbescholtener Bürger dem erhofften Effekt der neuen Befugnisse auch wirklich angemessen sind. Es reicht keinesfalls aus, einfach festzustellen, dass die Maßnahme der Verbrechensbekämpfung dient und der Polizei oder dem Verfassungsschutz bei deren Arbeit hilfreich sein kann.

Ich will hier angesichts der schon heute vorhandenen technischen Möglichkeiten nicht ausmalen, wohin wir in kürzester Zeit gelangen würden, wenn wir neue Grundrechtseinschränkungen nur noch unter dem Aspekt prüfen würden, ob sie der Sicherheit dienen. Natürlich kann niemand vorher genau wissen, ob eine bestimmte Maßnahme auch tatsächlich den Erfolg bringt, den man sich von ihr erhofft. Deshalb ist es gut, wenn der Gesetzgeber den Mut aufbringt, diese Zweifel erkennen zu lassen, indem solche Maßnahmen beispielsweise zeitlich begrenzt und evaluiert werden. In einigen Gesetzen, die derartige Grundrechtseinschränkungen mit sich bringen, ist dies bereits so praktiziert worden (Bundesverfassungsschutzgesetz, BND-Gesetz, G10-Gesetz, Sicherheitsüberprüfungsgesetz).

Unangebracht sind jedenfalls laute Töne oder Meldungen von Erfolgen, die bei genauerem Betrachten durchaus fragwürdig sind. So wurden beispielsweise bei der nach dem 11. September 2001 eilig durchgeführten Rasterfahndung schon im Vorfeld Ergebnisse verkündet und Befunde recht einseitig interpretiert. In unserem Land wurden von nahe-

zu 10.000 Einwohnern personenbezogene Daten erhoben und gespeichert. Im Ergebnis des bundesweiten Abgleichs wurde keine in Mecklenburg-Vorpommern lebende verdächtige Person festgestellt. Einige werten dieses Ergebnis als uneingeschränkt positiv. Bei genauerer Betrachtung jedoch ist es nichts anderes als der negative Befund eines großen Experimentes. Negative Befunde lassen sich aber prinzipiell nicht eindeutig interpretieren. Neben der Vermutung, dass sich unter den Überprüften tatsächlich kein Terrorist befindet, wäre es ja immerhin auch denkbar, dass die Rasterfahndung grundsätzlich nicht geeignet war, ihn zu entdecken. Und selbst wenn man unterstellt, dass die Rasterfahndung eine geeignete Methode ist, wäre denkbar, dass sie nicht sorgfältig genug beziehungsweise nicht mit der gebotenen Genauigkeit angewendet wurde. Zweifel sind nach dem Ergebnis also durchaus angebracht. Dabei kann und darf auch nicht außer Acht gelassen werden, dass bei dieser Maßnahme erheblich in das Grundrecht auf informationelle Selbstbestimmung einer Vielzahl von Unverdächtigen eingegriffen wurde (siehe Punkt 2.3.3).

Recht widersprüchlich muten die hektischen Aktivitäten des Gesetzgebers zur Befugniserweiterung bei der Verbrechensbekämpfung an, wenn man sie mit den Inaktivitäten der Verantwortlichen bei wichtigen technischen Ausstattungen der Polizei vergleicht. Nach jahrelangen Debatten ist es bis heute nicht gelungen, das hoffnungslos veraltete, analoge Funksystem der Polizei durch moderne, sichere Digitalfunktechnik zu ersetzen. Nach wie vor ist die Vertraulichkeit personenbezogener Daten von Bürgern nicht gewährleistet. Und natürlich stellt die extrem „abhörfreundliche“ Analogtechnik die Erfolge der polizeilichen Arbeit in Frage. Seit mehr als einem Jahrzehnt besteht hier unverändert dringender Handlungsbedarf (siehe Punkt 2.20.6).

Unser Landesdatenschutzgesetz ist im Berichtszeitraum umfassend novelliert worden (siehe Punkt 2.2.2). Damit hat auch in unserem Land die Modernisierung des Datenschutzrechtes begonnen. So sind beispielsweise die seit langem überholten Vorschriften zu technischen und organisatorischen Maßnahmen durch technikunabhängige Sicherheitsziele ersetzt worden. Das novellierte Gesetz verwendet darüber hinaus erstmalig die Begriffe Pseudonymisierung und Verschlüsselung und enthält nunmehr moderne Regelungen zur Datenvermeidung und zu Chipkarten.

Dennoch wird der Datenschutz auch weiterhin häufig als Störfaktor betrachtet. So wird ihm beispielsweise gelegentlich unterstellt, er stünde dem Bürokratieabbau entgegen. Ich habe im Rahmen meiner praktischen Tätigkeit jedoch festgestellt, dass gerade der Datenschutz in einer modernen Informations- und Kommunikationsgesellschaft maßgeblich dazu beitragen kann, bürokratische Hürden zu überwinden. Folgende Beispiele sollen dies veranschaulichen:

Wenn alle öffentlichen Stellen das jetzt im Landesdatenschutzgesetz normierte Prinzip der Datensparsamkeit berücksichtigen und somit nur noch die Daten verarbeiten würden, die sie zur Erfüllung ihrer gesetzlich vorgeschriebenen Aufgaben auch benötigen, kämen wir mit dem Bürokratieabbau schon ein gutes Stück voran. Dazu gehört beispielsweise auch, keine Daten auf Vorrat zu erheben und sie so zu verarbeiten, dass sie ohne größeren Aufwand gelöscht werden können, wenn die Aufgabe erledigt ist. Darüber hinaus muss der gesamte Prozess der Datenverarbeitung vom Erheben bis zum Löschen bereits bei der Planung und bei der Ausschreibung von Leistungen betrachtet werden, um zeitlich aufwändige und kostenintensive Nacharbeiten zu vermeiden.

Bürokratieabbau heißt in diesem Zusammenhang auch, die Barrieren zwischen Bürger und Verwaltung aus dem Weg zu räumen, um unnötigen Aufwand und Ärger auf beiden Seiten zu vermeiden. In der Datenschutzpraxis geht es darum, die Datenverarbeitung für den Betroffenen transparent zu machen. Die vom Gesetzgeber geregelten Auskunfts- und Einsichtsrechte gehören ebenso dazu wie die vorgesehenen Aufklärungspflichten über die Datenverarbeitung. Bedauerlicherweise müssen sich immer wieder Bürger an mich wenden, weil ihnen Informationen vorenthalten wurden und sie dadurch misstrauisch gegenüber der Verwaltung geworden sind. Von mir daraufhin eingeleitete Prüfungen zeigten, dass die öffentlichen Stellen sich bei der Verarbeitung der personenbezogenen Daten zumeist an die gesetzlichen Bestimmungen gehalten haben und „lediglich“ ihre Auskunfts- und Informationspflichten nicht wahrnehmen. Man könnte sich zwar darüber freuen, dass der datenschutzrechtliche Mangel sich auf diesen Aspekt beschränkt. Doch wäre die öffentliche Stelle gleich ihrer Auskunfts- und Informationspflicht nachgekommen, so hätte eine – unter Umständen für beide Seiten aufwändige – datenschutzrechtliche Prüfung vermieden und die so gesparte Zeit anderweitig genutzt werden können.

Vieles ließe sich bei etwas gutem Willen datenschutzfreundlicher und damit gleichzeitig unbürokratisch gestalten – zum Beispiel der Rundfunkgebühreneinzug. Die Gebühreneinzugszentrale (GEZ) erhebt für die Rundfunkanstalten die Rundfunkgebühr. Um Gebührengerechtigkeit herzustellen und die Einnahmesituation zu verbessern, erhält die GEZ von den Meldebehörden bei An- und Abmeldungen sowie in Todesfällen die Meldedaten der Betroffenen. Zusätzlich erhält sie Daten aus privaten Quellen. Dadurch entsteht bei der GEZ ein umfangreiches, zentrales Einwohnermelderegister – allerdings mit reduziertem Datensatz, weil für den Gebühreneinzug nicht alle Meldedaten benötigt werden. Die Landesrundfunkanstalten beschäftigen auch Rundfunkgebührenbeauftragte, die bisher nicht angemeldete Rundfunkteilnehmer ermitteln sollen. Insgesamt handelt es sich hierbei um ein sehr aufwändiges Verfahren, bei dem auch eine Vielzahl personenbezogener Daten von Betroffenen verarbeitet werden (siehe Punkt 2.6.4).

Schon vor einigen Jahren hatte ich daher vorgeschlagen, die Rundfunkgebühren von den Zahlungspflichtigen durch die Stellen zu erheben, die ohnehin schon über die erforderlichen Daten verfügen. Dabei sollten alle Bürger zunächst grundsätzlich zur Zahlung verpflichtet werden. Diejenigen, die sich aus bestimmten Gründen von der Zahlung befreien lassen können, müssten einen entsprechenden Antrag stellen. Die Landesregierung hatte seinerzeit meinen Vorschlag geprüft und im Juli 1996 hierzu mitgeteilt, dass sich dieser kurzfristig nicht umsetzen ließe, sie den Gedanken aber langfristig weiter verfolgen werde. Bis heute hat sich jedoch nichts geändert. Auch im Rahmen der geplanten Neuordnung der Rundfunkfinanzierung wurde dieser Vorschlag bisher nicht aufgegriffen. Und das, obwohl sich die Gebührengerechtigkeit für die Bürger zweifellos verbessern würde, der öffentlich-rechtliche Rundfunk höhere Einnahmen hätte und er zusätzlich seine Kosten erheblich reduzieren könnte. Nicht der Datenschutz verhindert hier die Vereinfachung im Sinne einer bürgerfreundlichen Lösung, sondern die Bürokratie allein ist es wohl, die ihren Abbau verhindert.

Ein weiteres Beispiel für Bürokratieabbau ist im Landesdatenschutzgesetz selbst zu finden. Mit den neuen Regelungen zum Datenschutzaudit soll die Beschaffung von Hard- und Software wesentlich vereinfacht werden. Es ist bisher mit erheblichem Aufwand verbunden, die Angebote verschiedener Hersteller zu prüfen, wenn es beispielsweise um die Anschaffung eines bestimmten IT-Produktes zur automatisierten Verarbeitung personenbezogener Daten geht. Der Aufwand könnte aber beträchtlich gesenkt werden, wenn unabhängige Stellen bereits vorab und allgemein gültig geprüft hätten, ob dieses Produkt bestimmte, vorher definierte Anforderungen erfüllt. Das daraufhin erteilte Gütesiegel wäre ein entscheidendes Auswahlkriterium und würde die Beschaffung wesentlich vereinfachen. Das Landesdatenschutzgesetz sieht mit dem Datenschutzaudit genau diesen Weg vor. Es bedarf lediglich einer Rechtsverordnung, die alle erforderlichen Details regelt. Leider hat unsere Landesregierung bisher diese Verordnung immer noch nicht erlassen (siehe dazu Punkt 2.18.1).

„Sie sind doch der Landesdatenschutzbeauftragte, warum sind Sie dann nicht für alle Datenschutzfragen im Land zuständig?“ – mit dieser vorwurfsvollen Frage erinnern mich Bürger immer häufiger an eine hervorragende Möglichkeit, Bürokratie abzubauen. Gegenwärtig sind in unserem Land die Zuständigkeiten für den Datenschutz geteilt – in den öffentlichen und in den nichtöffentlichen Bereich. Die für die Privatwirtschaft zuständige Datenschutzaufsichtsbehörde ist beim Innenminister angesiedelt. Das Kontrollrecht des Landesbeauftragten für den Datenschutz beschränkt sich hingegen auf den öffentlichen Bereich. Dies ist für den Rat suchenden Bürger eine verwirrende Angelegenheit. Denn selbst für Fachleute ist es nicht immer leicht zu unterscheiden, ob eine Institution

dem öffentlichen Bereich zuzuordnen ist oder nicht. Deshalb ist es gut, dass der Gesetzgeber dies demnächst ändern will. Ein erster Referentenentwurf, der die Zuständigkeit für beide Bereiche dem Landesbeauftragten für den Datenschutz überträgt, liegt bereits vor. So kann der Bürger künftig unbürokratisch und bürgerfreundlich „Datenschutz aus einer Hand“ erhalten.

2. SORGEN DER BÜRGER, EINZELFÄLLE, BERATUNGEN, KONTROLLEN, STELLUNGNAHMEN, GESETZE, VERORDNUNGEN

2.1 Rechtswesen

2.1.1 EUROJUST

Der Europäische Rat hat am 28. Februar 2002 die Errichtung von EUROJUST beschlossen, um die justizielle Zusammenarbeit in Europa zu verbessern. EUROJUST soll die Ermittlungsverfahren und Strafverfolgungsmaßnahmen im Bereich der schweren organisierten Kriminalität koordinieren, die das Gebiet mehrerer Mitgliedsstaaten betreffen. Eine Vorläuferstelle PRO-EUROJUST hatte bereits im März 2001 ihre Tätigkeit aufgenommen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte in einer Entschließung vom Oktober 2001 die datenschutzrechtlichen Anforderungen an EUROJUST benannt (siehe Fünfter Tätigkeitsbericht, Anlage 22), die teilweise berücksichtigt wurden.

Die Bundesregierung hat den Entwurf eines EUROJUST-Gesetzes vom 15. August 2003 auf den parlamentarischen Weg gebracht, um das nationale Recht entsprechend anzupassen (BR-Drs. 545/03). Die von den Datenschutzbeauftragten angeregten datenschutzrechtlichen Klarstellungen haben im Gesetzentwurf weitgehend Eingang gefunden.

Der Gesetzentwurf wird derzeit noch in den parlamentarischen Gremien beraten.

2.1.2 Fahndungsausschreibung im INPOL nicht rechtzeitig gelöscht

Der Bundesbeauftragte für den Datenschutz übersandte mir eine Petition zur datenschutzrechtlichen Prüfung. Der Petent hatte beim Bundesverwaltungsamt gemäß § 34 Ausländerzentralregistergesetz um Auskunft über die zu seiner Person im Ausländerzentralregister gespeicherten Daten gebeten. Die Auskunft enthielt den Hinweis, dass auch Daten von ihm gespeichert werden, die ihm aus gesetzlichen Gründen nicht mitgeteilt werden können. Der Petent hatte den Bundesbeauftragten für den Datenschutz gebeten zu bewerten, ob die Auskunftsverweigerung rechtmäßig ist. Da die Verweigerung auf einer Fahndungsausschreibung beruhte, die eine Staatsanwaltschaft unseres Landes veranlasst hatte, habe ich diesen Teilaspekt geprüft.

Die Fahndungsausschreibung beruhte auf einem Haftbefehl, da der Petent seinerzeit eine Ersatzfreiheitsstrafe antreten sollte. Die Ausschreibung war daher ursprünglich recht-

mäßig. Inzwischen war jedoch die Vollstreckung verjährt. Dabei war über einen Zeitraum von mehr als einem Jahr versäumt worden, die Fahndungsausschreibung im INPOL zu löschen. Nachdem die Staatsanwaltschaft den Fehler erkannt hatte, wurde dies unverzüglich nachgeholt. Warum dies nicht rechtzeitig veranlasst worden war, ließ sich nicht mehr nachvollziehen. Bei der Prüfung weiterer Petitionen in diesem Bereich konnte ich jedoch feststellen, dass alle Speicherungen rechtmäßig waren und es sich somit bei dem oben geschilderten Sachverhalt wohl um einen Einzelfall gehandelt hat.

Ich habe den Bundesbeauftragten für den Datenschutz über das Ergebnis unterrichtet. Die Fahndungsausschreibung wurde auch im Ausländerzentralregister gelöscht und der Petent über das Ergebnis informiert.

2.1.3 Kleine Anfragen des Landtages personenbezogen beantworten?

Die Landesregierung hat in einer Reihe von Fällen Rechtsanwaltskanzleien mit der Vertretung der Landesinteressen beauftragt. Ein Abgeordneter des Landtages bat in einer Kleinen Anfrage darum, die Anwaltskanzleien mitzuteilen, die ihren Sitz außerhalb von Mecklenburg-Vorpommern haben. Neben den Namen sowie der Art und der Anzahl der Fälle interessierten ihn auch die Gegenstandswerte sowie die Honorare der jeweiligen Kanzleien (LT-Drs. 3/2740). Die Landesregierung hat mich gebeten, hierzu aus datenschutzrechtlicher Sicht Stellung zu nehmen.

Nach Art. 40 Abs. 1 der Verfassung des Landes Mecklenburg-Vorpommern (Verf M-V) hat die Landesregierung Fragen einzelner Abgeordneter oder parlamentarische Anfragen nach bestem Wissen unverzüglich und vollständig zu beantworten. Gemäß Art. 40 Abs. 4 Verf M-V regelt das Nähere ein Gesetz. Dieses existiert bisher jedoch nicht. Daher richtet sich die Übermittlung personenbezogener Daten nach den Bestimmungen des Landesdatenschutzgesetzes (§ 10 DSG MV, nach der Novellierung § 14 DSG M-V) in Verbindung mit Art. 40 Verf M-V. Zu berücksichtigen ist, dass die Landesregierung Auskünfte – und damit eine Datenübermittlung – dann ablehnen kann, wenn dem Bekanntwerden des Inhaltes schutzwürdige Interessen Einzelner, insbesondere des Datenschutzes, entgegenstehen (Art. 40 Abs. 3 Verf M-V).

Datenschutzrechtliche Aspekte sind jedoch nur zu prüfen, wenn bei der Beantwortung der Anfrage auch tatsächlich personenbezogene Daten mitgeteilt werden. Personenbezogene Daten sind nach § 3 Abs. 1 DSG M-V Einzelangaben über die persönlichen oder sachlichen Verhältnisse einer bestimmten oder zumindest bestimmbaren natürlichen Person.

Angaben über juristische Personen und andere Personengruppen wie Personengesellschaften (z. B. Anwaltssozietäten) fallen nicht darunter, es sei denn, dass die Bezeichnung einer Kanzlei gleichzeitig auch die Verhältnisse einer dahinter stehenden natürlichen Person beschreibt. Dies würde beispielsweise zutreffen, wenn eine Kanzlei von einem Rechtsanwalt allein geführt oder wenn die Höhe des Honoraranteils jedes Mitgliedes der Gesellschaft angegeben wird.

Datenschutzrechtliche Aspekte schließen die Beantwortung von Kleinen Anfragen mit personenbezogenen Daten freilich nicht aus. Das Übermitteln personenbezogener Daten ist nach § 14 DSG M-V zulässig, wenn es zur Erfüllung einer in der Zuständigkeit der verarbeitenden Stelle liegenden Aufgabe erforderlich ist. Der Landesregierung wird mit Art. 40 Verf M-V eine Rechtspflicht zur Beantwortung von Abgeordnetenfragen auferlegt. Es ist in diesen Fällen gemäß Art. 40 Abs. 3 Satz 1 Verf M-V somit genau zu prüfen, ob schutzwürdige Interessen der Betroffenen einer Beantwortung entgegenstehen. Bei der Interessenabwägung ist das Recht des einzelnen Abgeordneten auf umfassende Information zu berücksichtigen, ohne die er seine verfassungsrechtlichen Aufgaben nicht ordnungsgemäß wahrnehmen kann. Dem steht das Recht auf informationelle Selbstbestimmung der Betroffenen gegenüber, wobei auch die Sensibilität der Daten eine entscheidende Rolle spielt. Je sensibler die Daten sind, desto größeres Gewicht haben sie bei der Interessenabwägung zugunsten des Betroffenen. Besonders zu berücksichtigen ist dabei der Umstand, dass die Antworten der Landesregierung nicht nur an den Abgeordneten persönlich gerichtet sind, sondern in vollem Umfang mit den Landtagsdrucksachen der Öffentlichkeit zugänglich gemacht werden.

Führt die Prüfung zu dem Ergebnis, dass einer Auskunft keine schutzwürdigen Interessen entgegenstehen, so ist die Anfrage so zu beantworten, wie es der Abgeordnete wünscht. Bleiben unter Berücksichtigung aller Interessen dennoch Zweifel, sollten die Daten zumindest nicht personenbezogen übermittelt werden. Um dem Informationsrecht des Abgeordneten in diesen Fällen dennoch Rechnung zu tragen, könnte meines Erachtens die Anfrage ganz oder teilweise in pseudonymisierter Form beantwortet werden. Zu diesem Zweck müsste der Name der Rechtsanwaltskanzlei oder eines Rechtsanwalts durch ein Pseudonym (z. B. fortlaufende Nummer der Beauftragung) ersetzt werden, das einen Rückschluss auf eine bestimmte natürliche Person nur unter bestimmten Bedingungen zulässt. Unter diesen Voraussetzungen könnten alle weiteren relevanten Daten, wie die Honorarhöhe, angegeben werden. Bei mehreren Aufträgen an eine Rechtsanwaltskanzlei wäre dann dasselbe Pseudonym zu verwenden. Die Angaben zu den einzelnen Aufträgen können auf diese Weise detailliert und differenziert dargestellt werden. In einer nichtöffentlichen Landtagsausschusssitzung könnten die personenbezogenen Daten offen gelegt wer-

den. Diese Verfahrensweise würde sowohl die datenschutzrechtlichen Belange der Betroffenen als auch die Informationsansprüche der Abgeordneten berücksichtigen.

In ihrer Antwort auf die Kleine Anfrage (LT-Drs. 3/2784) hat die Landesregierung die einzelnen Kanzleien nicht namentlich benannt. Sie berief sich dabei auf Art. 40 Abs. 3 in Verbindung mit Art. 6 Abs. 1 Verf M-V und auf die Übermittlungsvorschrift des Landesdatenschutzgesetzes (jetzt § 14 DSG M-V). Weil Landtagsdrucksachen im Internet veröffentlicht werden und personenbezogene Daten damit uneingeschränkt weltweit zur Verfügung stehen, sei es geboten, auf eine namentliche Nennung zu verzichten. Dies komme auch deshalb in Betracht, weil die Angaben nicht erforderlich seien, um die Kleine Anfrage in der gewünschten Zielrichtung zu beantworten (LT-Drs. 3/2843). Die Landesregierung hat stattdessen für jede Kanzlei eine Schlüsselnummer vergeben und die Angaben der einzelnen Verfahren zugeordnet, wobei die Mandate nur in allgemeiner Form beschrieben wurden.

Da der Landtagsabgeordnete mit dieser Art der Beantwortung nicht zufrieden war, rief er das Landesverfassungsgericht an. Im Urteil vom 19. Dezember 2002 (LVerfG 5/02) hat das Gericht entschieden, dass die Landesregierung die Kleine Anfrage des Abgeordneten unvollständig beziehungsweise inhaltlich nicht beantwortet hat. Der Antragsteller ist somit in seinem verfassungsrechtlich garantierten Recht aus Art. 40 Abs. 1 Satz 1 Verf M-V auf umfassende Sachinformation verletzt worden. Auf folgende Aspekte hat das Landesverfassungsgericht unter anderem hingewiesen:

- Lehnt die Landesregierung die Beantwortung von Fragen einzelner Abgeordneter ab, so muss sie dies begründen und die dabei maßgeblichen tatsächlichen und rechtlichen Gesichtspunkte nachvollziehbar darlegen. Der schlichte Hinweis auf Datenschutzgesichtspunkte genügt diesen Anforderungen nicht. Auch in der zweiten Antwort der Landesregierung fehlte eine nachvollziehbare Begründung. Eine datenschutzrechtliche Bewertung und die gebotene Abwägung wurden nicht durchgeführt.

- Die Landesregierung hat nicht das Recht, die Zielrichtung der Anfragen von Abgeordneten zu beurteilen, um so über den erforderlichen Umfang der zu übermittelnden Daten zu entscheiden. Die Abgeordneten entscheiden eigenverantwortlich, welche Informationen sie zur Erfüllung ihrer Aufgaben benötigen.

- Die Anfragen von Abgeordneten sind regelmäßig zu beantworten. Nur in Ausnahmefällen kann eine Beantwortung unter Berücksichtigung der Voraussetzungen abgelehnt werden (Regel-Ausnahme-Verhältnis). Diese Ausnahmefälle müssen im Hinblick auf

die herausragende Bedeutung des Informationsrechtes des Abgeordneten besonders gerechtfertigt sein. Die Landesregierung hat das Auskunftsersuchen in pauschaler Form abgelehnt, ohne die Einzelfälle näher zu prüfen. Dabei hatte sie nicht beachtet, dass von einer Auskunft nur abgesehen werden darf, wenn Datenschutzgründe entgegenstehen. Das war vorliegend nicht der Fall.

Dem Informationsinteresse des einzelnen Abgeordneten kommt im Rahmen der Gewaltenteilung in einer repräsentativen Demokratie herausragende Bedeutung zu. Die Entscheidung des Landesverfassungsgerichtes hat das Informationsrecht der Abgeordneten in besonderer Weise gestärkt und die Voraussetzungen für eine Auskunftsverweigerung eng definiert. Insofern sind Ausnahmefälle sorgfältig zu prüfen, um diesen Anforderungen Rechnung zu tragen. Die Prüfung der Erforderlichkeit der zu übermittelnden Daten gehört dabei nicht zu den Aufgaben der Landesregierung als übermittelnde Stelle. Den Lösungsansatz unter Nutzung eines Pseudonyms in Kombination mit der Bekanntgabe der Namen in einer nichtöffentlichen Landtagsausschusssitzung hat das Landesverfassungsgericht als Alternative nicht in Betracht gezogen.

Die Landesregierung hat die Fragen des Abgeordneten nunmehr vollständig beantwortet (LT-Drs. 4/148). Eine gesetzliche Regelung zu diesem Verfahren, wie in Art. 40 Abs. 4 Verf M-V vorgesehen, fehlt weiterhin.

2.1.4 Zu viele Steuerdaten in der Ermittlungsakte?

Ein Petent hatte gegen eine Mitarbeiterin eines Finanzamtes Strafanzeige erstattet, da sie seinen Einkommensteuerbescheid an eine andere öffentliche Stelle übersandt hatte. Die Staatsanwaltschaft ermittelte daraufhin wegen des Verdachtes der Verletzung des Steuergeheimnisses und nahm hierzu Unterlagen aus der Steuerakte des Petenten in Kopie zur Ermittlungsakte. Der Petent bezweifelte die Rechtmäßigkeit dieser Vorgehensweise, da seiner Meinung nach Steuerunterlagen zur Ermittlungsakte genommen wurden, die für das Verfahren nicht relevant waren. Nachdem er vergeblich die Staatsanwaltschaft ersucht hatte, diese Daten in der Akte zu löschen, bat er mich um Hilfe.

Die Staatsanwaltschaft teilte mir mit, dass sie nach Eingang der Steuerakte deren Inhalt nur kursorisch prüfe und von den wesentlichen Teilen Kopien fertige. Im Rahmen einer umfassenden Sachverhaltserfassung sei es zu diesem Zeitpunkt nicht möglich zu beurteilen, welche Aktenbestandteile nach Abschluss der Ermittlungen tatsächlich erforder-

lich sein werden. Darüber hinaus wäre es bei Akten nicht immer möglich, personenbezogene Daten genau zu trennen. Es wäre daher zulässig, auch solche Daten zu verarbeiten, die in der Sache nicht erheblich sind. Im vorliegenden Fall hielt es die Staatsanwaltschaft für zulässig, dass personenbezogene Daten im bisherigen Umfang zur Sachverhaltserforschung verarbeitet wurden. Insofern stellte sich für sie auch nicht die Frage nach der Löschung dieser Daten.

Das mit der Angelegenheit ebenfalls befasste Justizministerium unseres Landes hält die Auffassung der Staatsanwaltschaft für vertretbar.

Ich habe den Sachverhalt geprüft und bin zu dem Ergebnis gelangt, dass die Staatsanwaltschaft mehr Daten in der Akte gespeichert hatte, als für das Ermittlungsverfahren erforderlich gewesen wären.

Die Staatsanwaltschaft ist im Rahmen eines Ermittlungsverfahrens gemäß §§ 160, 161 Strafprozessordnung berechtigt und verpflichtet, den Sachverhalt umfassend zu erforschen und die in diesem Zusammenhang notwendigen Beweismittel sowohl zur Belastung als auch zur Entlastung der Beschuldigten zu erheben. Bei ihren Ermittlungen hat sie den Grundsatz der Verhältnismäßigkeit zu beachten. Die von ihr getroffenen Maßnahmen müssen unter Würdigung aller persönlichen und tatsächlichen Umstände des Einzelfalles zum Erreichen des angestrebten Zweckes geeignet und erforderlich sein, und die damit verbundene Beeinträchtigung darf nicht erkennbar außer Verhältnis zum beabsichtigten Erfolg stehen.

In diesem Fall ging es für die Staatsanwaltschaft allein um die Frage, ob die Mitarbeiterin des Finanzamtes mit der Übersendung des Steuerbescheides an eine andere öffentliche Stelle den Straftatbestand des § 355 Strafgesetzbuch – Verletzung des Steuergeheimnisses – erfüllt hatte.

Die Staatsanwaltschaft war berechtigt, die Steuerakte des Petenten im Ermittlungsverfahren beizuziehen. Um die notwendigen Informationen zu erhalten, war es auch unvermeidbar, dass hierbei personenbezogene Daten des Petenten zur Kenntnis genommen wurden, die keinen Bezug zum Sachverhalt hatten. Die Staatsanwaltschaft muss in einem solchen Fall prüfen können, welche Unterlagen aus der Akte für ihre Entscheidung relevant sind. Diese Unterlagen werden in die Ermittlungsakte aufgenommen. Dabei ist nicht immer von vornherein zu erkennen, welche Unterlagen dies tatsächlich sind.

Bei der Durchsicht der staatsanwaltschaftlichen Ermittlungsakte fand ich zahlreiche Kopien von Schreiben aus der Steuerakte des Petenten, die offensichtlich keinen Aussagegehalt hinsichtlich der zu prüfenden Strafvorschrift enthielten. Dies hätte die Staatsanwaltschaft erkennen können.

Auch die vom Petenten im Zuge des Ermittlungsverfahrens abgegebene Schweigepflichtentbindungserklärung berechtigte die Staatsanwaltschaft nicht, die beim Finanzamt geführte Steuerakte des Petenten wohl nahezu komplett zu kopieren. Mit der Entbindung von der Schweigepflicht ist der Steuerbeamte lediglich befugt, die Steuerdaten zu offenbaren. Inwieweit die offenbarten Steuerdaten kopiert und in die Akten der Staatsanwaltschaft aufgenommen werden dürfen, beurteilt sich allein nach der Erforderlichkeit dieser Daten für die im Strafverfahren notwendige Sachverhaltsaufklärung.

Die Bedenken des Petenten sind nach meiner Ansicht daher begründet.

Einvernehmen konnte in der Sache leider nicht erzielt werden. Die unterschiedlichen Rechtsauffassungen zu diesem Sachverhalt bestehen fort. Zwar handelt es sich nach meinen datenschutzrechtlichen Prüferfahrungen hierbei um einen Einzelfall. Dennoch habe ich dem Leitenden Oberstaatsanwalt empfohlen, die Staatsanwälte auf dieses Thema hinzuweisen.

2.1.5 Großer Lauschangriff

Am 1. Juli 2003 hat das Bundesverfassungsgericht mündlich über die Verfassungsbeschwerden einiger Privatpersonen verhandelt, die sich gegen die im Grundgesetz eingeführte akustische Wohnraumüberwachung, den so genannten Großen Lauschangriff, gewandt haben. Aus diesem Anlass habe ich gemeinsam mit den Datenschutzbeauftragten von Berlin, Bremen, Hamburg, Niedersachsen, Nordrhein-Westfalen und Schleswig-Holstein gegenüber dem Bundesverfassungsgericht eine Stellungnahme abgegeben. Wir haben deutlich gemacht, dass wir die Regelungen zum Großen Lauschangriff für verfassungswidrig halten.

Auf die besondere Eingriffstiefe des Großen Lauschangriffes in das Grundrecht auf informationelle Selbstbestimmung haben die Datenschutzbeauftragten des Bundes und der Länder in der Vergangenheit bereits mehrfach hingewiesen. Auch ich habe mich in früheren Tätigkeitsberichten (siehe Erster Tätigkeitsbericht, Punkt 2.4.1, 2.21.5; Zweiter Tätigkeitsbericht, Punkt 2.3.8 und Dritter Tätigkeitsbericht, Punkt 3.2.3) kritisch dazu geäußert.

In der oben genannten Stellungnahme werden die maßgeblichen Argumente gegen den Großen Lauschangriff nochmals ausführlich erläutert:

- Die akustische Wohnraumüberwachung verstößt sowohl gegen die Menschenwürde als auch gegen den Kerngehalt des allgemeinen Persönlichkeitsrechts und den Schutz der Unverletzlichkeit der Wohnung.

- Das Belauschen von Gesprächen, selbst aus der Intimsphäre von Ehepartnern, verstößt gegen den grundrechtlichen Schutz der Ehe.

- Die Ausgestaltung des Großen Lauschangriffes auf gesetzlicher Ebene ist in mehrfacher Hinsicht verfassungswidrig.

- Es ist nicht durch eine objektive Rechtstatsachenanalyse belegt, dass der Große Lauschangriff erforderlich ist, um die organisierte Kriminalität bekämpfen zu können.

- Der Straftatenkatalog für die Durchführung von Großen Lauschangriffen geht weit über die organisierte Kriminalität hinaus.

- Der Schutz der strafprozessualen Aussage- und Zeugnisverweigerungsrechte ist völlig unzureichend. Es müsste vielmehr ein absolutes Verwertungsverbot greifen, wenn sich nachträglich beispielsweise herausstellt, dass sich der Beschuldigte mit seinem Anwalt unterhalten hat.

- Die permanente richterliche Verlängerung von Lauschangriffen ist ohne große Hürden möglich.

- Obwohl es das Gesetz vorsieht, werden die Betroffenen auch im Nachhinein nur unzureichend, in vielen Fällen gar nicht davon unterrichtet, dass sie belauscht worden sind.

- Die Erforderlichkeit der akustischen Wohnraumüberwachung ist bisher nicht überzeugend belegt worden. Dies zeigt eindrucksvoll der Erfahrungsbericht der Bundesregierung zu den Wirkungen der Wohnungsüberwachung durch Einsatz technischer Mittel (Art. 13 Abs. 3-5 GG; § 100 c-100 f StPO) vom 30. Januar 2002 (BT-Drs. 14/8155).

Insgesamt ist festzustellen, dass gesicherte Aussagen zur Intensität des Grundrechtseingriffes nicht getroffen werden konnten. Gleichwohl äußern bereits jetzt einzelne Länder weitere Begehrlichkeiten, bis hin zur optischen Wohnraumüberwachung zu repressiven Zwecken.

2.1.6 DNA-Analyse – Erweiterung nur mit Augenmaß!

In der Vergangenheit hat es mehrere Gesetzesinitiativen und politische Absichtserklärungen gegeben, die DNA-Analyse (so genannter genetischer Fingerabdruck) erheblich auszuweiten. Unter Umständen soll sie sogar routinemäßig als Ermittlungsmaßnahme eingesetzt werden, wie dies bereits jetzt beim „normalen“ Fingerabdruck geschieht.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich in einer Entschließung vom Juli 2003 (siehe Anlage 19) gegen diese Bestrebungen gewandt und gefordert, dass

- die DNA-Analyse nicht mit dem einfachen Fingerabdruck gleichgesetzt werden darf,

- die DNA-Analyse auch künftig nur bei Straftaten von erheblicher Bedeutung in Betracht kommen soll,

- die DNA-Analyse auch weiter nur dann angewandt werden soll, wenn die Prognose gerechtfertigt ist, dass gegen den Betroffenen künftig erneut Strafverfahren wegen Straftaten von erheblicher Bedeutung zu führen sein werden,

- der Richtervorbehalt für die Anordnung der DNA-Analyse aufrechterhalten bleibt, da nur so gesichert ist, dass die Voraussetzungen der DNA-Analyse unabhängig überprüft werden und

- die weit verbreitete Praxis, DNA-Analysen ohne richterliche Entscheidung auf der Grundlage einer Einwilligung der Betroffenen durchzuführen, gesetzlich ausgeschlossen werden sollte.

Der Justizminister unseres Landes hat sich öffentlich zu diesem Thema geäußert und vorgeschlagen, den genetischen Fingerabdruck auf alle zu Haftstrafen Verurteilten auszudehnen. Ich halte das für bedenklich, da der verfassungsrechtlich garantierte Grundsatz der Verhältnismäßigkeit einer derart undifferenzierten Ausdehnung dieser Maßnahme entgegenstünde.

Auch das Bundesverfassungsgericht hat anlässlich mehrerer Verfassungsbeschwerden Betroffener im Dezember 2000 und im März 2001 entschieden, dass bei einem derartigen Eingriff in die Persönlichkeitssphäre sehr genau geprüft werden müsse, ob tatsächlich eine Wiederholungsgefahr vorliegt, und dies mit der Bedeutung und Tragweite des Grundrechtes auf informationelle Selbstbestimmung, dem Rechtsstaatsprinzip und dem Resozialisierungsgedanken begründet.

Der Bundestag hat im Jahre 2003 das Gesetz zur Änderung der Vorschriften über die Straftaten gegen die sexuelle Selbstbestimmung und zur Änderung anderer Vorschriften verabschiedet, mit dem eine Erweiterung der DNA-Analyse auf gegen die sexuelle Selbstbestimmung gerichtete Straftaten verbunden ist.

Unabhängig davon gibt es weitere Überlegungen zu einer erneuten Ausweitung der DNA-Analyse. Die Justizministerkonferenz hat eine Arbeitsgruppe unter Vorsitz von Mecklenburg-Vorpommern eingesetzt, die sich mit dem Thema intensiv befassen und eine Expertenanhörung zu naturwissenschaftlichen und rechtlichen Fragen durchführen wird. Erste Ergebnisse sollen bis Mitte des Jahres 2004 vorliegen. Es bleibt zu hoffen, dass die in der Entschließung genannten Anforderungen dabei hinreichend berücksichtigt werden.

2.2 Neues Datenschutzrecht

2.2.1 Reform des Datenschutzrechts erforderlich

Nach der Bundestagswahl im September 2002 haben die SPD und die Grünen in ihrem Koalitionsvertrag vereinbart, dass sie das Datenschutzrecht umfassend reformieren wollen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern in ihrer Entschließung vom 27./28. März 2003 (siehe Anlage 10), dass diese politische Absichtserklärung zügig verwirklicht wird. Sie sehen dabei die Schwerpunkte in

- der Modernisierung des Bundesdatenschutzgesetzes,
- der Stärkung des System- und Selbstdatenschutzes,
- der Förderung von datenschutzgerechter Technik,
- der Entwicklung des Datenschutzaudits und des Gütesiegels,
- der Gewährleistung der anonymen Internetnutzung,
- der Evaluierung der Eingriffsbefugnisse der Sicherheitsbehörden,
- der Verbesserung des Datenschutzes in den Bereichen der Medizin, der Gentechnik, des Steuerrechtes und des Arbeitnehmerschutzes,
- der Stärkung der Datenschutzkontrolle sowie
- der Schaffung eines Informationsfreiheitsgesetzes.

Die Datenschutzbeauftragten haben ausdrücklich ihre Bereitschaft erklärt, die Bundesregierung bei der Weiterentwicklung des Datenschutzrechtes zu unterstützen.

2.2.2 Das neue Landesdatenschutzgesetz

Am 18. April 2002 trat das „Gesetz zum Schutz des Bürgers bei der Verarbeitung seiner Daten“ (Landesdatenschutzgesetz – DSG M-V) vom 28. März 2002 in Kraft. Es löst das Landesdatenschutzgesetz vom 24. Juli 1992 ab.

Anlass für die Novellierung war die EU-Datenschutzrichtlinie vom Oktober 1995 (siehe Zweiter Tätigkeitsbericht, Punkt 2.1). Die Richtlinie hätte bis zum Oktober 1998 in Landesrecht umgesetzt sein müssen (siehe Dritter Tätigkeitsbericht, Punkt 2.4). Bereits im Vierten Tätigkeitsbericht habe ich unter Punkt 2.1 auf die Überschreitung der Umsetzungsfrist hingewiesen und der Landesregierung empfohlen, möglichst bald einen Gesetzentwurf vorzulegen.

Ein Grund für die späte Verabschiedung des Landesdatenschutzgesetzes war der Wunsch der Landesregierung, die Novellierung des Bundesdatenschutzgesetzes inhaltlich zu berücksichtigen. Die Novelle des Bundesdatenschutzgesetzes trat allerdings schon am 23. Mai 2001 in Kraft (siehe Fünfter Tätigkeitsbericht, Punkt 3.2.2).

Aus der EU-Datenschutzrichtlinie resultieren folgende wesentliche Änderungen:

- Es werden Kategorien besonders sensibler Daten definiert, an deren Verarbeitung erhöhte Anforderungen gestellt werden (§§ 7 Abs. 2 und 3, 10 Abs. 3 Satz 4).

- Die Informationsrechte der Betroffenen werden erweitert (§§ 9 Abs. 3 und 4, 24 Abs. 1 Satz 1).

- Automatisierte Einzelentscheidungen, die nicht bestimmte Voraussetzungen erfüllen, sind verboten (§ 12).

- Für die Datenübermittlung an europäische nichtöffentliche Stellen und an Staaten außerhalb der Europäischen Union (so genannte Drittstaaten) werden detaillierte Vorgaben festgelegt (§ 16).

- Vor dem Einsatz bestimmter Datenverarbeitungsverfahren ist zu prüfen, ob die Datenverarbeitung zulässig ist und ob die vorgesehenen technischen und organisatorischen Maßnahmen ausreichend sind (Vorabkontrolle, § 19 Abs. 2).

- Jede öffentliche Stelle hat einen behördlichen Datenschutzbeauftragten zu bestellen (§ 20).

- Die Verfahrensverzeichnisse der öffentlichen Stellen müssen öffentlich zugänglich sein (§ 20 Abs. 4).

- Betroffene erhalten unter bestimmten Bedingungen die Möglichkeit, zulässigen Verarbeitungen ihrer Daten zu widersprechen (§ 25 Abs. 3).

Neben der Umsetzung der Datenschutzrichtlinie hat das neue Landesdatenschutzgesetz die Modernisierung des Datenschutzrechts zum Ziel. Dies zeigt sich vor allem in nachstehenden Regelungen:

- Schon im Vorfeld einer Datenverarbeitung sind die Grundsätze der Datenvermeidung und der Datentrennung zu beachten (§ 5 Abs. 1 und 3).

- Behörden sollen vorrangig informationstechnische Produkte einsetzen, für die in einem Prüfverfahren (Datenschutzaudit) festgestellt wurde, dass sie mit den Datenschutz- und den Datensicherheitsvorschriften vereinbar sind (§ 5 Abs. 2).

- Betroffene Personen können auch elektronisch in eine Datenverarbeitung einwilligen, sofern die geforderten Voraussetzungen eingehalten werden (§ 8 Abs. 2).

- Automatisierte Verfahren müssen vor ihrem Einsatz vom Leiter der Daten verarbeitenden Stelle freigegeben werden (§ 19 Abs. 1).

- Die Anforderungen an die zu treffenden technischen und organisatorischen Maßnahmen werden als Sicherheitsziele definiert, die von der verwendeten Technik unabhängig sind (§ 21). Für die bisherigen Regelungen – die so genannten Zehn Gebote – galt dies nicht. Sie stammten aus den 70er Jahren und orientierten sich auch an der damaligen Technik und Datenverarbeitungsstruktur. Die neuen Forderungen basieren auf einem Vorschlag des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder. Ihre Vorteile gegenüber den alten Bestimmungen habe ich ausführlich im Vierten Tätigkeitsbericht unter Punkt 2.3 dargestellt.

- Sollen zur Verarbeitung personenbezogener Daten automatisierte Verfahren eingesetzt werden, sind generell bestimmte Maßnahmen zur Datensicherheit zu treffen, wie die Verschlüsselung personenbezogener Daten bei gewissen Verarbeitungen (§ 22). Diese

Bestimmung beinhaltet nur solche Vorkehrungen, von denen zu erwarten ist, dass sie längere Zeit dem Stand der Technik entsprechen (siehe Vierter Tätigkeitsbericht, Punkt 2.3).

- Die Bedingungen, unter denen mobile Datenverarbeitungssysteme, insbesondere Chipkarten, und Videoüberwachung eingesetzt werden dürfen, werden normiert (§§ 36, 37).

Eine weitere wichtige Änderung ist die Einfügung des neuen § 2 Absatz 2. Dieser stellt nunmehr ausdrücklich klar, dass alle Unternehmen in privater Rechtsform, also zum Beispiel Gesellschaften mit beschränkter Haftung und Aktiengesellschaften, an denen öffentliche Stellen mit absoluter Mehrheit der Anteile oder Stimmen beteiligt sind, selbst öffentliche Stellen sind und damit der Kontrolle des Landesbeauftragten für den Datenschutz unterliegen. In der Vergangenheit gab es vereinzelt kommunale Unternehmen, die diese Kontrollbefugnis nicht anerkannten.

Neben diesen positiven Neuerungen gibt es aber auch wesentliche Kritikpunkte:

- Die Datenverarbeitung ist weiterhin meist schon dann zulässig, wenn eine Rechtsnorm sie zwar nicht erlaubt, aber „zwingend voraussetzt". Diese unklare und verfassungsrechtlich bedenkliche Formulierung sollte nicht Rechtsgrundlage für eine Verarbeitung personenbezogener Daten sein.

- Der Landesbeauftragte für den Datenschutz ist auch nach dem neuen Landesdatenschutzgesetz nur für den öffentlichen Bereich zuständig. Die Chance, im Interesse der Bürger eine zentrale Datenschutzkontrollinstanz für alle Stellen des Landes einzurichten, wurde nicht wahrgenommen.

- Trotz ihrer großen Gefahrenpotentiale für das Recht auf informationelle Selbstbestimmung muss vor dem Einsatz mobiler Verarbeitungssysteme oder einer Videoüberwachung keine Vorabkontrolle durchgeführt werden.

- Es fehlt eine klarstellende Regelung, dass sich die Kontrolle des Landesbeauftragten für den Datenschutz auch auf personenbezogene Daten erstreckt, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Aufgrund eines konkreten Sachverhaltes (siehe Vierter Tätigkeitsbericht, Punkt 3.1.10) hat der Landtag im Zuge der Verabschiedung des neuen Landesdatenschutzgesetzes folgende Entschließung gefasst: „Hinsichtlich der Regelung in § 30 geht der Landtag davon aus, dass Notare als Träger eines öffentlichen Amtes der Datenschutzkontrolle durch den Landesbeauftragten für den Datenschutz unterliegen." Ich begrüße diese Aussage ausdrücklich. Allerdings

sollte das Gesetz selbst entsprechend eindeutig formuliert werden. Gleichzeitig sollte klargestellt werden, dass sich die Kontrollbefugnis ebenso auf alle anderen Träger von Berufs- oder besonderen Amtsgeheimnissen erstreckt.

Die Broschüre „Landesdatenschutzgesetz 2002 mit Erläuterungen“ gibt Hinweise zur Auslegung und Anwendung der einzelnen Bestimmungen. Sie ist kostenlos in meiner Behörde erhältlich und auch aus dem Internetangebot unter http://www.lfd.m-v.de/ges_ver/erldsg/erldsgmv02.pdf abrufbar.

Der Gesetzgeber hat in § 44 Abs. 2 DSG M-V festgelegt, dass am 31. Dezember 2004 § 30 DSG M-V, der das Kontrollrecht des Landesbeauftragten für den Datenschutz regelt, außer Kraft tritt. Diese Regelung verpflichtet die Landesregierung, bis dahin zu prüfen, ob dem Landesbeauftragten für den Datenschutz auch die Kontrolle über den nichtöffentlichen Bereich übertragen wird. Im Zuge dieser Änderungen sollten ebenfalls die oben dargestellten Kritikpunkte berücksichtigt werden.

2.3 Polizei

2.3.1 Nutzung polizeilicher Auskunftssysteme zur Überprüfung von Bewerbern bei der Polizei

Ein Kollege aus einem anderen Bundesland teilte mir mit, dass dort das polizeiliche Auskunftssystem nicht nur zur Erfüllung polizeilicher Aufgaben genutzt werde, sondern auch zur Überprüfung von Bewerbern für den Polizeidienst. Dies habe ich zum Anlass genommen, um von unserem Innenministerium zu erfahren, wie hierzulande verfahren wird.

Auch bei uns werden Daten, die zur Erfüllung polizeilicher Aufgaben gespeichert sind, zur Eignungsprüfung im Bewerbungsstadium genutzt. Alle Bewerber, die sich für eine Ausbildung im mittleren, gehobenen oder höheren Polizeivollzugsdienst beim Auswahl- und Einstellungsdienst im Polizeiinstitut der Polizei bewerben, werden gebeten, den Vordruck „Einverständniserklärung“ zu unterzeichnen. Damit stimmen die Bewerber zu, dass Auskünfte bei den für ihren Wohnsitz zuständigen Polizeidienststellen eingeholt werden. Der Bewerber wird darüber informiert, dass auch nach Erkenntnissen zu polizeilichen oder staatsanwaltschaftlichen Ermittlungen gefragt wird. Darüber hinaus soll festgestellt werden, ob aktenkundige Tatsachen darüber vorliegen, dass er in einer Weise polizeilich in Erscheinung getreten ist, die Zweifel an seiner Eignung für den Polizeidienst aufkommen lassen.

Das Ministerium ist der Auffassung, dass der Bewerber mit der oben genannten schriftlichen Einverständniserklärung – sozusagen schlüssig – auch darin eingewilligt hat, dass Auskünfte aus der polizeilichen Erkenntnisdatei (PED) beziehungsweise aus dem Informationssystem der Polizei (INPOL) und dem elektronischen Vorgangsassistenten (EVA) eingeholt werden. Rechtsgrundlage für die Nutzung der gespeicherten personenbezogenen Daten seien die entsprechenden Regelungen des Landesdatenschutzgesetzes (§ 7 Abs. 1 Nr. 3 in Verbindung mit § 8 Abs. 1 und § 10 Abs. 3 Nr. 2 DSG M-V).

Dazu habe ich dem Innenministerium unseres Landes Folgendes mitgeteilt: Im Auswahlverfahren soll der künftige Dienstherr prognostizieren, ob der Bewerber die persönliche, insbesondere auch die charakterliche Eignung für den Polizeivollzugsdienst besitzt. Daher ist anzuerkennen, dass sich der künftige Dienstherr schon während des Einstellungsverfahrens besonderes dafür interessiert, ob gegen den Bewerber strafrechtliche Ermittlungen durchgeführt wurden. Die im Einstellungsverfahren verwendeten Einwilligungsformulare müssen jedoch gerade im Hinblick auf die oben zitierte Vorschrift des § 8 Abs. 1 DSG M-V folgenden Voraussetzungen genügen:

- Der Betroffene ist eindeutig und umfassend aufzuklären. So sind in der Einwilligungserklärung die polizeilichen Auskunftssysteme zu nennen, die während der Überprüfung abgefragt werden sollen. Darüber hinaus sind der Verarbeitungszweck konkret zu erläutern und die Speicherungsdauer exakt zu bezeichnen.

- Die Abfrage sollte auf polizeiliche Auskunftssysteme beschränkt bleiben, in denen Erkenntnisse zu strafrechtlichen Ermittlungsverfahren hinterlegt sind. Verfahren, die der polizeilichen Vorgangsbearbeitung dienen (z. B. EVA), sollten nicht mit einbezogen werden.

- Im Rahmen der Abfrage dürfen nur die Erkenntnisse genutzt werden, die für die Beurteilung der persönlichen Eignung von ausschlaggebender Bedeutung sind.

- Die Abfrage ist auf den Bewerberkreis zu begrenzen, der nach dem Ergebnis des Bewerbungsverfahrens zur Einstellung vorgesehen ist.

Eine Antwort des Innenministeriums steht noch aus.

2.3.2 Identitätsnachweis für Auskunftsersuchen bei der Polizei

Ein Petent hatte sich an eine Polizeidienststelle gewandt und wollte wissen, was dort zu seiner Person gespeichert sei. Das Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V) hat ihn daraufhin gebeten, zunächst mitzuteilen, aus welchem Grund beziehungsweise in welcher Angelegenheit, wann und durch welche Polizeibehörde oder -dienststelle die Daten zu seiner Person gespeichert sein könnten. Darüber hinaus sei ein eindeutiger Nachweis seiner Identität erforderlich, um sicherzustellen, dass personenbezogene Informationen nicht an Dritte gelangen. Aus diesem Grunde solle er das für seinen Wohnsitz zuständige Einwohnermeldeamt aufsuchen, um sich dort unter Vorlage seines Personalausweises und unter Angabe der vorgesehenen Zweckbestimmung eine Identitäts- beziehungsweise Meldebestätigung ausstellen zu lassen. Erst nach Übersendung dieser Bescheinigung könne dem Antrag auf Auskunftserteilung entsprochen werden. Daraufhin hat der Petent bei mir angefragt, ob dies aus datenschutzrechtlicher Sicht in Ordnung sei.

Das LKA M-V begründete seine hohen Anforderungen mir gegenüber damit, dass eine sichere Identifizierung des Auskunftsersuchenden nicht möglich wäre, wenn beispiels-

weise lediglich Name, Anschrift und Geburtsdatum verlangt würden. Es sei durchaus möglich, dass ein Dritter, der die vorstehenden Angaben des Betroffenen kennt, unbefugt einen Auskunftsantrag stellt. Dabei handele es sich nach polizeilicher Erfahrung keineswegs um einen hypothetischen Fall. Auch die Vorlage einer Kopie des Personalausweises sei nicht geeignet, den geforderten sicheren Identitätsnachweis zu erbringen. Durch Abgleich der daraus ersichtlichen Unterschrift mit der des Antragstellers aus dessen jeweiligem Auskunftsersuchen lasse sich erfahrungsgemäß die Identität des Antragstellers nicht mit der erforderlichen Sicherheit feststellen. Hingegen stelle die Vorlage einer Meldebescheinigung ein geeignetes Mittel zum Nachweis der Identität dar.

Ich habe die Hürden, die hier vor der Auskunftserteilung aufgebaut wurden, aus (datenschutz-)rechtlicher Sicht als zu hoch und damit als unzulässig bewertet. Gemäß § 48 Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern (SOG M-V) ist dem Betroffenen auf Antrag gebührenfrei Auskunft zu erteilen. Es gibt im SOG M-V keine weiteren Anforderungen, die an ein Auskunftsersuchen zu stellen wären.

Gemäß § 24 Abs. 1 Satz 2 Landesdatenschutzgesetz soll zwar die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden, um es der Daten verarbeitenden Stelle zu erleichtern, die Daten zu finden. Dies heißt jedoch nicht, dass in jedem Fall eine nähere und schlüssige Bezeichnung erfolgen muss. Gerade im Polizeibereich, in dem sich der Bürger mit einer äußerst komplexen Datenverarbeitung konfrontiert sieht, ist es ihm nicht immer möglich, die Art der Daten und den Grund oder gar den Ort einer eventuellen Speicherung näher zu bezeichnen. Er wird nicht in jedem Fall über laufende und abgeschlossene Ermittlungsverfahren in Kenntnis gesetzt und kennt auch nicht jede Datei der Polizei, in der möglicherweise Daten zu seiner Person enthalten sein könnten. Darüber hinaus könnte sich der Betroffene mit einer detaillierten Bezeichnung der von ihm gewünschten Daten der Gefahr neuer, gegen seine Person gerichteter Aktivitäten aussetzen. Eine Selbstbezichtigung muss jedoch in einem Rechtsstaat ausgeschlossen sein.

Ein Identitätsnachweis der Auskunft ersuchenden Person ist verständlicherweise erforderlich, damit personenbezogene Daten nur an Berechtigte herausgegeben werden. Von dem Betroffenen jedoch generell zu verlangen, dass er bei seinem Auskunftsersuchen eine von dem zuständigen Einwohnermeldeamt auszustellende Identitäts- beziehungsweise Meldebestätigung vorzulegen hat, halte ich für zu weitgehend, wenn nicht offensichtlich Zweifel an der Identität des Betoffenen bestehen. Wenn generell eine solche Bescheinigung vorher eingeholt werden muss, wird das Auskunftsrechts unverhältnismäßig einge-

schränkt. Ein solcher Identitätsnachweis sollte nur dann vom Betroffenen verlangt werden, wenn sich aus seinen Angaben oder nach einem Vergleich mit den möglicherweise in den polizeilichen Dateien gespeicherten Angaben Abweichungen und damit tatsächlich Zweifel an seiner Identität ergeben. Bestehen keine Anhaltspunkte für die Annahme einer falschen Identität, reicht es aus datenschutzrechtlicher Sicht aus, wenn sich der Betroffene in seinem schriftlichen Auskunftsersuchen mit der Kopie seines Personalausweises oder Reisepasses ausweist.

Nach eingehender Erörterung der Materie konnte ich mich mit dem Landeskriminalamt auf ein abgestuftes Verfahren verständigen. Die Auskunft wird erteilt, wenn das Ersuchen Namen, Vornamen, Geburtsdatum, Anschrift und Unterschrift enthält und diese Daten mit den bei der Polizei oder dem LKA M-V gespeicherten Daten übereinstimmen. Hat das LKA M-V keine Anschrift des Betroffenen gespeichert, so dass ein Vergleich mit der Anschrift im Anschreiben nicht möglich ist, soll der Betroffene weitere Nachweise zu seiner Identität bringen. Er muss dann die oben genannte Bescheinigung des Einwohnermeldeamtes zusenden oder persönlich erscheinen. Eine Kopie des Personalausweises reicht im schriftlichen Verfahren nicht aus.

Das Landeskriminalamt hat diese Vorgehensweise nunmehr in der Dienstanweisung zur Führung von Kriminalakten festgeschrieben – für den Auskunft ersuchenden Bürger ein erfreuliches Signal.

2.3.3 Rasterfahndung in Mecklenburg-Vorpommern ergebnislos

In meinem Fünften Tätigkeitsbericht hatte ich unter Punkt 3.3.6 ausführlich über die Rasterfahndung nach den Ereignissen des 11. September 2001 berichtet. Alle Landeskriminalämter sollten damals dem Bundeskriminalamt (BKA) die Datensätze aus Meldebehörden, Ausländerbehörden, Sozialämtern, Universitäten, Hochschulen beziehungsweise Fachhochschulen übermitteln, welche die bundesweit vereinbarten Rasterkriterien (männlich, bestimmtes Alter, Student, islamische Religionszugehörigkeit, Geburtsland oder Nationalität) erfüllten. Das Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V) erhob daraufhin ca. 13.600 Datensätze.

Da die einzelnen Institutionen in der Regel nur einen Teil der Daten zu den Betroffenen gespeichert hatten, die für die vollständige Rasterung erforderlich waren, erhielt das LKA M-V auch Daten solcher Personen, auf die nur ein Teil der Auswahlkriterien zutraf. Darüber hinaus wurden einzelne Personen mitunter von mehreren Institutionen gemeldet. Zu Mehrfacherfassungen kam es auch wegen der unterschiedlichen Schreibweisen der arabi-

schen Namen und weil Personen unter Alias-Namen (anderen Namen) gemeldet waren. Nachdem mehrfach gespeicherte Daten einzelner Personen gelöscht wurden, blieben noch rund 9.400 Datensätze übrig. Von diesen erfüllten lediglich 952 Personendatensätze die Rasterkriterien des BKA vollständig. 57 Datensätze von Personen, die ihren Wohnsitz nicht in Mecklenburg-Vorpommern hatten, wurden gemäß den Festlegungen der Koordinierungsgruppe Internationaler Terrorismus an andere Bundesländer übermittelt. Das BKA erhielt dann im Jahr 2002 die verbliebenen 895 Datensätze und speicherte sie zusammen mit den von anderen Bundesländern gelieferten Daten in der Verbunddatei „Schläfer“

Um den Datenbestand weiter einzuschränken, glich das BKA die Daten der Datei „Schläfer“ mit anderen Datenbeständen (so genannten Abgleichsdateien) ab. Maßgeblich hierfür waren weitere Kriterien, die aus den Täterprofilen der zeitweise in Deutschland wohnhaften Attentäter vom 11. September 2001 resultierten. Das Ergebnis des Datenabgleichs wurde in einer so genannten Ergebnisdatei bereitgestellt. Sie enthielt die Datensätze der Datei „Schläfer“, die das BKA nach dem Abgleich als Treffer klassifiziert hatte. Das LKA unseres Landes erhielt vom BKA 280 dieser Datensätze per E-Mail zur weiteren Überprüfung. Letztlich wurden (von den ursprünglich 9.400 gemeldeten!) lediglich drei Treffer registriert. Nach kurzer Zeit stellte sich jedoch heraus, dass diese Personen bereits vor Jahren in andere Bundesländer verzogen waren. Es ergab sich am Ende der insgesamt 13 Abgleichserien keine verdächtige Person für Mecklenburg-Vorpommern.

Aus datenschutzrechtlicher Sicht war sicherzustellen, dass Daten von bereits herausgefilterten „Unverdächtigen“ frühzeitig gelöscht werden. Dies ist für die ursprünglich noch verbliebenen 895 Personendatensätze im Mai 2003 geschehen. Die Verbunddatei „Schläfer“ wurde am 30. Juni 2003 als Datei gelöscht. Mit Ablauf des 21. Juli 2003 waren auch alle Abgleichsdaten gelöscht.

Es ist festzustellen, dass die Daten von fast 10.000 Einwohnern unseres Landes in einen gigantischen Datenabgleich geraten sind, ohne dass ein verdächtiger Einwohner ermittelt wurde. Dieses Resultat mag auf den ersten Blick erfreulich erscheinen. Bei genauerem Hinsehen ist es jedoch nichts anderes als das negative Ergebnis eines aufwändigen Experimentes. Und negative Ergebnisse von Experimenten haben immer den Nachteil, dass sie sich nicht eindeutig interpretieren lassen. Zumindest drei Interpretationen sind möglich:

- unter den Überprüften befand sich tatsächlich kein Terrorist,

- die angewandte Methode ist prinzipiell nicht geeignet, um Terroristen ausfindig zu machen,

- die Methode wurde nicht mit der erforderlichen Genauigkeit beziehungsweise Sorgfalt durchgeführt.

Angesichts dieser Tatsache erscheint es durchaus legitim, einmal wieder darüber nachzudenken, ob die Rasterfahndung als geeignetes und angemessenes Mittel zur Kriminalitätsbekämpfung in Frage kommt.

2.4 Verkehr

2.4.1 Fahrerlaubnisakten zu dick

Ein Petent hatte seine Fahrerlaubnisakte eingesehen und dabei festgestellt, dass darin auch Unterlagen über lange zurückliegende Sachverhalte aufbewahrt wurden. Er hat mich gebeten zu prüfen, ob die Speicherung dieser Daten rechtmäßig sei.

Nach § 2 Abs. 9 Straßenverkehrsgesetz (StVG) sind Registerauskünfte, Führungszeugnisse, Gutachten, Gesundheitszeugnisse und weitere in der Fahrerlaubnisakte enthaltene Unterlagen nach bestimmten Fristen auszusondern und zu vernichten. § 65 Abs. 1 StVG enthält in diesem Zusammenhang eine Übergangsregelung, wonach Unterlagen, die sich bereits vor dem 1. Januar 1999 in den Akten befanden, erst dann zu vernichten sind, wenn der Bearbeiter mit der jeweiligen Akte wieder befasst ist. Diese Altfälle müssen jedoch spätestens bis zum 1. Januar 2014 überprüft sein. Die Unterlagen brauchen nur dann ausnahmsweise nicht vernichtet zu werden, wenn es wegen der besonderen Art der Aktenführung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Aber auch in diesen Fällen muss die Fahrerlaubnisbehörde die Akten prüfen und die zur Aussonderung anstehenden Unterlagen sperren. Gesperrte Daten sind gemäß § 13 Abs. 5 Landesdatenschutzgesetz gesondert zu speichern. Nur wenn dies nicht möglich ist, sind die jeweiligen Daten mit einem Sperrvermerk zu versehen.

In diesem Fall enthielt die Fahrerlaubnisakte des Petenten unter anderem auch umfangreichen Schriftwechsel zu einer gebührenpflichtigen Verwarnung, die im Ergebnis zurückgenommen wurde, Auszüge aus dem örtlichen Fahrerlaubnisregister einer zu einem früheren Zeitpunkt zuständigen Fahrerlaubnisbehörde, den Beschluss eines Amtsgerichtes über die vorläufige Entziehung der Fahrerlaubnis sowie den dazugehörigen Aufhebungsbeschluss.

Die Fahrerlaubnisbehörde bereinigte die Akte umfassend und vernichtete die Unterlagen, die sie nicht mehr brauchte, um ihre Aufgaben zu erfüllen. Des Weiteren sicherte die Behörde zu, künftig regelmäßig zu prüfen, welche Unterlagen aus den Fahrerlaubnisakten auszusondern sind.

Im Rahmen eines Kontroll- und Informationsbesuches bei einer anderen Fahrerlaubnisbehörde wurde mir Folgendes mitgeteilt:

- Die Fahrerlaubnisbehörde bewahrt die Unterlagen über erteilte Fahrerlaubnisse nach der Übernahme der Daten in das Fahrerlaubnisregister jahrgangsweise für fünf Jahre

auf. Anschließend werden die Unterlagen vernichtet. Zuvor wird geprüft, ob Eintragungen im Verkehrszentralregister enthalten sind, die im Einzelfall eine längere Aufbewahrung der Unterlagen erfordern.

- Die weiteren Fahrerlaubnisakten werden in folgende Kategorien unterteilt: Probezeit, Mehrfachtäter, Fahrerlaubnisentzüge und laufende Verfahren. Diese Vorgänge werden einmal jährlich überprüft. Unterlagen, die zur Aufgabenerfüllung nicht mehr erforderlich sind, werden ausgesondert.

- Unterlagen über ein Fahrverbot werden gesondert aufbewahrt und nach dessen Ablauf nicht in die Fahrerlaubnisakte aufgenommen.

- Mitteilungen von Polizeidienststellen über die fehlende Eignung eines Fahrerlaubnisinhabers werden zunächst separat aufbewahrt und erst in die jeweilige Fahrerlaubnisakte übernommen, wenn weitere Maßnahmen durchgeführt werden. Anderenfalls werden diese Unterlagen nach sechs Monaten vernichtet.

- Die Mitarbeiter der Fahrerlaubnisbehörde prüfen schon während der Sachbearbeitung, ob Unterlagen aus den Akten auszusondern sind.

Diese Verfahrensweise genügt den datenschutzrechtlichen Anforderungen. Die Löschfristen werden eingehalten, weil bestimmte Akten separat aufbewahrt und jährlich durchgesehen werden. Bei einer stichprobenweisen Einsichtnahme in die Akten habe ich keine Verstöße gegen datenschutzrechtliche Bestimmungen festgestellt.

Meine Erfahrungen der vergangenen Jahre haben gezeigt, dass Altdatenbestände nur dann bereinigt und Unterlagen nach Ablauf bestimmter Fristen ausgesondert werden, wenn hieran kontinuierlich und aufgrund einheitlicher Vorgaben gearbeitet wird. Daher habe ich das Wirtschaftsministerium unseres Landes über die Prüferkenntnisse informiert und empfohlen, diese im Rahmen der Fachaufsicht zu berücksichtigen und falls erforderlich den Fahrerlaubnisbehörden entsprechende Hinweise zu geben.

2.4.2 Ordnungsbehörde „petzte“ beim Dienstvorgesetzten

Eine Mitarbeiterin eines Ordnungsamtes überwachte die Einhaltung der Gurtpflicht im Straßenverkehr. Um Verstöße zu ahnden, fertigte sie Videoaufnahmen von Fahrzeuginsassen an, die nicht angeschnallt waren. Die Aufzeichnungen sollten im anschließenden

Ordnungswidrigkeitenverfahren als Beweismittel genutzt werden. Diese Art der Verkehrsüberwachung erzeugte bei einem Petenten Unmut, und er beleidigte die Verkehrsüberwacherin durch eine eindeutige Geste.

Nach Prüfung der Videoaufzeichnung stellte das Ordnungsamt fest, dass der Petent entgegen des ersten Anscheins doch ordnungsgemäß angeschnallt war. Jedoch war eine Geste zu erkennen, die den Straftatbestand der Beleidigung nach § 185 Strafgesetzbuch (StGB) erfüllt. Da ein Mitarbeiter des Ordnungsamtes den Petenten und auch dessen Dienststelle kannte, wandte sich das Amt mit einer Dienstaufsichtsbeschwerde an den Dienstvorgesetzten des Petenten, um die Angelegenheit auf diese Weise zu klären. Der Petent, der zum Zeitpunkt der Aufnahme nicht dienstlich unterwegs war, hatte Bedenken gegen diese Datenweitergabe und bat mich um eine datenschutzrechtliche Prüfung.

Bereits in der Vergangenheit habe ich die Videoaufzeichnung von Verkehrsordnungswidrigkeiten geprüft. Unter welchen Voraussetzungen diese Maßnahmen zulässig sind, habe ich unter Punkt 3.4.2 meines Fünften Tätigkeitsberichtes dargestellt. Unser Wirtschaftsministerium hat hierzu im Jahre 2002 einen Erlass verabschiedet, in dem eine datenschutzgerechte Verfahrensweise geregelt ist.

Die Aufzeichnung dieses Einzelfalles war gerechtfertigt, da zunächst ein Anfangsverdacht für einen Verstoß gegen die Gurtpflicht bestand. Für diese gespeicherten Daten gilt der Grundsatz der Zweckbindung. Da nach Einsichtnahme in die Aufzeichnung festgestellt wurde, dass keine Verkehrsordnungswidrigkeit vorlag, waren die Daten nicht mehr für die Aufgabenerfüllung des Ordnungsamtes erforderlich und hätten gelöscht werden müssen. Die Daten wurden jedoch aufgrund des Verdachtes einer Straftat nach § 185 StGB weiter gespeichert. Eine Nutzung der Daten für einen anderen Zweck ist nur unter gesetzlich bestimmten Voraussetzungen zulässig, so auch zur Verfolgung von Straftaten. Das Ordnungsamt verwendete die Daten jedoch nicht für diesen Zweck. Es erstattete keine Strafanzeige, sondern informierte den Arbeitgeber des Petenten. Für diese Übermittlung und die damit verbundene zweckändernde Nutzung der Daten existiert keine Rechtsgrundlage. Die Vorgehensweise des Ordnungsamtes war somit unzulässig.

Hätte das Ordnungsamt eine Strafanzeige erstattet, wäre – abhängig vom Ausgang des Verfahrens – unter Umständen auch der Dienstvorgesetzte des Petenten informiert worden. Allein der Verdacht einer Straftat genügt für eine solche Mitteilung jedoch nicht. Der Gesetzgeber hat geregelt, wann und unter welchen Voraussetzungen einem Dienstvorgesetzten Informationen über Strafsachen gegen Beamte oder Arbeitnehmer des öffentlichen Dienstes mitzuteilen sind (§ 125c Beamtenrechtsrahmengesetz, § 13 Abs. 2, § 14

Abs. 1 Nr. 5, Abs. 2 Einführungsgesetz zum Gerichtsverfassungsgesetz). Diese Mitteilung obliegt den für das Strafverfahren zuständigen Behörden.

Ich habe der Verwaltung empfohlen, die Mitarbeiter auf den Rechtsverstoß sowie auf die datenschutzrechtlichen Bestimmungen zur Verarbeitung personenbezogener Daten, insbesondere zur Zweckbindung, hinzuweisen. Die Stadt ist meinen Empfehlungen gefolgt und hat zugesichert, dass es sich hierbei um einen Einzelfall handelte. Künftig wird die zweckändernde Nutzung personenbezogener Daten genau geprüft. Den Petenten habe ich über das Ergebnis informiert.

2.4.3 Übersenden von Beweisfotos an die Personalausweisbehörde

Um bei Verkehrsordnungswidrigkeiten den Fahrzeugführer zu ermitteln, kann es notwendig sein, das Beweisfoto mit dem Lichtbild des Betroffenen aus dem Pass- oder dem Personalausweisregister abzugleichen. Dazu sehen die Mitarbeiter der Bußgeldstelle in das Register vor Ort ein. Ist dies nicht möglich, sendet die Bußgeldstelle ein entsprechendes Ersuchen an die Pass- und Personalausweisbehörde – gegebenenfalls über die Meldebehörde –, um zunächst die zuständige Ausweisbehörde zu ermitteln. Von dort erhält die Bußgeldstelle dann das Lichtbild.

Die Bußgeldstelle eines Landkreises fügte ihren Auskunftsersuchen allerdings regelmäßig Kopien der Beweisfotos bei. Auf diese Weise erfuhren die Melde- sowie die Pass- und Personalausweisbehörden Details über die Ordnungswidrigkeiten, die sie für ihre Aufgabenerfüllung nicht benötigten. Der Landkreis begründete sein Vorgehen damit, dass keine gesetzlichen Bestimmungen existierten, die das Mitsenden von Beweisfotos untersagen.

Das Übersenden von Beweisfotos, auf denen Betroffene und das Kfz-Kennzeichen zu erkennen und darüber hinaus auch Angaben zum Tatgeschehen enthalten sind, ist gemäß § 4 Satz 2 Nr. 4 Landesdatenschutzgesetz eine Übermittlung personenbezogener Daten und somit ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen. Die Verarbeitung personenbezogener Daten ist nur auf der Basis einer Rechtsvorschrift oder mit Einwilligung der Betroffenen zulässig. Somit müsste die Übersendung der Fotos gesetzlich erlaubt sein, oder die Betroffenen müssten in die Übersendung eingewilligt haben. Beides ist hier nicht der Fall. Für das oben geschilderte Auskunftsersuchen dürfen nur die erforderlichen Daten an die Melde- sowie die Pass- und Personalausweisbehörden übermittelt werden. Das Beweisfoto gehört jedoch nicht dazu. Die

befragten Behörden können die Auskünfte auch ohne Vorliegen des Fotos geben, da der Betroffene, dessen Lichtbild übermittelt werden soll, im Ersuchen eindeutig zu bezeichnen ist. Somit war die Übersendung der Fotos unzulässig.

Der Landkreis hat hier einen wesentlichen datenschutzrechtlichen Grundsatz nicht beachtet und den Sachverhalt falsch bewertet. Er hätte nicht prüfen müssen, ob eine Rechtsnorm der Datenverarbeitung entgegensteht, sondern ob eine Rechtsvorschrift diese Verarbeitung erlaubt. Ich habe deshalb empfohlen, diese rechtswidrige Praxis umgehend einzustellen. Der Landkreis ist der Empfehlung gefolgt.

2.4.4 Videoüberwachung in öffentlichen Verkehrsmitteln

Ein Verkehrsunternehmen beabsichtigte, seine Straßenbahnen mit Videokameras auszurüsten. Es hält den Einsatz dieser Überwachungstechnik für notwendig, um die Fahrgäste sicher befördern und vor Gewalt schützen zu können und um Vandalismusschäden zu verhindern. Zuvor hatte das Unternehmen durch entsprechende Tests festgestellt, dass Straftaten in Straßenbahnen auch mit mehr Personal nicht zu verhindern sind. Ein auf Dauer angelegter noch umfassenderer Personaleinsatz wäre finanziell nicht zu tragen gewesen.

Für das Verkehrsunternehmen ist die Zulässigkeit der Videoüberwachung gemäß § 2 Abs. 5 Landesdatenschutzgesetz nach § 6b Bundesdatenschutzgesetz zu beurteilen. Die Beobachtung öffentlich zugänglicher Räume mittels Videoüberwachung ist hiernach unter anderem zulässig, wenn sie zur Wahrnehmung des Hausrechtes erforderlich ist und die schutzwürdigen Interessen der Betroffenen nicht überwiegen. Die erhobenen Daten dürfen weiter verarbeitet werden, wenn dies zum Erreichen des verfolgten Zweckes notwendig ist. Dabei sind ebenfalls die schutzwürdigen Interessen der Betroffenen zu beachten. Eine Verarbeitung der Daten zu einem anderen Zweck ist unter anderem zulässig, um Straftaten zu verfolgen. Liegen diese Voraussetzungen nicht oder nicht mehr vor, dürfen die Daten nicht verarbeitet werden und sind unverzüglich zu löschen. Darüber hinaus müssen die Fahrgäste durch entsprechende Hinweisschilder auf die Videoüberwachung aufmerksam gemacht werden.

Ich habe das Vorhaben als zulässig bewertet und Hinweise für eine datenschutzgerechte Realisierung des Verfahrens gegeben. Das Verkehrsunternehmen hat das Vorhaben unter Berücksichtigung meiner Empfehlungen wie folgt umgesetzt:

- Die Fahrgäste werden durch deutlich sichtbare Piktogramme in jedem Fahrzeug auf die Videoüberwachung aufmerksam gemacht. Für Nachfragen ist als Ansprechpartner der betriebliche Datenschutzbeauftragte genannt.

- Die Videoaufnahmen vom Fahrzeuginnenraum werden 16 Stunden hintereinander auf einer besonders gesicherten Festplatte aufgezeichnet und danach automatisch überschrieben.

- Aufgezeichnet wird ausschließlich zum Zwecke der Beweissicherung.

- Der Fahrer des Fahrzeuges hat keinen Zugang zu den gespeicherten Daten. Soll ein aufgezeichnetes Ereignis erhalten bleiben, beauftragt die Leitstelle des Verkehrsunternehmens einen berechtigten Mitarbeiter, die Datenaufzeichnung zu dem jeweiligen Geschehen zu sichern. Dieser Vorgang wird dokumentiert.

- Die aufgezeichneten Videosequenzen dürfen nur als Beweismittel genutzt und hierfür an die Polizei, die Staatsanwaltschaft beziehungsweise das Gericht übermittelt werden. Nach Abschluss des jeweiligen Verfahrens sind die Daten beim Verkehrsunternehmen zu löschen.

- Die Einzelheiten des Verfahrens sind in einer Betriebsanordnung detailliert festgelegt.

- Nach Ablauf von zwei Jahren überprüft das Verkehrsunternehmen, ob und inwieweit die mit der Videoüberwachung verfolgten Zwecke erreicht wurden und ob ein weiterer Einsatz dieser Technik erforderlich ist.

Auf diese Weise wird dem Recht auf informationelle Selbstbestimmung der Betroffenen hinreichend Rechnung getragen.

2.5 Verfassungsschutz

2.5.1 Novellierung des Landesverfassungsschutzgesetzes

Im Juli 2003 erhielt ich aus unserem Innenministerium einen Gesetzentwurf, der Vorschriften auf dem Gebiet des Verfassungsschutzes novellieren soll, zur Stellungnahme. Der Entwurf sieht unter anderem vor, der Verfassungsschutzbehörde unseres Landes neue Befugnisse zur Erfüllung ihrer Aufgaben zuzuweisen. Die Behörde soll künftig von den Banken Daten über Kontenbewegungen, von den Luftverkehrsunternehmen alle Reisedaten und von den Post- und Telekommunikationsunternehmen alle Informationen darüber bekommen, wer zum Beispiel von wem Post erhalten oder wer wann und mit wem telefoniert hat. Diese Maßnahmen werden damit begründet, dass auch in unserem Bundesland der internationale Terrorismus wirksam bekämpft werden müsse. Es wird darauf verwiesen, dass diese Befugnisse dem Bundesamt für Verfassungsschutz nach dem Terrorismusbekämpfungsgesetz bereits zustehen.

Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte in Frage stellen. Es ist zu befürchten, dass eine ständig zunehmende staatliche Überwachung die freie und unbeobachtete Aktion, Bewegung und Kommunikation der Bürger immer weiter einschränkt. Ohnehin ist fraglich, ob die vorgeschlagenen Maßnahmen ausreichend dazu beitragen, den internationalen Terrorismus wirksam zu bekämpfen, und ob sie dem Grundsatz der Verhältnismäßigkeit genügen. Viel wichtiger sind meines Erachtens „verfahrenssichernde“ Maßnahmen, beispielsweise eine umfassende Information und Kontrollmöglichkeit durch die G 10-Kommission beziehungsweise die Parlamentarische Kontrollkommission, aussagekräftige Berichtspflichten des Innenministers, eine Evaluierung der Maßnahmen oder eine Befristung des Gesetzes.

In meiner Stellungnahme habe ich auf folgende Aspekte besonders hingewiesen:

- Soll die Verfassungsschutzbehörde tatsächlich die oben genannten, einschneidenden und umfassenden Befugnisse erhalten, sind sie nach dem Prinzip der Normenklarheit auszuformulieren. Umfang und Ausmaß der Datenerhebung sind daher konkret im Landesgesetz zu regeln. Dies entspricht dem Transparenzgebot. Der alleinige Bezug auf die entsprechenden Bestimmungen des Bundesverfassungsschutzgesetzes reicht als Begründung keinesfalls aus.

- Der Gesetzentwurf sieht vor, dass der Leiter der Verfassungsschutzbehörde die oben genannten Datenerhebungen schriftlich beim Innenminister beantragen muss. Ich habe vorgeschlagen, diesen Antrag detailliert zu begründen. Nur durch eine solche Begründung kann nachvollzogen werden, warum im Einzelfall sehr sensible Daten wie Kontostände oder Telefongesprächsdaten zur Bekämpfung des internationalen Terrorismus notwendig sind.

- Des Weiteren habe ich empfohlen, dass die Parlamentarische Kontrollkommission umfassender als im Gesetzentwurf vorgesehen über Anlass, Dauer, Umfang, Ergebnis und Kosten der durchgeführten Maßnahmen unterrichtet wird.

- Die Rechte des Betroffenen sind aus datenschutzrechtlicher Sicht ebenfalls zu stärken.

Es bleibt abzuwarten, ob die Landesregierung meine Empfehlungen aufgreift.

2.5.2 Einmal im Verfassungsschutzbericht – für immer im Internet?

Ein Petent aus einem anderen Bundesland hatte in mindestens zwei Fällen wegen einer dauerhaften Veröffentlichung seiner Daten in einem Verfassungsschutzbericht aus den 80er-Jahren negative Auswirkungen auf seine berufliche Laufbahn als Künstler erfahren. Dabei ging es unter anderem um strafrechtliche Verurteilungen, die im Bundeszentralregister bereits getilgt waren. Trotzdem war es für jedermann möglich, diese Daten beispielsweise über eine Suchmaschine im Internet zu recherchieren und auf der Homepage der Verfassungsschutzbehörde einzusehen.

In Mecklenburg-Vorpommern regelt § 22 Landesverfassungsschutzgesetz (LVerfSchG M-V) Datenübermittlungen an die Öffentlichkeit. Danach dürfen personenbezogene Daten nur dann veröffentlicht werden, wenn dies zu einer sachgemäßen Information der Öffentlichkeit über Erkenntnisse der Verfassungsschutzbehörde erforderlich ist. Eine Voraussetzung für personenbezogene Veröffentlichungen ist somit, dass die Informationen zu einer Person für das Verständnis von Zusammenhängen oder der Darstellung von Organisationen überhaupt erforderlich sind. Der Veröffentlichung dürfen darüber hinaus keine schutzwürdigen Interessen der betroffenen Person entgegenstehen. Weist beispielsweise das Führungszeugnis einer Person keine Eintragungen mehr auf, dürfen ihr die Tat und die Verurteilung im Rechtsverkehr nicht mehr vorgehalten oder zu ihrem Nachteil verwendet werden. Dies bedeutet beispielsweise, dass nach der Tilgung der entsprechenden

Eintragung im Bundeszentralregister auch kein Verfassungsschutzbericht personenbezogene Darstellungen der Tat mehr enthalten darf.

Die Verfassungsschutzbehörde unseres Landes hat mir mitgeteilt, dass sie generell nur Daten von Personen veröffentlicht, die in besonderem Maße und über einen längeren Zeitraum als Träger von Bestrebungen im Sinne von § 5 Abs. 1 LVerfSchG M-V (also Personen, die verfassungsfeindliche Ziele verfolgen) anzusehen sind und daher über einen entsprechenden Bekanntheitsgrad verfügen. Dies sind zum Beispiel Führungspersonen, die in der Regel von sich aus die Öffentlichkeit suchen.

Damit Daten nicht jahrzehntelang weltweit über Internetseiten der Verfassungsschutzbehörde abgerufen werden können, ist beabsichtigt, die Berichte nach Ablauf von fünf Jahren vom Webserver zu nehmen. Allerdings kann damit nicht verhindert werden, dass Kopien der Berichte weiterhin im Internet verfügbar und recherchierbar sind. Dennoch trägt diese Verfahrensweise dazu bei, die schutzwürdigen Belange Betroffener besser zu wahren.

2.6 Einwohnerwesen

2.6.1 Kurverwaltung – Meldebehörde für Touristen?

Kur- und Erholungsorte dürfen nach § 11 Kommunalabgabengesetz Mecklenburg-Vorpommern eine Kurabgabe erheben, um öffentliche Einrichtungen zu finanzieren, die Kur- und Erholungszwecken dienen. Urlauber sind nach der Kurabgabesatzung verpflichtet, die hierfür erforderlichen Auskünfte zu erteilen. Sie müssen ferner im Rahmen der so genannten Hotelmeldepflicht nach § 26 Landesmeldegesetz (LMG) besondere Meldescheine in den Beherbergungsstätten ausfüllen. Die Durchschriften dieser Meldescheine dürfen nach § 27 Abs. 3 LMG verwendet werden, um die Kurabgabe einzuziehen. Urlauber zahlen in vielen Orten daher regelmäßig bereits bei ihrem Quartiergeber die Kurabgabe, der die Einnahmen zusammen mit den Durchschriften der Meldescheine an die für die Einziehung der Kurabgabe verantwortliche Stelle weiterleitet.

In einem Ostseebad waren einer privatrechtlichen Einrichtung neben der Tourismus- und Fremdenverkehrsförderung auch die Aufgaben der Kurverwaltung übertragen worden. Darüber hinaus war auch eine Auftragsdatenverarbeitung nach § 38 LMG vereinbart. Danach sollte die Gesellschaft

- die Durchschriften der besonderen Meldescheine der Beherbergungsstätten nutzen, um ein zentrales Gästeregister für die Meldebehörde zu führen,

- diese Unterlagen jederzeit und uneingeschränkt für die Meldebehörde bereithalten,

- dafür sorgen, dass sich die Gäste nach § 26 Abs. 2 LMG in den Beherbergungsstätten anmelden und

- Verstöße gegen diese Vorschrift der Meldebehörde mitteilen.

Die Art der Auftragsdatenverarbeitung entsprach nicht den Bestimmungen des Landesmeldegesetzes. Deshalb habe ich diesen Sachverhalt gemäß § 32 Abs. 1 Satz 1 Nr. 2 Landesdatenschutzgesetz beanstandet.

Mit der Vereinbarung zur Auftragsdatenverarbeitung hatte die Gesellschaft Befugnisse erhalten, die selbst der Meldebehörde nicht zustehen. Ferner war zu berücksichtigen, dass hoheitliche Aufgaben nur auf der Basis einer gesetzlichen Regelung und nicht über den Weg der Auftragdatenverarbeitung übertragen werden dürfen.

Urlauber in Beherbergungsstätten, deren Aufenthalt die Dauer von zwei Monaten nicht übersteigt, unterliegen keiner allgemeinen Meldepflicht. Der Gesetzgeber verzichtet bei diesen vorübergehenden Aufenthalten auf die Anmeldung bei der Meldebehörde und auf eine damit verbundene Speicherung im Melderegister. Stattdessen gilt für sie die so genannte Hotelmeldepflicht nach § 26 LMG. Die Gäste müssen die oben genannten besonderen Meldescheine in den Beherbergungsstätten ausfüllen. Die Meldebehörden und die Polizei können diese Meldescheine vor Ort einsehen. Lediglich die Polizei kann im Einzelfall verlangen, dass ihr die Meldescheine ausgehändigt werden. Für die Übermittlung der Daten an die Meldebehörde, die sie an zentraler Stelle speichert und somit ein zentrales Urlauberregister für meldebehördliche Zwecke einrichtet, gibt es aber keine Rechtsgrundlage. Die fehlende Befugnis der Meldebehörde kann deshalb auch nicht im Rahmen einer Auftragsdatenverarbeitung übertragen werden.

Die für die Erhebung der Kurabgabe zuständige Stelle erhält eine Durchschrift der besonderen Meldescheine. Diese Daten dürfen nur zweckgebunden für die Kurabgabe genutzt werden, nicht jedoch für melderechtliche Aufgaben. Vielmehr ist die Datenverarbeitung nach den melderechtlichen Vorschriften einerseits und nach den abgaberechtlichen Bestimmungen andererseits deutlich zu trennen.

Ferner ist allein die Meldebehörde berechtigt, Verstöße gegen das Landesmeldegesetz bei der Anmeldung von Gästen in Beherbergungsstätten und damit verbundene Ordnungswidrigkeiten festzustellen. Es handelt sich hier um eine hoheitliche Tätigkeit, die nicht einfach per Vertrag übertragen werden kann. Der Sachverhalt ist im Einzelfall durch die Meldebehörde aufzuklären. Es ist nicht zulässig, Private ohne gesetzliche Grundlage hinzuzuziehen.

Die Meldebehörde darf nach § 38 LMG andere Meldebehörden oder geeignete öffentlich- oder privatrechtliche Einrichtungen in Mecklenburg-Vorpommern beauftragen, melderechtliche Aufgaben mit Hilfe automatisierter Verfahren durchzuführen. Um die melderechtlichen Vorschriften einzuhalten, sind allerdings technische und organisatorische Vorkehrungen erforderlich. Die Meldebehörde bleibt weiterhin in vollem Umfang für die Wahrnehmung der melderechtlichen Aufgaben verantwortlich. Die Auftragsdatenverarbeitung stellt lediglich eine automatisierte verfahrenstechnische Unterstützung dar. § 38 LMG war in diesem Fall jedoch nicht anwendbar, weil eine solche Auftragsdatenverarbeitung nicht beabsichtigt war.

Im Rahmen einer Beratung hatte ich die Stadt bereits frühzeitig darauf hingewiesen, dass die vertraglichen Regelungen den melderechtlichen Bestimmungen widersprechen. Die

Stadt reagierte auf meine Hinweise trotz mehrfacher Aufforderungen nicht. Erst meine Beanstandung führte zu einem Umdenken in der Verwaltung. Der Bürgermeister sicherte zu, die entsprechenden Regelungen zu ändern, um künftig eine datenschutzgerechte Verfahrensweise zu gewährleisten.

2.6.2 Falsche Daten im Melderegister

Eine Petentin hatte als Hauseigentümerin von der Amtsverwaltung einen Abgabenbescheid zur Abwasserabgabe für Kleineinleiter erhalten. Die Abgabenhöhe richtete sich unter anderem nach der Anzahl der im Haus lebenden Personen. In diesem Bescheid waren jedoch anstelle der zwei in diesem Haus lebenden Personen drei Personen eingetragen. Die Verwaltung berief sich dabei auf das Melderegister, wonach für den fraglichen Zeitraum eine weitere Person dort gemeldet war. Sie lehnte den Widerspruch der Petentin ab, worauf diese klagte. Das Verwaltungsgericht entschied auf Basis des Melderegisterauszuges gegen die Petentin. Da die Eintragung im Melderegister offensichtlich fehlerhaft war, bat sie mich um Unterstützung.

Im vorliegenden Fall war eine weitere Person mit Nebenwohnsitz für das Haus der Petentin im Melderegister eingetragen. Auf Betreiben der Petentin hatte diese Person der Meldebehörde inzwischen mitgeteilt, dass dieser Wohnsitz seit mehr als 17 Jahren nicht mehr besteht. Die für den Hauptwohnsitz zuständige Meldebehörde hatte dies bestätigt. Da der Sachverhalt viele Jahre zurücklag, konnte die Ursache für die fehlerhafte Speicherung nicht mehr ermittelt werden. Die Meldebehörde bereinigte das Melderegister rückwirkend, und der Bescheid zur Deckung der Abwasserabgabe wurde im weiteren Verfahren auf zwei Personen geändert.

Aufgabe der Meldebehörde ist es, die Einwohner zu registrieren, um deren Identität und Wohnsitze feststellen zu können. Sie erteilt Melderegisterauskünfte und übermittelt Daten, damit andere öffentliche Stellen ihre Aufgaben erfüllen können. Die Speicherung richtiger Daten im Melderegister ist sowohl für Betroffene als auch für die Verwaltung insbesondere dann von Bedeutung, wenn die Daten Grundlage für Verwaltungsentscheidungen sind. Unrichtige Daten können zu fehlerhaften Entscheidungen und unter Umständen auch zu erheblichen Nachteilen für die betroffenen Personen führen. Daher trägt die Meldebehörde als Anlaufstelle für viele Behörden, Einrichtungen und Privatpersonen eine besondere Verantwortung.

Nach § 10 Landesmeldegesetz hat die Meldestelle fehlerhafte Daten von Amts wegen oder auf Antrag des Betroffenen zu berichtigen. Bei der Anzahl der in einem Haus lebenden Personen handelt es sich um ein Datum, das für den Eigentümer als Abgabenpflichtigen von besonderer Relevanz ist, weil es als Berechnungsgrundlage für die Erhebung bestimmter Abgaben dient. Der Eigentümer ist nicht dafür verantwortlich, dass Mieter ihren melderechtlichen Pflichten nachkommen. Das Landesmeldegesetz sieht lediglich eine Mitwirkungspflicht bei der An- und Abmeldung vor. So hat der Vermieter den Ein- und Auszug des Meldepflichtigen schriftlich zu bestätigen und der Meldebehörde auf Anfrage Auskünfte zu erteilen. Es existiert jedoch keine Ersatzmeldepflicht.

Der Fehler im Melderegister durfte nicht zu Lasten der Eigentümerin gehen, da sie keinen Einfluss auf das Meldeverhalten ehemaliger Hausbewohner nehmen kann. Zu kritisieren war daher, dass die Amtsverwaltung nicht frühzeitig auf die Einlassungen der Petentin reagiert und das Register berichtigt hatte.

2.6.3 Meldedatenübermittlung zum Aufbau eines Katastrophenschutzregisters?

Den Katastrophenschutzbehörden müssen bestimmte Daten der Einwohner zur Verfügung stehen, um bei entsprechenden Gefährdungen die notwendigen Maßnahmen durchführen zu können. Ein Landkreis hatte daher die Meldebehörden aufgefordert, die Daten aller Einwohner des Landkreises, unter anderem Vor- und Familiennamen, Doktorgrad, Anschriften, Tag und Ort der Geburt, frühere Namen, Staatsangehörigkeit, verheiratet oder nicht, Tag des Ein- und Auszuges, zu übermitteln. Die Daten sollten in einer Datenbank gespeichert und monatlich durch die Meldebehörden aktualisiert werden. Der Landkreis stützte diese Datenübermittlung auf § 31 Landesmeldegesetz (LMG). Eine Meldebehörde zweifelte an der Rechtmäßigkeit dieses Vorhabens und bat mich um eine datenschutzrechtliche Prüfung.

Meldebehörden dürfen nach § 31 Abs. 1 LMG Daten aus dem Melderegister an andere öffentliche Stellen übermitteln, sofern diese zur Aufgabenerfüllung des Empfängers erforderlich sind. Die Aufgaben der Katastrophenschutzbehörden sind im Landeskatastrophenschutzgesetz (LKatSG M-V) festgelegt. Um Katastrophenschutzmaßnahmen vorbereiten und durchführen zu können, dürfen diese Behörden personenbezogene Daten verarbeiten (§ 35 LKatSG M-V). Die Einrichtung eines zentralen Katastrophenschutzregisters beim Landkreis, in dem die Daten sämtlicher Einwohner auf Vorrat gespeichert werden, ist hiernach jedoch nicht vorgesehen. Ohnehin wäre der Umfang der angefor-

derten Daten zu weitgehend, da mehr Informationen erhoben werden sollten, als im Katastrophenfall tatsächlich erforderlich sind.

Auch der geplante Änderungsdienst wäre nicht zulässig. Es existiert keine bundes- oder landesrechtliche Vorschrift, die eine regelmäßige Meldedatenübermittlung zum Zwecke der Datenpflege eines Katastrophenschutzregisters zulässt.

Eine Speicherung auf Vorrat ist schon deshalb nicht notwendig, weil die technischen Möglichkeiten inzwischen so weit entwickelt sind, dass Datenbestände auch in kürzester Zeit an die Katastrophenschutzbehörde übermittelt werden können. Dazu muss aber bereits im Vorfeld feststehen, welche Daten tatsächlich erforderlich und welche technischen Voraussetzungen nötig sind.

Werden Daten auf Ersuchen des Empfängers übermittelt, trägt dieser die Verantwortung für die Zulässigkeit der Übermittlung (§ 14 Abs. 2 Satz 2 Landesdatenschutzgesetz). Deshalb habe ich dem Landkreis empfohlen, davon abzusehen, die Daten zu erheben. Er sicherte zu, bis zu einer abschließenden Klärung der Rechtslage seine Aktivitäten ruhen zu lassen, und informierte hierüber auch die Meldebehörden.

Ich habe das Innenministerium als zuständige oberste Aufsichtsbehörde für den Katastrophenschutz und das Meldewesen über den Sachverhalt und meine Bewertung unterrichtet. Es hat die Angelegenheit geprüft und ein datenschutzkonformes Verfahren festgelegt. Die Meldebehörden stellen danach den Katastrophenschutzbehörden im Katastrophenfall innerhalb von sechs Stunden folgende Angaben ihrer Einwohner zur Verfügung: Vor- und Familienname, Anschriften, Tag und Ort der Geburt sowie Geschlecht. Hierfür sind die notwendigen technischen und organisatorischen Voraussetzungen zu schaffen.

Das Innenministerium hat die zuständigen kommunalen Behörden über die Rechtslage und über die nunmehr festgelegte Verfahrensweise informiert.

2.6.4 Datenerhebung durch Gebührenbeauftragten des Norddeutschen Rundfunks

Ein Gebührenbeauftragter des Norddeutschen Rundfunks (NDR) wollte die Anschriften sämtlicher Einwohner einer Stadt nutzen, um die Rundfunkgebührenpflicht festzustellen. Die Mitarbeiterin der Meldebehörde hatte datenschutzrechtliche Bedenken, die Meldedaten zu übermitteln, und bat mich um eine Bewertung des Sachverhaltes.

Um die Einziehung der Rundfunkgebühren zu unterstützen, hat der Gesetzgeber verschiedene Übermittlungsregelungen geschaffen. Für die gewünschte umfassende Datenübermittlung existiert jedoch keine Rechtsgrundlage.

So dürfen die Meldebehörden dem NDR beziehungsweise der von ihm beauftragten Gebühreneinzugszentrale (GEZ) bei der Anmeldung und Abmeldung einer Wohnung oder im Todesfall unter anderem die Namen und Anschriften der volljährigen Einwohner mitteilen (Artikel 5 Abs. 1 des Gesetzes zum Staatsvertrag über den Norddeutschen Rundfunk).

Ferner dürfen die Meldebehörden gemäß § 31 Abs. 1 Landesmeldegesetz (LMG) im Einzelfall Daten an öffentliche Stellen übermitteln, soweit diese zur Aufgabenerfüllung des Empfängers erforderlich sind. Der NDR ist nach § 4 Abs. 6 Rundfunkgebührenstaatsvertrag berechtigt, entsprechende Auskünfte bei den Meldebehörden über Personen einzuholen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie ihrer Anzeigepflicht als Rundfunkteilnehmer nicht oder nicht vollständig nachgekommen sind. Voraussetzung ist weiter, dass die Daten zur Überwachung der Rundfunkgebührenpflicht erforderlich sind und beim Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können. Die Gebührenbeauftragten dürfen nach der Satzung des NDR ebenfalls diese für den NDR gesetzlich bestimmten Auskünfte verlangen.

Ich habe deshalb der Stadt empfohlen, keine Meldedaten in diesem Umfang zu übermitteln. Des Weiteren habe ich den Datenschutzbeauftragten des NDR eingeschaltet, der den Sachverhalt umgehend geklärt hat. Der Gebührenbeauftragte des NDR hat von seinem Ansinnen Abstand genommen. Über dieses Ergebnis habe ich die Meldebehörde informiert.

2.7 Bau-, Wohnungs- und Liegenschaftswesen

2.7.1 Standortverzeichnisse von Mobilfunkantennen

Immer häufiger wenden sich Bürger an ihre Kommune, um die Standorte von Mobilfunkantennen in ihrer Umgebung zu erfragen. Deshalb haben viele Kommunen in Verzeichnissen die Standorte mit Straßen und Hausnummern der Grundstückseigentümer veröffentlicht. Es entspann sich eine öffentliche Diskussion darüber, ob dies datenschutzrechtlich zulässig ist.

Aufgrund der bundesweiten Bedeutung dieser Frage fordern die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 24./25. Oktober 2002 (siehe Anlage 8) den Bundesgesetzgeber auf, die Erstellung und Veröffentlichung derartiger Verzeichnisse gesetzlich zu regeln.

Als Reaktion auf diese Entschließung sagte das Bundesministerium für Wirtschaft und Arbeit zu, die erforderlichen gesetzlichen Grundlagen für ein Mobilfunkkataster zu schaffen und der Öffentlichkeit die bereits vorhandene Standortdatenbank der Regulierungsbehörde für Post und Telekommunikation zugänglich zu machen.

2.7.2 Veröffentlichung von Eigentümernamen bei Grenzfeststellungen von Grundstücken

Ein Amt für Landwirtschaft gab in einem amtlichen kommunalen Mitteilungsblatt die Grenzfeststellung für ein Gebiet öffentlich bekannt und nannte dabei die Namen der Grundstückseigentümer. Mein Informationsbesuch in dem Amt ergab, dass einige Vermessungsstellen die Namen der Eigentümer nicht veröffentlichen. Daher stellt sich die Frage, unter welchen Umständen die öffentliche Bekanntgabe der Namen erforderlich und somit auch zulässig ist.

Maßgeblich ist § 18 des Vermessungs- und Katastergesetzes (VermKatG). Danach sind den Eigentümern der betroffenen Grundstücke und anderen Berechtigten Zeit und Ort des Grenztermins rechtzeitig mitzuteilen, damit sie sich zur geplanten Grenzfeststellung äußern können. Das Ergebnis der Grenzfeststellung ist während des Grenztermins bekannt zu geben. Abwesende Beteiligte sind darüber schriftlich – in begründeten Einzelfällen durch öffentliche Bekanntgabe – zu unterrichten.

Um eine einheitliche und datenschutzgerechte Vorgehensweise zu erreichen, habe ich mich mit dem Innenministerium unseres Landes als oberster Vermessungsbehörde in Verbindung gesetzt. Ergebnis dieser konstruktiven Zusammenarbeit mit den Mitarbeitern der Vermessungsabteilung war der „Erlass zum Umgang mit personenbezogenen Daten in Grenzfeststellungs- und Abmarkungsverfahren“, der meine inhaltlichen Empfehlungen vollständig berücksichtigt. Der Erlass regelt verbindlich:

„1. Eine ortsübliche Bekanntmachung als Mitteilung des Grenztermins nach § 18 Abs. 2 Satz 2 VermKatG kommt nur im Hinblick auf diejenigen Beteiligten in Betracht, deren Namen oder Adressen nicht ermittelbar sind. Den übrigen Beteiligten ist der Termin schriftlich, mündlich oder fernmündlich mitzuteilen.

Konnten Namen von Beteiligten nicht ermittelt werden, erfolgt eine ortsübliche Bekanntmachung mit Hinweis auf Ort, Datum und Uhrzeit des Grenztermins. Sind Adressen von einzelnen Beteiligten nicht ermittelbar, werden in der ortsüblichen Bekanntmachung die Namen dieser Personen aufgeführt. Weitere personenbezogene Daten, zum Beispiel Art und Umfang der Beteiligung am Verfahren, werden nicht genannt.

2. Eine Offenlegung im Sinne des § 18 Abs. 3 VermKatG darf nur in begründeten Fällen, insbesondere bei trotz hinreichenden Aufwandes nicht zu ermittelnden Adressaten der Verwaltungsakte oder bei einer großen Anzahl Beteiligter, angewendet werden.

In der Bekanntgabe über die Offenlegung sind die Angaben auf Gemeinde, Gemarkung, Flur und Flurstück zu beschränken. Personenbezogene Daten wie Name und Vorname der Beteiligten sind nicht bekannt zu machen.“

Diese Verfahrensweise stellt sicher, dass die einzelnen Vermessungsstellen im Land bei Veröffentlichungen künftig in gleicher Weise verfahren werden und die schutzwürdigen Belange der Grundstückseigentümer somit gewahrt bleiben.

2.8 Kommunales

2.8.1 Vertrauliche Themen bei Dienstbesprechungen im Amt

Eine Petentin hatte im Rahmen eines gewerberechtlichen Verfahrens einen Bußgeldbescheid erhalten und dagegen Einspruch eingelegt. Diesen Einspruch erörterte das Ordnungsamt auf der wöchentlichen Dienstbesprechung der Amtsverwaltung, an welcher der leitende Verwaltungsbeamte, die Leiter der Fachbereiche sowie die Bürgermeister der amtsangehörigen Gemeinden teilnehmen. Dabei wurde allen Teilnehmern der Name der Petentin, die Art ihrer Tätigkeit und die Tatsache, dass sie Beteiligte eines gegen sie gerichteten Bußgeldverfahrens ist, offenbart. Anschließend wurde das Protokoll, das diese persönlichen Angaben enthielt, an die Leiter und Bürgermeister verschickt. Die Petentin hat sich bei mir über dieses Verfahren beschwert und mich gebeten, die Zulässigkeit der Datenweitergabe zu prüfen.

Die Erörterung des Einspruchs unter Verwendung der personenbezogenen Daten war gemäß § 7 Abs. 1 Landesdatenschutzgesetz (DSG M-V) unzulässig, da hierfür keine Rechtsgrundlage existierte und die Betroffene auch nicht in das Verfahren eingewilligt hatte.

Personenbezogene Daten dürfen nach § 10 Abs. 1 DSG M-V nur genutzt werden, wenn und soweit dies zur Erfüllung einer in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgabe erforderlich ist. Aufgrund des Einspruchs musste das Ordnungsamt nach § 69 Abs. 2 des Gesetzes über Ordnungswidrigkeiten prüfen, ob es den Bußgeldbescheid aufrechterhält oder zurücknimmt. Dafür war es nicht erforderlich, die personenbezogenen Daten der Petentin auf der Dienstbesprechung zu offenbaren. Erforderlich ist die Verarbeitung personenbezogener Daten nur, wenn die Aufgabe ohne diese Daten nicht oder nicht vollständig erfüllt werden kann. Auf eine bloße Nützlichkeit bestimmter Daten kommt es dabei nicht an. Für seine Entscheidung hatte das Ordnungsamt zunächst den Sachverhalt zu klären und anschließend die Rechtsfrage zu entscheiden. Die Erörterung der Angelegenheit auf der Dienstbesprechung diente lediglich der Klärung der Rechtsfrage. Hierfür war die Preisgabe der persönlichen Angaben nicht erforderlich. Diese Frage hätte genauso gut abstrakt erläutert werden können.

Ebenso war es unzulässig, das Protokoll mit den persönlichen Angaben zu versenden, weil diese weder für Aufgaben der versendenden noch für Aufgaben der empfangenden Stelle erforderlich waren.

Darüber hinaus ist zu berücksichtigen, dass die Mitarbeiter der einzelnen Fachbereiche dem Datengeheimnis nach § 6 DSG M-V unterliegen. Das Datengeheimnis gilt nicht nur gegenüber außerhalb des Amtes stehenden Dritten, sondern auch gegenüber anderen Fachbereichen desselben Amtes. Für bestimmte Fachbereiche gelten darüber hinaus noch spezielle Datengeheimnisse, wie das Sozialgeheimnis nach § 35 Abs. 1 des Ersten Buches des Sozialgesetzbuches oder das Steuergeheimnis nach § 30 Abs. 1 Abgabenordnung.

Ich habe den leitenden Verwaltungsbeamten über meine Bewertung informiert und ihm folgende Punkte für die Gestaltung von Dienstbesprechungen empfohlen:

- Der Teilnehmerkreis der Dienstbesprechungen sollte über die Bedeutung und Reichweite des Datengeheimnisses belehrt werden.

- Im Kreis aller Fachbereiche sollten nur Angelegenheiten besprochen werden, die keine personenbezogenen Daten beinhalten.

- Angelegenheiten mit Personenbezug sollte der jeweilige Fachbereich allein mit dem leitenden Verwaltungsbeamten erörtern. Sofern diese Sachverhalte ins Protokoll aufgenommen werden, sollte dies nur anonymisiert geschehen.

Der leitende Verwaltungsbeamte hat zugesagt, diese Empfehlungen künftig zu berücksichtigen.

2.8.2 Datenübermittlung aus Bauakten

Ein Mitarbeiter eines Bauamtes hat mich zu folgendem Sachverhalt um eine datenschutzrechtliche Bewertung gebeten:

Ein Bauherr hatte einen Architekten mit der Planung seines Bauvorhabens beauftragt. Die Bauverwaltung lehnte den Bauantrag ab, worauf der Bauherr dem Architekten kein Honorar zahlte. Er war der Auffassung, dass der Bauantrag wegen einer fehlerhaften Planung des Architekten nicht genehmigt worden sei. Der Bauherr weigerte sich jedoch, dem Architekten den ablehnenden Bescheid zur Kenntnis zu geben. Um seine Forderungen gegenüber dem Bauherrn geltend zu machen, hatte der Architekt die Bauverwaltung um eine Kopie des Bescheides gebeten.

Die Herausgabe der Kopie des Bescheides war eine Datenübermittlung an eine nichtöffentliche Stelle, die nur unter den Voraussetzungen des § 15 Abs. 1 Satz 2 Landesdatenschutzgesetz (DSG M-V) zulässig ist. Hiernach muss der Antragsteller ein berechtigtes Interesse an den Daten glaubhaft darlegen, und der Betroffene darf kein schutzwürdiges Interesse haben, um die Übermittlung auszuschließen.

Der Architekt hatte glaubhaft dargelegt, dass er diese Informationen benötigt, um prüfen zu können, ob seine Forderungen berechtigt sind und ob er diese auf rechtlichem Wege durchsetzen kann. Insofern besaß er nicht nur ein berechtigtes, sondern sogar ein rechtliches Interesse an der Auskunft.

Ein schutzwürdiges Interesse des Bauherrn stand dieser Auskunftserteilung nicht entgegen. Allein die Unzufriedenheit über die abgelehnte Baugenehmigung und die verweigerte Zahlung des Honorars ließen ein solches nicht erkennen. Da der Architekt die Planung für den Bauherrn erstellt und den Bauantrag als Entwurfsverfasser nach § 66 Landesbauordnung unterschrieben hatte, waren ihm sämtliche Informationen zum Bauvorhaben bereits bekannt, so dass auch insoweit kein schutzwürdiges Interesse des Petenten zu erkennen war. Allein die Ablehnungsgründe waren für den Architekten neu. Diese Informationen waren für ihn von besonderem Interesse, weil sich hieran der Streit um die Zahlung des Honorars entzündet hatte.

Im Ergebnis war es daher zulässig, dem Architekten die Einzelheiten der ablehnenden Entscheidung mitzuteilen. Ich habe das Bauamt hierüber informiert und darauf hingewiesen, dass der Bauherr über die Mitteilung an den Architekten nach § 15 Abs. 1 Satz 3 DSG M-V zu unterrichten ist.

2.9 Telekommunikation und Medien

2.9.1 Abbau des Datenschutzes im Telekommunikationsrecht geplant

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit vier Entschließungen entschieden gegen Bestrebungen gewandt, das Datenschutzniveau in der Telekommunikation zu senken.

Die Entschließung vom 24. Mai 2002 (siehe Anlage 5) kritisiert den damals vorliegenden Entwurf zur Änderung des Telekommunikationsgesetzes. Danach ist jedes Unternehmen, das geschäftsmäßig Telekommunikationsdienste erbringt, verpflichtet, Namen, Anschriften und Rufnummern seiner Kunden zu speichern. Dies betrifft auch Nutzer von Prepaid-Karten, obwohl die Unternehmen die Daten dieser Kunden nicht benötigen. Allein für Zwecke der Sicherheitsbehörden sollen sie gespeichert werden. Des Weiteren sollen diese Behörden mit unvollständigen Suchbegriffen Kundendateien abfragen dürfen, wodurch sie Zugang zu personenbezogenen Daten unbeteiligter Dritter erhalten.

Auf der 64. Konferenz am 24. und 25. Oktober 2002 wurde die „Entschließung zur systematischen verdachtslosen Datenspeicherung in der Telekommunikation und im Internet“ (siehe Anlage 6) verabschiedet. Darin werden die Vorschläge abgelehnt, dass alle Anbieter von Telekommunikations- und Multimediadiensten verpflichtet sein sollen, sämtliche Bestands-, Verbindungs-, Nutzungs- und Abrechnungsdaten auf Vorrat für mindestens ein Jahr verdachtslos zu speichern, auch wenn sie für die Geschäftszwecke der Anbieter nicht (mehr) notwendig sind. Der riesige Datenpool soll nur dem Zugriff der Sicherheitsbehörden dienen.

„Transparenz bei der Telefonüberwachung“ fordert die Entschließung der 65. Datenschutzkonferenz am 27. und 28. März 2003 (siehe Anlage 16). Betreiber von Telekommunikationsanlagen müssen bisher eine Jahresstatistik über die Überwachungsmaßnahmen erstellen, die sie zu Strafverfolgungszwecken durchgeführt haben. Anlass für die Entschließung waren Pläne der Bundesregierung, diese Statistik abzuschaffen. Begründet wird dieses Vorhaben mit einer Entlastung der Telekommunikationsunternehmen von überflüssigen Arbeiten. Zudem wird darauf verwiesen, dass das Bundesjustizministerium eine ähnliche Statistik führt, die sich auf Zahlen der Landesjustizbehörden stützt. In der Entschließung wird erläutert, dass die Statistik des Bundesjustizministeriums keinen Ersatz bietet, da die Telekommunikationsunternehmen jede Überwachungsmaßnahme getrennt nach den einzelnen Anschlüssen zählen, während die Landesjustizverwaltungen lediglich die Anzahl der Strafverfahren erfassen.

Die Entschließung vom 21. November 2003 (siehe Anlage 23) befasst sich mit dem von der Bundesregierung am 15. Oktober 2003 beschlossenen Entwurf für ein neues Telekommunikationsgesetz (BR-Drs. 755/03). Der Gesetzentwurf sieht zwar die Beibehaltung der oben genannten Unternehmensstatistik zu Überwachungsmaßnahmen vor, enthält ansonsten aber schwer wiegende Verschlechterungen des Datenschutzes. Vor allem folgende geplante Regelungen sind Gegenstand der Entschließung:

- Die Telekommunikationsunternehmen sollen grundsätzlich alle entstehenden Verkehrsdaten, also auch alle Zielrufnummern, unverkürzt bis zu sechs Monaten nach Rechnungsversand speichern dürfen.

- Alle Erwerber von Prepaid-Handys sollen sich gegenüber dem jeweiligen Diensteanbieter identifizieren müssen.

- Sicherheitsbehörden soll der Zugriff auf Passwörter, PINs und andere Daten, mit denen die Inhalte oder näheren Umstände einer Telekommunikationsverbindung geschützt werden, erleichtert werden.

Am 19. Dezember 2003 hat der Bundesrat zum Regierungsentwurf Stellung genommen (BR-Drs. 755/03(B)). In dem Beschluss werden Änderungen gefordert, die den Datenschutz weiter abbauen würden. Beispiele dafür sind:

- Die Telekommunikationsunternehmen sollen verpflichtet werden, die Verkehrsdaten unverkürzt sechs Monate zu speichern. Im Gegensatz zu der Regelung im Regierungsentwurf wäre es den Unternehmen danach verboten, die Daten früher zu löschen, auch wenn sie diese für ihre Zwecke nicht mehr benötigen. Besonders schwer wiegt die damit verbundene Streichung der Kundenoption zur verkürzten Speicherung der Daten beziehungsweise zu deren Löschung nach Rechnungsversand.

- Die Auskunftspflicht der Telekommunikationsunternehmen soll auf Finanzbehörden erweitert werden, falls dies rechtlich möglich ist.

- Die bisherige Bestimmung, wonach die Telekommunikationsunternehmen Bestandsdaten der Kunden nur mit deren Einwilligung zur Werbung und zur Marktforschung verwenden dürfen, soll gestrichen werden.

- Die Übermittlung personenbezogener Telekommunikationsdaten an ausländische Stellen soll auch über Telekommunikationszwecke hinaus möglich sein.

- In die Telekommunikations-Überwachungsverordnung soll eine Regelung aufgenommen werden, die es den Sicherheitsbehörden ermöglicht, Handys auch auf Grundlage der Gerätenummer anstatt nur der Rufnummern zu überwachen.

Es ist zu hoffen, dass der Bundestag dem Recht auf informationelle Selbstbestimmung und dem Telekommunikationsgeheimnis größeres Gewicht beimisst und das künftige Telekommunikationsgesetz datenschutzfreundlicher wird, als es Bundesregierung und Bundesrat mit ihren bisherigen Vorschlägen beabsichtigen.

2.9.2 Datenverarbeitung durch Internet- und Telekommunikationsdienste

Angesichts der rasant wachsenden Nutzung des Internet haben die Datenschutzbeauftragten des Bundes und der Länder auf ihrer 63. Konferenz im März 2002 eine Entschließung zum „Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikationsdiensten“ verabschiedet (siehe Anlage 2). Darin weisen sie auf folgende Punkte hin:

- Das Telekommunikationsgeheimnis gilt auch für Multimedia- und E-Mail-Dienste.

- Ein in sich schlüssiges System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten Betroffener fehlt.

- Anbieter von Tele-, Medien- und Telekommunikationsdiensten sind weder berechtigt noch verpflichtet, Nutzerdaten, die sie nicht für eigene Zwecke benötigen, generell auf Vorrat zu erheben, zu speichern oder herauszugeben.

- Eine Pflicht zur Vorratsdatenspeicherung würde dem Grundrecht auf unbeobachtete Kommunikation nicht gerecht, da der Staat dann jede Internetaktion beobachten könnte.

2.9.3 Wer bezahlt digitale Privatkopien?

Die Bundesregierung hat im August 2002 einen Gesetzentwurf zur Umsetzung der EU-Urheberrechtsrichtlinie in den Bundestag eingebracht (BR-Drs. 684/02). Im Gesetzgebungsverfahren hat der Bundesrat gefordert, die Vergütung für digitale Privatkopien (z. B. mit Hilfe von CD-Brennern kopierte CDs) nicht mehr über Pauschalabgaben auf Vervielfältigungsgeräte und Datenträger zu regeln, sondern ein System der individuellen Lizenzierung einzuführen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen in ihrer Entschließung vom 24./25. Oktober 2002 (siehe Anlage 9) darauf hin, dass das bisher praktizierte Verfahren der Pauschalabgaben auf der Rechtsprechung des Bundesgerichtshofes beruht. Danach ist es mit dem Schutz der Freiheitsrechte von Privatpersonen unvereinbar, wenn individuell geprüft wird, ob sie analoge Kopiertechniken einsetzen. Die Datenschutzbeauftragten betonen, dass dieser Grundsatz auch für die digitalen Vervielfältigungstechniken seine Berechtigung hat.

Der Bundestag hat im April 2003 das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft verabschiedet (BR-Drs. 271/03). Die Forderung des Bundesrates hat darin keinen Niederschlag gefunden. Somit erfolgt auch die Vergütung digitaler Privatkopien durch ein Verfahren, das ohne personenbezogene Einzelabrechnungen auskommt.

2.9.4 Neuordnung der Rundfunkfinanzierung

Die Länder bereiten eine Änderung des Rundfunkgebührenstaatsvertrages vor, um die Finanzierung des Rundfunks neu zu regeln. Zunächst war unter anderem geplant, dass

- die Meldebehörden verpflichtet werden, einmalig die Daten aller Personen über sechzehn Jahre an die Gebühreneinzugszentrale (GEZ) zu übermitteln,

- die regelmäßige Übermittlung aus dem Melderegister bei Zu- und Wegzügen um Übermittlungen aus dem Schuldnerverzeichnis, dem Gewerbezentralregister und den Registern berufsständischer Kammern erweitert wird und

- ausdrücklich erlaubt wird, personenbezogene Daten bei Dritten ohne Wissen des Betroffenen einzuholen.

Die Datenschutzbeauftragten des Bundes und der Länder haben in ihrer Entschließung vom 30. April 2003 (siehe Anlage 18) darauf hingewiesen, dass die bereits bestehenden datenschutzrechtlichen Defizite beim Verfahren des Gebühreneinzugs durch die geplanten Änderungen weiter vertieft werden. Sie greifen unverhältnismäßig in die Rechte des Bürgers ein. Schon in ihrer Entschließung vom 12./13. Oktober 2000 hatten die Datenschutzbeauftragten gefordert, bei der Neuordnung der Rundfunkfinanzierung ein Modell zu Grunde zu legen, das sich stärker an den Prinzipien der Datenvermeidung und der Datensparsamkeit orientiert (siehe Fünfter Tätigkeitsbericht, Anlage 9).

Die Länder haben inzwischen ein überarbeitetes Konzept vorgestellt, in dem die oben beschriebenen Ansätze nicht weiter verfolgt werden.

2.10 Finanzwesen

2.10.1 Unzulässige Nutzung von Hundesteuerdaten

Ein Petent hat sich darüber beschwert, dass er ein Schreiben von einer Gemeindevertreterin erhalten hatte, in dem er auf seine Ordnungspflichten als Hundehalter hingewiesen wird. Er vermutete eine unzulässige Nutzung von Hundesteuerdaten für diesen Zweck.

Die Amtsverwaltung teilte mir dazu mit, dass wiederholt Beschwerden über die Verschmutzung öffentlicher Wege und Plätze durch Hundekot eingegangen seien und die Gemeinde beraten habe, wie hiergegen effektiv vorgegangen werden könne. Weder die entsprechenden Aufrufe im amtlichen Mitteilungsblatt noch das Aufstellen von Hundetoiletten hatten bisher zu einer dauerhaften Verbesserung der Situation geführt. Deshalb entschloss sich die ehrenamtliche Bürgermeisterin, Hundehaltern in bestimmten Gemeindegebieten einen Brief zu schreiben. Für diesen Zweck erhielt sie Name und Anschrift der Halter aus der Hundesteuerdatei. Sie gab diese Daten an eine Gemeindevertreterin weiter, die die Anschreiben formulierte und versandte.

Das Anliegen der Gemeinde ist zwar durchaus verständlich, jedoch war die gewählte Verfahrensweise aus datenschutzrechtlicher Sicht nicht zulässig. Namen und Anschriften von Hundehaltern, die im Rahmen des Hundesteuererhebungsverfahrens gespeichert werden, unterliegen nach § 12 Abs. 1 Kommunalabgabengesetz Mecklenburg-Vorpommern in Verbindung mit § 30 Abgabenordnung dem Steuergeheimnis, in das nur unter besonderen Voraussetzungen eingegriffen werden darf. In diesem Fall aber gab es keine Rechtsgrundlage, um die Daten für den verfolgten Zweck zu nutzen.

Ich habe der Amtsverwaltung empfohlen, in derartigen Fällen das so genannte Adressmittlungsverfahren zu nutzen. Zu diesem Zweck werden die Anschreiben ohne namentliche Anrede des Hundehalters vorbereitet und kuvertiert. Die Adressierung übernimmt die für die Einziehung der Hundesteuer zuständige Stelle. Auf diese Weise können die Hundehalter erreicht werden, ohne dass Hundesteuerdaten an andere Stellen übermittelt werden müssen.

Der leitende Verwaltungsbeamte des Amtes hat meine Bewertung geteilt und zugesichert, künftig entsprechend meiner Empfehlung zu verfahren.

2.10.2 Mehr Steuerrecht – weniger Datenschutz

Im Berichtszeitraum sind einige Artikelgesetze in Kraft getreten, die verschiedene Bundessteuergesetze ändern. Besonders die Einführung der Identifikationsnummer und des Abrufverfahrens bei Kreditinstituten schränken das Recht auf informationelle Selbstbestimmung im Steuerbereich erheblich ein.

Identifikationsnummer
Künftig erhält jeder Steuerpflichtige – also jede Person, die in Deutschland wohnt oder ihren gewöhnlichen Aufenthalt hat – eine eindeutige Identifikationsnummer für Steuerzwecke. Die Nummer soll bereits ab der Geburt vergeben werden. Das Steueränderungsgesetz 2003 vom 15. Dezember 2003 (BGBl. I S. 2645) fügt dazu die §§ 139a bis 139d in die Abgabenordnung ein, welche die Voraussetzungen für die Einführung der Identifikationsnummer regeln. Unter anderem um sicherzustellen, dass eine Person nur eine Identifikationsnummer erhält und keine Nummer mehrfach vergeben wird, darf das Bundesamt für Finanzen (BfF) zu jeder Person eine Vielzahl von Daten speichern, beispielsweise Familienname, frühere Namen, Vornamen, Tag und Ort der Geburt, Anschrift. Die Daten wird das BfF von den Meldebehörden erhalten, die ihrerseits alle Meldedatensätze um die Identifikationsnummer der jeweiligen Person ergänzen müssen.

Erstmals wird somit mit dem BfF eine einzige Stelle über ein vollständiges Register der Einwohner der Bundesrepublik Deutschland („zentrales Melderegister“) verfügen. Auch wenn die Zweckbindung dieser Datensammlung für Steuerangelegenheiten durch entsprechende Regelungen sichergestellt werden soll, ist zu befürchten, dass sie gegebenenfalls durch geringfügige Gesetzesänderungen durchbrochen wird. Insofern besteht durchaus die Gefahr, dass die Identifikationsnummer außerhalb des Steuerbereiches genutzt wird, womit sich dann die von verschiedenen Stellen zu einer Person gespeicherten Daten leicht verknüpfen ließen.

Insbesondere halte ich für unverhältnismäßig, dass schon alle Neugeborenen eine Identifikationsnummer erhalten und somit als „geborene Steuerschuldner“ pauschal beim BfF erfasst werden sollen. Vor diesem Hintergrund begegnet die Datenübermittlung **aller** in den Melderegistern gespeicherten Personen von den Meldebehörden an das BfF grundsätzlichen datenschutzrechtlichen Bedenken.

Es ist zu hoffen, dass bis zu der tatsächlichen Einführung der Identifikationsnummer, die wohl erst in einigen Jahren erfolgen wird, die entsprechenden Rechtsvorschriften noch einmal deutlich im Sinne des Datenschutzes verbessert werden.

Abruf von Kundendaten bei Kreditinstituten

Im November 2001 hat die Bundesregierung einen Gesetzentwurf in den Bundestag eingebracht, mit dem unter anderem das Kreditwesengesetz geändert werden sollte (BR-Drs. 936/01). Nach dem Entwurf muss jedes Kreditinstitut eine stets aktuelle Datei mit den bei ihm geführten Konten und Depots sowie den dazugehörigen persönlichen Angaben der Kunden führen. Die Bundesanstalt für Finanzdienstleistungsaufsicht, die im Rahmen der Bankenaufsicht vor allem Missstände im Kreditwesen bekämpft, darf diese Daten jederzeit zur eigenen Aufgabenerfüllung oder in bestimmten Fällen auf Ersuchen anderer öffentlicher Stellen abrufen.

In ihrer Entschließung vom 7./ 8. März 2002 (siehe Anlage 4) stellen die Datenschutzbeauftragten des Bundes und der Länder fest, dass diese Abrufmöglichkeiten der Bundesanstalt einen neuen Eingriff in die Vertraulichkeit der Bankbeziehungen darstellen. Sie fordern daher, dass die Kreditinstitute ihre Kunden über dieses Abrufverfahren informieren, um den Eingriff zumindest transparent zu machen.

Der Bundestag hat Ende März 2002 das Vierte Finanzmarktförderungsgesetz (BGBl. I S. 2010) verabschiedet und dabei die im Entwurf enthaltene Regelung zum Abrufverfahren unverändert übernommen. Die Banken und Sparkassen sind nun aufgerufen, ihre Kunden auf dieses Verfahren und die dazugehörigen Rechtsgrundlagen hinzuweisen.

Den Bedenken der Datenschutzbeauftragten gegen dieses Verfahren wurde unter anderem damit begegnet, dass die Finanzbehörden ausdrücklich vom Zugriff ausgeschlossen sind und die Auskünfte nicht für Steuerstrafverfahren genutzt werden dürfen. Mit dem Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003 (BGBl. I S. 2928) wurden diese Einschränkungen jedoch aufgehoben. Denn mit diesem Gesetz wird § 93 der Abgabenordnung um die Absätze 7 und 8 ergänzt, die auch den Finanzbehörden die Befugnis zum Abruf einzelner Daten einräumen, und zwar

- zu Zwecken der Steuerfestsetzung oder -erhebung und

- zur Aufgabenerfüllung anderer Behörden, wenn das zu Grunde liegende Gesetz an Begriffe des Einkommensteuergesetzes anknüpft.

Hiermit wird das Abrufverfahren erheblich ausgeweitet und der mit diesem Verfahren ohnehin schon geschaffene schwere Eingriff in das Recht auf informationelle Selbstbestimmung der Bankkunden deutlich verschärft.

2.10.3 Steuerberaterkammer ist keine Ermittlungsbehörde

Die Steuerberaterkammer unseres Landes wollte von einer Zeitung den Namen und die Anschrift einer Person wissen, die eine Chiffreanzeige geschaltet hatte. Die Kammer vermutete, dass diese Person nicht befugt war, die von ihr angebotene Hilfeleistung in Steuersachen zu erbringen. Die Zeitung kam der Aufforderung nach. Nunmehr trat die Kammer an die Inserentin heran und forderte diese auf, eine Unterlassungserklärung zu unterschreiben. Die Inserentin beschwerte sich bei mir und hat darum gebeten, die Vorgehensweise der Steuerberaterkammer zu prüfen.

Die Kammer hat besonders geschützte Daten bei einem Dritten erhoben, um eine Person zu ermitteln, die möglicherweise unbefugt Hilfeleistung in Steuersachen erbracht hat. Dazu berechtigt sind jedoch nur die Staatsanwaltschaft und das zuständige Finanzamt, soweit es als Bußgeldbehörde tätig wird, nicht aber die Steuerberaterkammer. Ihr stehen im Gegensatz zu den anderen genannten Stellen nicht die dafür erforderlichen Befugnisse nach dem Gesetz über Ordnungswidrigkeiten (OWiG) und der Strafprozessordnung zu. Da die Steuerberaterkammer somit personenbezogene Daten ohne Rechtsgrundlage erhoben hat, habe ich dieses Verfahren beanstandet.

Die Steuerberaterkammer teilte mir daraufhin mit, dass sie nunmehr mit dem Finanzministerium und der zuständigen Oberfinanzdirektion für derartige Fälle eine neue Vorgehensweise vereinbart hat. Die Steuerberaterkammer ist nach § 5 Abs. 2 Steuerberatergesetz verpflichtet, dem zuständigen Finanzamt Tatsachen mitzuteilen, die den Verdacht begründen, dass eine Person geschäftsmäßig und unbefugt Hilfe in Steuersachen leistet. Sie zeigt also den Verdacht auf unbefugte Hilfeleistung bei der Oberfinanzdirektion an und veranlasst so ein Bußgeldverfahren. Diese leitet wiederum den Vorgang an das als Bußgeldbehörde örtlich zuständige Finanzamt weiter. Das Finanzamt ermittelt den Inserenten und führt das Bußgeldverfahren durch. Nach Abschluss dieses Verfahrens teilt das Finanzamt der Steuerberaterkammer ihr Ergebnis und somit auch den Namen und die Anschrift des Inserenten mit. Rechtsgrundlage für die Übermittlung dieser personenbezogenen Daten ist § 49a Abs. 4 Satz 2 OWiG. Danach darf die Bußgeldbehörde, also das Finanzamt, ihre abschließende Entscheidung derjenigen Verwaltungsbehörde übermitteln, die das Verfahren veranlasst hat, wenn dies zur Erfüllung einer Aufgabe der Verwaltungsbehörde erforderlich ist.

Die Steuerberaterkammer als veranlassende Behörde erhält das Ergebnis des Bußgeldverfahrens zur Kenntnis, da sie die beruflichen Belange der Gesamtheit der Mitglieder wahren und die Erfüllung der beruflichen Pflichten überwachen soll. Im vorliegenden Fall

geht es um die Abwehr einer unbefugten Hilfeleistung. Wer Hilfe in Steuersachen leistet, obwohl er dies nicht darf, verhält sich sittenwidrig im Sinne von § 1 des Gesetzes gegen den unlauteren Wettbewerb. Die Steuerberaterkammer ist nach diesem Gesetz berechtigt, gegen die betreffenden Personen im Wege einer Abmahnung und einer Unterlassungsklage vorzugehen.

Im Ergebnis ist jetzt sichergestellt, dass die Steuerberaterkammer bei Verdacht nicht auf eigene Faust ermittelt. Sie muss sich wie jede andere öffentliche Stelle an die zuständige Bußgeldbehörde wenden und wird anschließend als „Anzeigeerstatter“ über den Ausgang des Verfahrens informiert.

2.10.4 PROfiskal – sicheres Update, aber wie?

Bereits seit seiner Inbetriebnahme begleite ich das Haushalts-, Kassen-, Rechnungswesenverfahren PROfiskal des Landes (siehe Fünfter Tätigkeitsbericht, Punkt 3.10.4). Im Berichtszeitraum habe ich das Finanzministerium, welches die Hauptverantwortung für dieses Client-Server-Verfahren trägt, hauptsächlich zur IT-Sicherheit der PROfiskal-Endgeräte beraten.

Die PROfiskal-Software läuft auf Personalcomputern in der gesamten Landesverwaltung, sowohl in großen Behörden mit qualifizierter IT-Administration als auch in sehr kleinen Ämtern mit nur geringer IT-Betreuung. Die Software muss durch entsprechende Updates regelmäßig aktualisiert werden (siehe auch Punkt 2.18.4). Das Finanzministerium möchte die erforderlichen Wartungsarbeiten verständlicherweise mit möglichst geringem Aufwand realisieren. Vor diesem Hintergrund war zu prüfen, mit welchem Verfahren die Clientsoftware auf den PROfiskal-Arbeitsplätzen aktualisiert werden kann.

Das Ministerium hatte vorgesehen, dass die PROfiskal-Nutzer selbst die Updates von einem zentralen Server des Landes herunterladen und installieren. Dazu sollte ihnen Schreibzugriff auf Programm- und Konfigurationsdaten der Clientsoftware eingeräumt werden. Dieses Verfahren hätte jedoch nicht den Vorgaben des Landesdatenschutzgesetzes (DSG M-V) entsprochen. Nach § 22 Abs. 2 Satz 1 dürfen Änderungen an automatisierten Verfahren nur den dafür ausdrücklich berechtigten Personen, also dem Administrationspersonal, möglich sein.

Im Übrigen entsprach das geplante Verfahren auch nicht dem derzeitigen Stand der Technik (§ 21 Abs. 1 DSG M-V). Einerseits sollte die Integrität der heruntergeladenen Pro-

gramme nicht geprüft werden. Andererseits war nicht auszuschließen, dass bereits installierte PROfiskal-Software durch schädliche Programme manipuliert werden kann. Viele PROfiskal-Nutzer können sowohl auf Internetdienste als auch auf Disketten- und CD-ROM-Laufwerke zugreifen, so dass derartige Schadsoftware auf den Rechner gelangen kann.

Darüber hinaus ließe sich mit dem geplanten Verfahren der Updatevorgang nicht ordnungsgemäß protokollieren und demzufolge auch nicht kontrollieren (§ 22 Abs. 2 Satz 2 DSG M-V). Der PROfiskal-Server registriert lediglich die Versionsbezeichnung der Clientsoftware. Da die Updates jedoch ausschließlich vom Nutzer installiert werden sollten, hätten die zuständigen Administratoren dies nicht kontrollieren können.

Schließlich hätte diese Verfahrensweise auch nicht dem Transparenzgebot des § 21 Abs. 2 Nr. 6 DSG M-V genügt, da nicht ausreichend nachvollziehbar gewesen wäre, welche Softwareversion gerade installiert ist.

Ich habe daher empfohlen, dass nur ein speziell berechtigter Administrator die Software herunterlädt, prüft und einspielt. Auf diese Weise ist garantiert, dass Nutzung und Installation der Clientsoftware wirksam voneinander getrennt werden. Die Nutzer erhielten dann auch nur die Rechte, die sie für PROfiskal tatsächlich benötigen. Damit wird das Risiko der bewussten oder unbewussten Manipulation der Clientsoftware wesentlich reduziert.

Aufgrund meiner Empfehlung hat das Finanzministerium von der geplanten Updateprozedur Abstand genommen und wird nun wie folgt verfahren:

Für größere Behörden prüft das Ministerium derzeit eine Lösung auf der Basis eines Terminalservers. In diesem Fall kann eine Person mit Administrationsberechtigung die Clientsoftware vieler Nutzer installieren, ohne dass diese daran mitwirken müssen.

Damit auch kleine Behörden die Software auf den neuesten Stand bringen können, wird unter anderem ein Prüfsummenverfahren eingeführt. Das Verfahren berechnet bei jedem Programmstart eine Prüfsumme und vergleicht diese mit einem auf dem Server gespeicherten Wert. So kann erkannt werden, ob Clientsoftware unbefugt installiert oder geändert wurde. Eine so veränderte Software wird vom Prüfverfahren nicht zur Nutzung freigegeben. Darüber hinaus werden Download und Installation des Updates zwangsweise miteinander gekoppelt und auf dem Server protokolliert.

Da PROfiskal in einem relativ gut gesicherten Netz, dem Corporate Network der Landesregierung, betrieben wird, halte ich die für die kleinen Behörden genannten Maßnahmen derzeit für ausreichend. Die Lösung auf der Basis des Terminalservers bietet jedoch ein höheres Datensicherheitsniveau. Deshalb habe ich empfohlen, diese Variante zu realisieren.

2.10.5 Notarielle Verschwiegenheit im steuerlichen Verfahren

Das Justizministerium unseres Landes hat mich um Stellungnahme zu folgendem Sachverhalt gebeten:

Ein Notar wollte von dem für ihn zuständigen Landgericht wissen, ob er verpflichtet sei, dem Finanzamt im Rahmen einer laufenden Betriebsprüfung das Kostenregister und betriebliche Bankbelege herauszugeben, weil daraus die Namen Dritter, deren Bankverbindung und unter Umständen auch deren Beteiligung an notariellen Vorgängen zu ersehen sind. Das Landgericht teilte dem Notar mit, dass er auch gegenüber den Betriebsprüfern zur Verschwiegenheit verpflichtet sei. Daraufhin stellte das Finanzamt die Pflicht zur Vorlage der Unterlagen verbindlich fest und drohte Zwangsmaßnahmen an. Das Landgericht vereinbarte mit dem Finanzamt, dass Zwangsmaßnahmen gegen den Notar bis zur Klärung der Rechtslage durch das Finanz- und das Justizministerium unterbleiben.

Ich habe dem Justizministerium mitgeteilt, dass ich das Vorgehen des Finanzamtes aus datenschutzrechtlicher Sicht für unzulässig erachte. Ein Zugriff auf personenbezogene Daten ist ohne Einwilligung der Betroffenen nur zulässig, sofern eine Rechtsvorschrift es erlaubt oder zwingend voraussetzt (§ 7 Abs. 1 Landesdatenschutzgesetz – DSG M-V).

Der Notar hat zwar nach § 200 Abgabenordnung (AO) als Steuerpflichtiger bei der Feststellung des steuerlichen Sachverhaltes mitzuwirken und muss den Prüfern auch betriebliche Unterlagen vorlegen. Er kann jedoch gemäß § 102 AO die Auskunft über personenbezogene Daten seiner Mandanten verweigern. Nach § 18 Bundesnotarordnung (BNotO) ist er sogar zur Verweigerung verpflichtet. Auf diese Weise wird der notwendige Schutz der Vertrauensbeziehung zwischen dem Notar und seinen Mandanten gewährleistet.

Eine Auskunftspflicht des Notars kann auch nicht damit begründet werden, dass die Angehörigen der Finanzbehörde dem Steuergeheimnis nach § 30 AO unterliegen. Der Notar kann nicht gegenüber der Finanzbehörde von seiner Verschwiegenheitspflicht entbunden werden, nur weil die Daten wiederum in einen durch Amtsverschwiegenheit geschützten

Bereich übertragen werden. Die Verschwiegenheitspflicht des Notars besteht grundsätzlich gegenüber allen Dritten, unabhängig davon, ob diese wiederum einer Pflicht zur Verschwiegenheit unterliegen.

Sofern der Notar die Auskunft verweigert, wird die Finanzbehörde zur Steuerschätzung schreiten. Dabei ist nicht auszuschließen, dass es zu einer erheblichen Abweichung zuungunsten des Notars kommt. Mit Blick auf § 18 BNotO darf der Notar selbst unter diesen Voraussetzungen keine Daten seiner Mandanten offen legen.

Dieser Fall hat insoweit weitergehende Bedeutung, als sich die in § 102 AO ebenfalls genannten Angehörigen der Heilberufe und der Rechtspflege, die Wirtschaftsprüfer, Steuerberater, Steuerbevollmächtigten sowie die vereidigten Buchprüfer in der gleichen Situation befinden. Auch sie sind nach der Abgabenordnung berechtigt, nach anderen gesetzlichen Vorschriften sogar verpflichtet, die Verschwiegenheit zu wahren.

Aufgrund der Bedeutung dieses Themas habe ich die anderen Datenschutzbeauftragten des Bundes und der Länder in die Diskussion mit einbezogen. Ein Landesjustizministerium hat vorgeschlagen, steuerlich relevante Informationen von geheimhaltungspflichtigen Daten zu trennen. Insbesondere für elektronisch gespeicherte Daten ist eine derartige Trennung praktikabel. Schon jetzt bieten Hersteller von Anwendungssoftware, beispielsweise für Notariate, Programme mit automatischen Trennungsmöglichkeiten an. Ein endgültiges Ergebnis der Erörterung unter den Datenschutzbeauftragten und den damit befassten Ministerien steht noch aus.

2.11 Soziales

2.11.1 Neue Regelungen in der gesetzlichen Krankenversicherung

Disease-Management-Programme
Der Bundesgesetzgeber hat Ende des Jahres 2001 eine Rechtsvorschrift in das Fünfte Buch Sozialgesetzbuch (SGB V) eingefügt, nach der strukturierte Behandlungsprogramme, so genannte Disease-Management-Programme (DMP), entwickelt werden können. Sie sollen dazu beitragen, den Behandlungsverlauf und die Qualität der medizinischen Versorgung chronisch Kranker zu verbessern. Gleichzeitig wird ein gesundheitspolitisches Ziel verfolgt. Krankenkassen, die solche Programme einrichten, erhalten aus dem Risikostrukturausgleich einen Teil ihrer Kosten erstattet. Damit sollen auch Nachteile für Kassen mit einem hohen Anteil chronisch kranker Versicherter gegenüber solchen mit überwiegend gesunden und leistungsfähigen Versicherten ausgeglichen werden. Aus diesem Ziel resultiert auch ein umfangreiches Datenmanagement für diese Programme.

Die AOK M-V hat mich frühzeitig darüber informiert, dass sie zunächst ein Disease-Management-Programm für die Krankheit Diabetes mellitus Typ 2 einführen wird. Sie verwies darauf, dass wesentliche mit dem Programm zusammenhängende Datenverarbeitungsschritte rechtlich vorgegeben sind (Risikostrukturausgleichsverordnung). Außerdem muss das Bundesversicherungsamt ein solches Programm genehmigen.

Versicherte mit Diabetes mellitus Typ 2 und die diese Krankheit behandelnden Ärzte können an solchen Programmen auf freiwilliger Basis teilnehmen. Entscheiden sie sich dafür, müssen sie sich für das Programm registrieren lassen. Die Rechtsgrundlage für die Verarbeitung der Daten der Versicherten ist dann die Einwilligung. Die AOK M-V wollte die Versichertengemeinschaft allgemein über das DMP informieren, aber auch Betroffene gezielt ansprechen. Für den zuletzt genannten Fall war zu klären, welche Daten über die Versicherten auf welcher Rechtsgrundlage dazu genutzt werden können.

Aus ambulanten ärztlichen Behandlungen liegen der Krankenkasse keine versichertenbezogenen Diagnosedaten vor. Aber aus Daten der stationären Krankenhausbehandlung oder der Arzneimittelabrechnung kann sie Versicherte ermitteln, die an einer chronischen Krankheit leiden. Solche Daten darf die Krankenkasse verarbeiten, um Teilnehmer zu gewinnen (§ 284 Abs. 1 Satz 1 Nr. 11 SGB V). Die AOK M-V kann somit die potentiellen Teilnehmer anschreiben, um sie für das Programm zu werben, wenn sie gleichzeitig darauf hinweist, dass die Teilnahme freiwillig ist. Sie will diese Versicherten darüber hinaus auch auf das DMP ansprechen, wenn sie eine Geschäftsstelle besuchen. Auch dagegen bestehen keine Bedenken.

Ein weiterer datenschutzrechtlich relevanter Punkt ist die Dokumentation der Daten der Teilnehmer an dem DMP. Die AOK M-V hat zu diesem Zweck zusammen mit anderen Krankenkassen und Einrichtungen einen Vertrag mit einer privatrechtlich organisierten Gesellschaft geschlossen. Ihr wurde die Funktion übertragen, festgelegte Daten aus der medizinischen Behandlung der Versicherten zu speichern und bestimmte Daten je nach Verwendungszweck versichertenbezogen oder pseudonymisiert den am Programm beteiligten Stellen zur Verfügung zu stellen. Es handelt sich hierbei um eine Datenverarbeitung im Auftrag. In § 80 Abs. 5 Zehntes Buch Sozialgesetzbuch (SGB X) ist unter anderem geregelt, dass die Verarbeitung solcher Sozialdaten durch eine nichtöffentliche Stelle im Auftrag eines Sozialleistungsträgers nur zulässig ist, wenn die übertragenen Aufgaben beim Auftragnehmer erheblich kostengünstiger erfüllt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst.

Vor diesem Hintergrund ist es auf den gegenwärtig bestehenden Rechtsgrundlagen nicht zulässig, den gesamten Datenbestand der DMP-Teilnehmer von einer nichtöffentlichen Stelle speichern zu lassen. Die AOK M-V hat sich aber darauf berufen, dass sie in dieser Hinsicht an die Vorgaben des Bundesversicherungsamtes gebunden sei. Das Amt fordere sogar die europaweite Ausschreibung dieser Leistungen. Der Bundesbeauftragte für den Datenschutz hat zugesagt, diese Frage mit dem Bundesministerium für Gesundheit und Soziale Sicherung und dem Bundesversicherungsamt zu klären.

Gesetz zur Modernisierung der gesetzlichen Krankenversicherung

Der Bundesgesetzgeber hat in der zweiten Hälfte des Jahres 2003 das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung erlassen. Die neuen Regelungen treten zu Beginn des Jahres 2004 in Kraft. Unter anderem wird dadurch auch die Datenverarbeitung gravierend verändert.

Schon vor diesem Gesetzgebungsverfahren hat es Bestrebungen des zuständigen Bundesministeriums und anderer Akteure des Gesundheitswesens gegeben, stärker auch Daten zu nutzen, aus denen zwar nicht der einzelne Versicherte direkt identifiziert werden kann, die es aber dennoch ermöglichen, dass Kosten und Leistungen dem jeweiligen „Versicherungsfall“ zugeordnet werden. Das damals entwickelte Transparenzgesetz der gesetzlichen Krankenversicherung hat dazu weitgehend moderne datenschutzgerechte Technologien, insbesondere die Pseudonymisierung der Daten, vorgesehen. Diese Entwicklung ist leider nicht in dem ursprünglichen Umfang in das nun geltende Gesetz aufgenommen worden. So werden bei ambulanten ärztlichen Behandlungen mehr Daten

über den Gesundheitszustand des Versicherten an seine Krankenkasse als bisher übermittelt. Sie werden vorher auch nicht pseudonymisiert. Außerdem fehlen Regelungen, die eine strenge Zweckbindung für diese Daten vorsehen.

An dem Gesetzgebungsverfahren sind die Datenschutzbeauftragten des Bundes und der Länder nicht ausreichend beteiligt worden. Deshalb konnten datenschutzrechtliche Verbesserungen beziehungsweise Klarstellungen nicht mehr in das Gesetz aufgenommen werden, sondern sind in die Beschlussfassung des Ausschusses des Deutschen Bundestages für Gesundheit und Soziale Sicherung und in eine Entschließung des Bundestages eingegangen.

Die Auffassungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Gesetzgebung in der gesetzlichen Krankenversicherung sind aus den betreffenden Entschließungen ersichtlich (siehe Anlagen 13 und 21).

2.11.2 Gesetz für Kindertagesstätten

Im Mai 2003 hat mir das Sozialministerium unseres Landes den Entwurf eines neuen Kindertagesstättengesetzes (KitaG) zugesandt und um Hinweise gebeten. Datenschutzrechtlich relevant waren insbesondere die Bestimmungen zu den Zugangsvoraussetzungen für die Kindertagesförderung sowie zu den Aufgaben der Fachkräfte.

In § 9 war als Zugangsvoraussetzung für die Kindertagesförderung geregelt, dass die Einrichtung oder die Tagespflegestelle einen Nachweis über Vorsorgeuntersuchungen sowie den Impfschutz verlangen kann, bevor das Kind aufgenommen wird. Die damit verbundene Erhebung personenbezogener Daten ist jedoch nur zulässig, wenn diese zur Aufgabenerfüllung der Kindertageseinrichtung erforderlich sind. Diese Voraussetzung war aus meiner Sicht nicht erfüllt.

Nach den Vorschriften des Gesetzes über den Öffentlichen Gesundheitsdienst (ÖGDG M-V) untersuchen die Gesundheitsämter alle Kinder unter anderem regelmäßig vor der Einschulung, um Krankheiten und Fehlentwicklungen frühzeitig zu erkennen (§ 15 Abs. 2 ÖGDG M-V). Die damit zusammenhängenden Daten müssen dem Gesundheitsamt, nicht aber der Kindertagesstätte bekannt sein.

Vor diesem Hintergrund habe ich dem Sozialministerium empfohlen, auf den Nachweis zu verzichten. Stattdessen könnten die Personensorgeberechtigten gebeten werden, das

Datum und die Stufe der letzten Vorsorgeuntersuchung anzugeben. Diese Daten sind für die Kindertagesstätte zur Vorbereitung einer nachfolgenden Untersuchung erforderlich. Das Ministerium hat die Empfehlung bei der Überarbeitung des Entwurfes berücksichtigt.

Den Fachkräften der Kindertagesstätten war ursprünglich unter anderem die Aufgabe zugewiesen worden, kindbezogene Beobachtungen zu dokumentieren, sie zu reflektieren, sich fachlich dazu auszutauschen und sie mit den Personensorgeberechtigten zu besprechen. Für welchen Zweck die Dokumentation verwendet werden soll und welche Angaben sie enthalten darf, ließ die Regelung jedoch offen. Daher war fraglich, ob eine Kindertagesstätte solche Aufzeichnungen benötigt, um ihre Aufgabe zu erfüllen.

Diese Regelung wurde aufgrund meiner Kritik zwar geändert und das Wort „dokumentieren“ durch das Wort „aufnehmen“ ersetzt; allerdings wird dadurch aus meiner Sicht noch keine vollständige Klarstellung erreicht. Weil der Gesetzentwurf aber inzwischen dem Landtag zur Beratung und Beschlussfassung vorlag, habe ich dem Vorsitzenden des Sozialausschusses alternative Formulierungen vorgeschlagen und gebeten, sie in das Gesetzgebungsverfahren einzubringen. So sollten die kindbezogenen Beobachtungen entweder nur mit Einwilligung der Personensorgeberechtigten aufgenommen werden dürfen, oder es sollte formuliert werden, dass die Fachkräfte besondere Begabungen oder Verhaltensmuster eines Kindes mit den Personensorgeberechtigen lediglich besprechen. Dadurch würde in jedem Fall diese Tätigkeit der Fachkräfte einer Kindertagesstätte für die Personensorgeberechtigten transparenter.

Im vorliegenden Gesetzentwurf wird nun auch der Zweck für diese Regelung genannt. Durch die kindbezogenen Beobachtungen soll eine auf die Persönlichkeit des jeweiligen Kindes bezogene pädagogische Förderung erreicht werden.

Die parlamentarische Beratung des jetzt als „Gesetz zur Förderung von Kindern in Tageseinrichtungen und in Tagespflege – KiföG“ bezeichneten Entwurfes wird zu Beginn des Jahres 2004 fortgesetzt.

2.11.3 Modellvorhaben zur Zusammenarbeit zwischen Arbeits- und Sozialämtern (MoZArT)

Der Bundesgesetzgeber hat im November 2000 das Gesetz zur Verbesserung der Zusammenarbeit zwischen den Arbeitsämtern und den Trägern der Sozialhilfe verabschie-

det. Mit den neuen gesetzlichen Regelungen können diese Sozialleistungsträger durch Modellvorhaben erproben, ob es sich bewährt, die sozialen Leistungen aus „einer Hand“ zu erbringen. Auch in unserem Bundesland haben ein Arbeitsamt und eine Kommune eine Kooperationsvereinbarung unterzeichnet und sich somit an den bundesweiten Modellvorhaben beteiligt.

Im Rahmen eines Kontroll- und Informationsbesuches habe ich mich im Mai 2003 über das Vorhaben MoZArT informiert und geprüft, wie die datenschutzrechtlichen Bestimmungen eingehalten werden.

Auf der Basis der Kooperationsvereinbarung wurde ein Team aus Mitarbeitern beider Behörden gebildet. Dieses Team betreute zu Beginn rund 200 Personen beziehungsweise Familien, die bereits Arbeitslosengeld und ergänzende Sozialhilfe erhielten. Die Betroffenen hatten in diese Betreuung schriftlich eingewilligt. Neue Antragsteller wurden durch ein Informationsblatt auf die gemeinsame Betreuung hingewiesen. Eine schriftliche Einwilligung wurde von ihnen nicht eingeholt.

Da Arbeits- und Sozialamt unterschiedliche Datenverarbeitungssysteme nutzen, wurden die Angaben aus den Anträgen über getrennte Rechner in die entsprechenden Dateien eingegeben. Ziel war es jedoch, künftig nur noch einen gemeinsamen Antrag für beide Leistungen zu verwenden, der dann auch von nur einem Sachbearbeiter bearbeitet werden soll.

Die Mitarbeiter des Teams konnten sowohl auf die Daten der Arbeitsverwaltung als auch auf die Daten des Sozialhilfebereiches zugreifen, wobei nur der schreibende Zugriff protokolliert wurde. Rechtsgrundlage für die Datenverarbeitung sollte § 18a Bundessozialhilfegesetz (BSHG) sein.

§ 18a BSHG erlaubt den an Modellvorhaben beteiligten Leistungsträgern zwar, die erforderlichen Sozialdaten zu erheben, zu verarbeiten und zu nutzen, verpflichtet aber die Leistungsempfänger nicht, daran teilzunehmen. Auch aus anderen Sozialrechtsvorschriften lässt sich eine Verpflichtung zur Teilnahme nicht ableiten. Ich habe daher empfohlen, die Betroffenen darüber zu informieren, dass die gemeinsame Betreuung freiwillig ist und sie deshalb schriftlich darin einwilligen müssen. Darüber hinaus sind die Betroffenen darauf hinzuweisen, dass sie der Teilnahme widersprechen können, wenn sie dieses Angebot nicht mehr wahrnehmen und sich künftig wieder getrennt an beide Ämter wenden möchten. Ein allgemeiner Hinweis in Form eines Informationsblattes über die Leistungsgewährung aus „einer Hand“ genügt den datenschutzrechtlichen Anforderungen nicht.

Um sicherzustellen, dass nur befugte Personen auf die Daten der Arbeits- und Sozialverwaltung zugreifen können, haben beide Ämter entsprechende technische und organisatorische Maßnahmen festzulegen. Diese sind in einem Datenschutz- und Datensicherheitskonzept zu fixieren. Die Zugriffe sind darüber hinaus so zu protokollieren, dass jederzeit nachvollzogen werden kann, wer wann welche Daten gelesen oder geändert hat.

Die Leiterin des Sozialamtes teilte mir mit, dass das Modellvorhaben ab September 2003 nicht in der bisherigen Form weitergeführt wird. Erwerbsfähige Sozialhilfeempfänger haben dann zwar eine gemeinsame Anlaufstelle im Arbeitsamt, auf die Daten wird aber getrennt nach der Zuständigkeit der Ämter zugegriffen. Die Dienstanweisung zur Gewährleistung des Datenschutzes wurde überarbeitet.

2.11.4 Beratung von Versicherten zu Arzneimitteln

Die AOK M-V hat mir mitgeteilt, dass Versicherte zur sachgerechten Anwendung und Dosierung von Arzneimitteln beraten werden sollen. Wissenschaftliche Untersuchungen hätten unter anderem gezeigt, dass mitunter mehrere Medikamente eingenommen werden, die bei gleichzeitiger Anwendung miteinander unverträglich oder gar schädlich sind. Eine Ursache dafür ist, dass die Patienten dem jeweils behandelnden Arzt oft nur unzureichend Auskunft über bereits eingenommene Mittel geben können. Die AOK M-V wollte aber nicht selbst beraten, sondern den Medizinischen Dienst der Krankenversicherung Mecklenburg-Vorpommern (MDK M-V) damit beauftragen, weil dort der medizinische Sachverstand dafür vorhanden ist.

Aus datenschutzrechtlicher Sicht war zu klären, nach welchen Kriterien und auf welcher rechtlichen Grundlage die Versicherten für eine freiwillige Beratung durch den MDK M-V gewonnen und wie die dazu erforderlichen Daten verarbeitet werden können.

Die AOK M-V wollte die ihr vorliegenden ärztlichen Verordnungsdaten nutzen, um Versicherte mit einem hohen oder auffälligen Arzneimittelkonsum auszuwählen. Sie stützte sich bei dieser Verfahrensweise auf § 284 Abs. 1 Nr. 4 Sozialgesetzbuch Fünftes Buch (SGB V). Danach kann eine Krankenkasse Sozialdaten unter anderem für die Prüfung ihrer Leistungspflicht und die Gewährung von Leistungen an Versicherte verarbeiten. Anschließend wollte sie Name und Adresse der Versicherten dem MDK M-V übermitteln, damit dieser die Versicherten zu der Beratung einladen kann.

Weil die Versicherten aber auf freiwilliger Basis beraten werden sollten, besteht für die Übermittlung der Daten an den MDK M-V keine Rechtsgrundlage. Denn die Versicherten haben ja zum Zeitpunkt der Datenübermittlung noch keine Entscheidung treffen können. Deswegen habe ich der AOK M-V empfohlen, die Versicherten selbst anzuschreiben und sie – verbunden mit dem Hinweis auf die Freiwilligkeit – zu der Beratung bei dem MDK M-V einzuladen.

Die AOK M-V hat meine Empfehlung umgesetzt.

2.11.5 Datenerhebung durch Betreuungsbehörden

Betreuungsbehörden unterstützen die Vormundschaftsgerichte bei Betreuungsverfahren. In der Regel erteilen die Gerichte den Auftrag, einen Sozialbericht über die Person zu erstellen, für die eine Betreuung zu prüfen ist. Auf der Grundlage dieses Berichtes entscheidet das Gericht, ob für die Person ein Betreuer zu bestellen ist oder nicht.

Die Betreuungsbehörden arbeiten dabei eigenständig, unterliegen aber datenschutzrechtlichen Bestimmungen. Für den Sozialbericht müssen sie den Betroffenen, seine Angehörigen oder andere ihm nahe stehende Personen oder auch die behandelnden Ärzte befragen. Da hierzu in den bereichsspezifischen gesetzlichen Regelungen keine Datenverarbeitungsvorschriften existieren, sind die allgemeinen Regelungen des Landesdatenschutzgesetzes (DSG M-V) für diese Datenerhebung anzuwenden.

Ich habe die Betreuungsbehörden darauf hingewiesen, dass sie personenbezogene Daten nur bei der betroffenen Person oder mit ihrer schriftlichen Einwilligung bei einem Dritten erheben dürfen. Dieser Hinweis rief bei den Behörden weiteren Beratungsbedarf hervor. Sie haben mich deshalb zu einer Diskussion zu diesem Thema eingeladen. Im Ergebnis dieser Beratung wollen sie folgende Empfehlung umsetzen:

Im ersten Schritt wird immer der Betroffene selbst nach seiner persönlichen Situation befragt. Können bei ihm nicht alle erforderlichen Daten erhoben werden, werden dritte Personen mit einbezogen, sofern der Betroffene eingewilligt hat. Willigt er jedoch nicht ein, wird das Vormundschaftsgericht informiert, um über weitere Schritte zu entscheiden.

Falls der Betroffene wegen seines Gesundheitszustandes die Bedeutung und die Tragweite einer Einwilligung nicht verstehen kann und er deswegen nicht einwilligungsfähig ist, befragt der Mitarbeiter der Betreuungsbehörde die nächsten Angehörigen. Kann er

von ihnen nicht alle Daten erheben, bittet er sie, der Datenerhebung bei Dritten zuzustimmen. Willigen die Angehörigen nicht ein, werden keine Daten bei Dritten erhoben. Wenn dem Mitarbeiter der Betreuungsbehörde eine Betreuung dennoch notwendig erscheint, teilt er dieses dem Vormundschaftsgericht mit, damit es entscheiden kann, wie weiter vorzugehen ist.

Diese Vorgehensweise ist vereinbar mit den datenschutzrechtlichen Bestimmungen und gibt den Betreuungsbehörden gleichzeitig den erforderlichen Handlungsspielraum, um einen Sozialbericht für das Vormundschaftsgericht erstellen zu können.

2.11.6 Datenverarbeitung im Jugendamt – ungenügend!

In einem Jugendamt habe ich kontrolliert, wie die datenschutzrechtlichen Bestimmungen bei der Verarbeitung von Sozialdaten eingehalten werden.

Jugendämter haben bei der Verarbeitung von Sozialdaten das Sozialgeheimnis zu wahren (§ 35 Sozialgesetzbuch Erstes Buch – SGB I) und sie unterliegen den sozialdatenschutzrechtlichen Bestimmungen der Sozialgesetzbücher Achtes Buch (SGB VIII) und Zehntes Buch (SGB X) sowie ergänzend einigen Vorschriften des Landesdatenschutzgesetzes (DSG M-V). Bei der automatisierten Datenverarbeitung sind Sicherheitsmaßnahmen zum Schutz der Sozialdaten zu treffen sowie die Rechte und Pflichten der Nutzer zu regeln (§ 78 a SGB X) und zu dokumentieren (§ 18 DSG M-V).

In dem kontrollierten Jugendamt stehen den Mitarbeitern Rechner zur Verfügung, die über ein lokales Netz miteinander verbunden sind. Zwar waren einige Maßnahmen zum Schutz der Daten getroffen worden, jedoch existierte keine Dokumentation zur Datenverarbeitung. Durch diesen Missstand ist es den Mitarbeitern nur schwer möglich zu prüfen, ob sie bei der Datenverarbeitung die erforderlichen Sicherheitsmaßnahmen einhalten. Weil die erforderlichen Dokumentationen wie Verfahrensverzeichnis, Dienstanweisung zur Verarbeitung der Sozialdaten oder Sicherheitskonzept fehlten, habe ich die Datenverarbeitung des Jugendamtes beanstandet und empfohlen, die erforderlichen Arbeitsunterlagen zu erstellen. Über die Beanstandung habe ich den Innenminister als für den kommunalen Bereich zuständige oberste Aufsichtsbehörde informiert.

Der Leiter des Jugendamtes teilte mir mit, dass meine Empfehlungen zur Datenverarbeitung geprüft werden. Eine abschließende Antwort steht noch aus.

2.11.7 Unzulässiger Datenabgleich der BAföG-Ämter mit dem Bundesamt für Finanzen

Im Juli 2002 wurde ich von einem Kollegen darüber informiert, dass die BAföG-Ämter die Daten aller Leistungsempfänger mit den beim Bundesamt für Finanzen (BfF) gespeicherten Daten aus den Freistellungsanträgen abgleichen. Durch die damit verbundene Prüfung der Daten zur Besteuerung der Zinserträge wollten die Ämter kontrollieren, ob das in den BAföG-Anträgen angegebene Vermögen den Tatsachen entspricht. Dieses Vorgehen wurde auf § 45 d Abs. 3 Satz 1 Einkommensteuergesetz (EstG) gestützt.

Auf meine Anfrage teilte mir ein Studentenwerk unseres Landes mit, dass auch dort die Daten entsprechend abgeglichen wurden. Die Daten würden dabei über das Ministerium für Bildung, Wissenschaft und Kultur an das BfF übermittelt. Die Ergebnisse des Abgleichs erhält das Studentenwerk ebenfalls über das Ministerium. Als Rechtsgrundlage für das Verfahren verwies die Mitarbeiterin des Studentenwerkes auf § 41 Abs. 1 BAföG in Verbindung mit der dazugehörigen Verwaltungsvorschrift.

In § 41 Abs. 1 BAföG werden lediglich die Aufgaben der Ämter für Ausbildungsförderung genannt. Diese Norm erlaubt jedoch nicht den regelmäßigen Abgleich der Daten aller BAföG-Antragsteller mit ihren Daten beim BfF. Auch die Vorschriften im Sozialgesetzbuch Zehntes Buch (SGB X) gestatten diesen regelmäßigen Abgleich nicht. Ebenso ist § 45 d Abs. 3 Satz 1 EStG keine Rechtsgrundlage für den umfassenden Datenabgleich, da hier lediglich eine Übermittlungsbefugnis des BfF statuiert, eine Datenerhebungsbefugnis der BAföG-Ämter aber nicht gegeben ist. Ein Abgleich der Daten aller BAföG-Antragsteller mit den Daten beim BfF wäre im vollen Umfang demnach nur zulässig, wenn er gesetzlich geregelt wäre, etwa im BAföG. Deshalb habe ich das Ministerium für Bildung, Wissenschaft und Kultur unseres Landes gebeten, auf eine entsprechende Änderung des BAföG hinzuwirken. Vorstellbar wäre beispielsweise eine Regelung, wie sie im Bereich der Sozialhilfe in § 117 Abs. 1 Bundessozialhilfegesetz getroffen worden ist. Diese erlaubt den Abgleich bestimmter Sozialdaten der Sozialämter mit den Daten des BfF.

Die 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich im September 2003 mit dem Thema befasst. Im Ergebnis hat der Vorsitzende den beteiligten Bundesministerien die Rechtsposition der Datenschutzbeauftragten mitgeteilt und darum gebeten, diese in die laufenden Überlegungen mit einzubeziehen.

Im November 2003 hat das Bundesministerium für Bildung und Forschung zugesagt, für den Datenabgleich eine klarstellende Regelung im BAföG zu schaffen.

2.11.8 Dienstanweisung zum Datenschutz in der Unfallkasse

Die Unfallkasse Mecklenburg-Vorpommern bat mich im Mai 2003 um Hinweise zu ihrer Dienstanweisung zum Datenschutz und zur Sicherheit beim Einsatz der automatisierten Datenverarbeitung. Ein Schwerpunkt meiner Empfehlungen betraf das Recht der Betroffenen, einen Gutachter auszuwählen:

Damit die Kasse eine Entscheidung über die zu gewährenden Leistungen nach einem Arbeits- oder Wegeunfall treffen kann, ist sie auf medizinische Gutachten angewiesen. Im Sozialgesetzbuch Siebtes Buch (SGB VII) ist festgeschrieben, dass Betroffene einen Gutachter wählen können. Dieses Recht hat insofern datenschutzrechtliche Bedeutung, weil bei einem Verstoß dagegen die Verarbeitung der Daten unzulässig ist.

Die gesetzliche Verpflichtung (§ 200 Abs. 2 SGB VII), dem Versicherten mehrere Gutachter vorzuschlagen, war auch in der Dienstanweisung umgesetzt worden. Ich habe der Unfallkasse aber noch empfohlen, von vornherein klarzustellen, welchen der Gutachter sie schließlich beauftragen wird, wenn der Versicherte selbst sich nicht dazu äußert. Denn es wäre mit dem Recht des Versicherten nicht vereinbar, wenn die Unfallkasse aus den von ihr genannten Personen selbst eine freie Auswahl trifft.

Außerdem habe ich empfohlen, dass die Unfallkasse den Versicherten darauf hinweist, dass er auch selbst Gutachter vorschlagen kann. Dieses Recht lässt sich dem Bericht des Bundestags-Ausschusses für Arbeit und Sozialordnung zum Unfallversicherungs-Einordnungsgesetz entnehmen (BT-Drs. 13/4853 vom 12.06.1996). Darüber hinaus begrüßte der Deutsche Bundestag in seinem Beschluss zum 18. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (BT-Drs. 14/9490 vom 18.06.2002) ausdrücklich, dass die Versicherten in der gesetzlichen Unfallversicherung das Recht haben, einen oder mehrere Gutachter vorzuschlagen. Die Unfallkasse ist zwar nicht an den Gutachtervorschlag des Versicherten gebunden, sie ist aber verpflichtet, gegebenenfalls sachlich zu begründen, warum sie ihn ablehnt.

Die Unfallkasse hatte darüber hinaus in ihrer Dienstanweisung und entsprechenden Vordrucken vorgesehen, dass ein Betroffener die Ablehnung eines Gutachters sachlich begründen muss, bevor ihm weitere vorgeschlagen werden. Dem ist jedoch nicht so. Ein Betroffener muss nicht darlegen, weshalb er sein Recht wahrnimmt. Allerdings kann die Kasse den Versicherten auf seine Mitwirkungspflicht bei der Auswahl eines Gutachters hinweisen, wenn er die vorgeschlagenen ablehnt und selbst keinen benennt. Denn in diesem Fall könnte nicht über die Leistung entschieden werden.

Die Unfallkasse hat mir bisher noch nicht mitgeteilt, wie sie meine Empfehlungen in ihrer Dienstanweisung berücksichtigen wird.

2.11.9 Datenerhebung zur Durchsetzung von Beitragsregressen

Träger von Behinderteneinrichtungen zahlen für die bei ihnen Beschäftigten mit Behinderungen Beiträge zur gesetzlichen Rentenversicherung. Diese Beiträge werden ihnen vom Bund erstattet. In bestimmten Fällen kann der Bund die erstatteten Beiträge zurückfordern (§ 179 Abs. 1 a Sozialgesetzbuch Sechstes Buch, SGB VI). Eine solche Rückforderung ist möglich, wenn der Beschäftigte nur noch in einer Einrichtung für behinderte Menschen beruflich tätig sein kann, weil er durch einen Dritten, zum Beispiel bei einem Unfall, geschädigt worden ist. Der Bund kann dann den Schädiger in Regress nehmen.

In Mecklenburg-Vorpommern bearbeitet das Landesversorgungsamt (LVersA M-V) die Rückforderungen. Es meldet dem Bundesversicherungsamt jährlich die eingenommenen Beiträge. In diesem Zusammenhang hat das Amt allen Behindertenwerkstätten in unserem Land einen Erhebungsbogen gesandt. Dort wurde nach den Namen und den Anschriften derjenigen Geschädigten gefragt, deren Behinderung Folge einer Schädigung durch einen Dritten sein könnte. Eine Werkstatt hatte Zweifel, ob das Vorgehen des Landesversorgungsamtes zulässig sei.

Es ist nicht zulässig, dass das LVersA M-V bei den Behindertenwerkstätten Daten ohne Mitwirkung der betroffenen Personen erhebt, weil die gesetzlichen Voraussetzungen nicht vorliegen. Sozialdaten sind beim Betroffenen und somit bei den Geschädigten oder deren Personensorgeberechtigten direkt zu erheben (§ 67a Abs. 1 und 2 Sozialgesetzbuch Zehntes Buch – SGB X). Diese Personen kennt das LVersA M-V aber nicht. Deshalb kann es durchaus die Werkstätten um Mithilfe bitten. Zulässig aus datenschutzrechtlicher Sicht ist es, wenn das LVersA M-V den Werkstätten Informationsblätter und gegebenenfalls Datenerhebungsbögen zur Verfügung stellt, die an die Behinderten oder deren Personensorgeberechtigte weitergegeben werden. Diese können dann die erforderlichen Daten an das LVersA M-V senden. Diese Verfahrensweise entspricht dem Grundsatz der Datenerhebung beim Betroffenen.

Ich habe das Landesversorgungsamt aufgefordert, künftig in dieser Weise zu verfahren.

2.11.10 Auskunftsersuchen der Krankenkassen beim Landesbesoldungsamt

Das Finanzministerium unseres Landes hat mich gefragt, ob das Landesbesoldungsamt an Krankenkassen Auskunft über Zahlungen von Abfindungen und Vorruhestandsgeldern an ehemalige Beschäftigte geben darf. Die Krankenkassen wollten sich auf diesem Wege über die Einkünfte ihrer Versicherten informieren, um danach den Versicherungsbeitrag festsetzen zu können. Ich habe dem Finanzministerium meine Bedenken mitgeteilt. Denn es existiert keine rechtliche Grundlage dafür, dass Krankenkassen Auskunft über Abfindungen erhalten.

Einmalig gezahltes Arbeitsentgelt zählt zwar zu den beitragspflichtigen Einnahmen eines Versicherten (§ 28 a Abs. 3 Satz 2 Nr. 2 Sozialgesetzbuch Viertes Buch – SGB IV), und deshalb muss der Arbeitgeber es der Krankenkasse melden. So genannte „klassische“ Abfindungen jedoch, die der Arbeitgeber zahlt, weil der Arbeitsplatz wegfällt, sind nicht meldepflichtig. Dieses Entgelt wird für Zeiten nach dem Ende des Arbeitsverhältnisses gezahlt. Das Bundessozialgericht hat entschieden, dass zum Arbeitsentgelt aber nur solche Einnahmen zählen, die auf die Zeit der Beschäftigung und der Versicherungspflicht entfallen (BSG in NJW 1990, S. 2274).

Im Gegensatz dazu unterliegt das vom Arbeitgeber an seinen ehemaligen Beschäftigten gezahlte Vorruhestandsgeld der Meldepflicht. Dies hat zur Folge, dass der Arbeitgeber dies der Krankenkasse mitteilen muss.

Das Finanzministerium hat meine Rechtsauffassung an das Landesbesoldungsamt weitergeleitet. Dieses wird in Zukunft entsprechend der datenschutzrechtlichen Vorschriften verfahren.

2.11.11 Krankenkasse wollte Arbeitseinkommen pfänden

Ein Petent hat bis vor einigen Jahren ein eigenes Unternehmen geführt. Aus dieser Zeit bestanden noch Beitragsschulden gegenüber einer Krankenkasse, die diese nunmehr mit einer Pfändungs- und Einziehungsverfügung auf das zu erwartende Arbeitseinkommen des Petenten einfordern wollte. Der Petent ist jetzt im Unternehmen seiner Ehefrau angestellt. Die Krankenkasse hat die Verfügung jedoch nicht an die Ehefrau als derzeitige Arbeitgeberin gesandt, sondern an die Adresse seiner Stieftochter. Die Stieftochter habe jedoch weder etwas mit den Forderungen der Krankenkasse zu tun, noch habe er der Krankenkasse die Anschrift seiner Stieftochter mitgeteilt. Er wandte sich daher an die Kran-

kenkasse und bat um Auskunft, wie es zu dieser – wohl versehentlich falschen – Versendung der Verfügung kommen konnte. Da er weder von der zuständigen Sachbearbeiterin noch von deren Vorgesetzten eine Antwort zum Umgang mit seinen Daten erhalten hatte, bat er mich um Unterstützung.

Die Krankenkasse teilte mir mit, sie habe erst durch das Telefongespräch mit dem Petenten erfahren, dass die verwendete Anschrift nicht die seiner Arbeitgeberin, sondern die seiner Stieftochter sei. Deshalb war es der Mitarbeiterin auch nicht möglich, dem Petenten sofort zu erklären, wie es zu dem Versehen kommen konnte. Ein Gespräch mit der zuständigen Sachbearbeiterin ergab, dass ihr der Vorname der Ehefrau nicht bekannt war. Aus den in der Akte des Petenten vorhandenen Anschriften hat sie daher irrtümlich die seiner Stieftochter gewählt. Wie diese Anschrift in die Akte gelangt ist, konnte nicht geklärt werden.

Der Vorfall wurde mit der Sachbearbeiterin besprochen und der Datenbestand berichtigt. Darüber hinaus erhielt der Petent eine Stellungnahme, in der sich die Krankenkasse auch für die fehlerhafte Ermittlung und Verwendung der Daten entschuldigt.

2.12 Gesundheitswesen

2.12.1 Telemedizin

In unserem Bundesland gibt es mehrere telemedizinische Projekte (siehe auch Fünfter Tätigkeitsbericht, Punkt 3.12.1). Gegenwärtige Schwerpunkte sind die Teleradiologie und die Telepathologie. Ein Grund für die Konzentration auf diese Bereiche ist, dass nicht an allen Krankenhäusern spezialisierte Fachärzte beschäftigt sind. Es liegt deshalb auf der Hand, hier das Fachwissen externer Spezialisten zu nutzen. Nach den bestehenden Konzepten sollen radiologische Bilder oder Bilder von Zellgewebe, das bei einer Operation entfernt und entsprechend aufbereitet wird, an spezialisierte Fachärzte übertragen werden. Die Fachärzte erstellen daraufhin einen Befund, der den Chirurgen beispielsweise bei der Entscheidung unterstützt, wie die Operation weiter durchgeführt wird.

Teleradiologie und Telepathologie sind für die Verarbeitung pseudonymisierter Patientendaten prädestiniert. Dies vor allem auch deshalb, weil der externe Spezialist den Patienten nicht selbst untersucht. Er benötigt daher auch keine personenbezogenen Daten des Patienten, sondern lediglich Daten zum Krankheitsfall. Ein pseudonymisierter Datensatz kann alle medizinisch relevanten Daten des Patienten enthalten, die erforderlich sind, um einen Befund zu erstellen, beispielsweise auch das Alter, das Geschlecht, die Körpermasse und -länge oder den Bodymaßindex.

Die Nutzung pseudonymisierter Daten hat für die Ärzte entscheidende Vorteile. Bei sachgerechter Pseudonymisierung können Dritte weder aus den übermittelten Bilddaten noch aus den anderen medizinischen Daten einen Patienten bestimmen. Folglich wäre die ärztliche Schweigepflicht selbst dann nicht verletzt, wenn diese Daten einem unbefugten Dritten bekannt würden. Das Datenmanagement vereinfacht sich dadurch erheblich, denn es sind dann weniger aufwändige technische und organisatorische Maßnahmen erforderlich.

Werden personenbezogene Patientendaten in öffentlichen Netzen übertragen, so sind sie mit sicheren kryptographischen Verfahren zu verschlüsseln und zu signieren, um zu verhindern, dass Dritte sie zur Kenntnis nehmen und unbemerkt verändern können. Bei pseudonymisierten Daten kann hingegen auf die Verschlüsselung verzichtet werden. Das Signieren der Daten ist bei solchen Übermittlungen aber immer erforderlich. Nur so wird gewährleistet, dass der Adressat unzulässige Veränderungen immer sicher erkennt und die Daten zweifelsfrei dem Absender zuordnen kann (siehe Fünfter Tätigkeitsbericht, Punkt 3.12.1).

Die Sicherheit der pseudonymisierten Daten ist allerdings entscheidend davon abhängig, dass die Zuordnungsfunktion, mit deren Hilfe der Personenbezug wiederhergestellt werden kann, geheim gehalten wird. Auch sollte das Pseudonym für jeden Patienten bei jedem Behandlungsfall neu erzeugt werden. Wird für eine Person immer wieder dasselbe Pseudonym verwendet, ist nicht auszuschließen, dass Daten verschiedener Behandlungen ohne medizinischen Grund miteinander verkettet werden. Dadurch würde unter Umständen die gesamte Krankengeschichte offen gelegt werden, wenn lediglich für ein Detail der Personenbezug hergestellt werden muss. Ist es aus medizinischen Gründen allerdings notwendig, beispielsweise auch die Krankengeschichte an einen weiter behandelnden Arzt zu übermitteln, so kann das geschehen, sofern der Patient nichts anderes bestimmt (§ 17 Abs. 1 Nr. 2 Landeskrankenhausgesetz).

Gegen die Verarbeitung pseudonymisierter Daten bei Ärzten wird häufig eingewandt, dass damit die ärztliche Dokumentationspflicht nicht erfüllt werden könne. Dieses Argument ist meines Erachtens nicht stichhaltig. Denn wenn ein medizinischer oder rechtlicher Grund besteht, dass auch der Datenempfänger die Identität des Patienten kennen muss, kann er den Daten versendenden Arzt ersuchen, ihm beispielsweise den Namen und die Anschrift des Patienten mitzuteilen. Der Daten versendende Arzt kann den Patienten mit Hilfe der entsprechenden Zuordnungsfunktion bestimmen.

Ein weiteres Argument gegen Pseudonyme ist, dass damit die Verwechselungsgefahr steige. Auch das ist aus meiner Sicht nicht zutreffend. Ordnungsgemäß erzeugte Pseudonyme sind gerade durch ihre Eindeutigkeit gekennzeichnet. Bei häufig auftretenden Namen und unterschiedlicher Schreibweise hingegen kann es viel eher zu Verwechselungen kommen.

Die telemedizinischen Projekte in unserem Land werde ich weiterhin datenschutzrechtlich begleiten.

2.12.2 Qualitätssicherungsregister für eine spezielle Behandlung

Eine gemeinnützige Gesellschaft informierte mich darüber, dass sie ein Qualitätssicherungsregister für die LDL-Eliminationstherapie (LDL-Apherese) einrichten möchte. Die Abkürzung LDL steht hier für die englische Bezeichnung low density lipoproteins, also bestimmte Fettmoleküle geringer Dichte. Die LDL-Apherese ist eine besondere Art der Blutwäsche und zählt zu den so genannten neuen Untersuchungs- und Behandlungsmethoden.

Im Sozialgesetzbuch Fünftes Buch (§ 135 SGB V) ist festgelegt, dass die Krankenkassen die Kosten für diese Behandlungen nur unter bestimmten gesetzlichen Voraussetzungen erstatten dürfen. Eine dieser Voraussetzungen ist, dass mit einer neuen Behandlungsmethode ein therapeutischer Nutzen erreicht wird. Das Qualitätssicherungsregister soll dazu beitragen, diesen Nutzen durch weiteres Datenmaterial zu belegen und die Therapie weiter zu verbessern.

Eine Besonderheit der LDL-Apherese ist, dass bundesweit nur rund 1.000 Patienten in etwa 150 Einrichtungen mit dieser Methode über längere Zeiträume behandelt werden. Es war vorgesehen, die Daten der Patienten nur mit ihrer Einwilligung zu verarbeiten und unter einem Pseudonym im Register zu speichern. Die Anonymisierung war nicht möglich, weil die Datensätze im Laufe der Behandlung ergänzt werden sollen. Denn nur aus dem Behandlungsverlauf ergeben sich auswertbare Ergebnisse.

Die gemeinnützige Gesellschaft wollte ein Datenschutz- und Datensicherheitskonzept erarbeiten und hat dazu um Beratung gebeten. Unter anderem habe ich Folgendes empfohlen:

Die Erklärung eines Patienten, an der Behandlung teilzunehmen, ist eindeutig von der Einwilligung zur Registrierung seiner Daten zu trennen. Beide Erklärungen dürfen deshalb nicht zusammen eingeholt werden, weil ein Patient sich durchaus für die LDL-Apherese entscheiden kann, aber nicht möchte, dass seine Daten in dem Register gespeichert und verarbeitet werden. Die Einwilligung zur Speicherung der Daten ist in diesem Fall keine rechtliche Voraussetzung, um an der Behandlung teilnehmen zu können.

Das Pseudonym des Patienten sollte ursprünglich mit einer Software auf dem Rechner des Arztes erzeugt werden. Dieser Rechner hat für die Kommunikation mit der Daten speichernden Stelle (Registerstelle) einen Internetzugang. Unter Umständen könnten dann Unberechtigte die gespeicherten Daten einer Person zuordnen. Deshalb sollte ausschließlich eine Vertrauensstelle das Pseudonym bilden. Der Rechner dieser Stelle ist nicht an das Internet angeschlossen. Der behandelnde Arzt kommuniziert mit der Vertrauensstelle per Brief und erhält von dort das Pseudonym.

Auf die gespeicherten Daten soll neben dem behandelnden auch ein weiterer Arzt für die Beratung (Konsiliararzt) zugreifen können, um die Behandlung weiter zu optimieren. Hierzu ist, wie auch bei anderen ärztlichen Beratungen außerhalb der unmittelbaren Behandlung, die Zustimmung des Patienten einzuholen.

Im Verfahren war vorgesehen, die Pseudonyme und Daten zur Identität erst 50 Jahre nach dem Tod oder 130 Jahre nach der Geburt (wenn ein Todesdatum nicht bekannt ist) zu löschen. Die Daten sind aber nach Abschluss der Behandlung von der Registerstelle zu anonymisieren, da für die Qualitätssicherung dann kein Personenbezug mehr hergestellt werden muss. Bei dem behandelnden Arzt werden die Patientendaten im Übrigen für Zwecke der ärztlichen Dokumentation bis 10 Jahre nach Abschluss der Behandlung weiter gespeichert.

Meine Empfehlungen wurden umgesetzt. Interessierte können weitere Informationen zu dem Register unter der Internetadresse www.quasa.de abrufen.

2.12.3 Kontrolle im Krankenhaus

Im Juni 2003 habe ich in einem Krankenhaus kontrolliert, ob die datenschutzrechtlichen Bestimmungen des Landeskrankenhausgesetzes (LKHG M-V) und des Landesdatenschutzgesetzes (DSG M-V) eingehalten werden. Es zeigte sich, dass es nach wie vor Defizite bei der Umsetzung dieser Vorschriften gibt (siehe auch Dritter Tätigkeitsbericht, Punkt 3.13.3). Die folgenden Beispiele sollen dies veranschaulichen:

Unzulässiger Zugang zu Patientendaten
Alle Patientendaten, die während einer Krankenhausbehandlung erhoben wurden, sind in einer Krankenakte dokumentiert und im Krankenhausinformationssystem KIS gespeichert. Neben Grunddaten wie Name, Anschrift oder Krankenkasse werden hier auch die medizinischen Daten wie Diagnosen oder Befunde erfasst. Kommt ein Patient wegen einer neuen Behandlung wieder in dieses Krankenhaus, ist es allen zugelassenen Nutzern (Ärzten und Schwestern) möglich, jederzeit auf bereits vorhandene Daten von abgeschlossenen Behandlungen des Patienten zuzugreifen.

Diese Zugriffe sind jedoch nach den Vorschriften des Landeskrankenhausgesetzes nicht zulässig. Gemäß § 19 LKHG M-V sind Patientendaten in Krankenunterlagen nach Abschluss der Behandlung zu sperren und gesondert zu speichern. Wann eine Behandlung abgeschlossen ist, entscheidet der verantwortliche Arzt. Werden die Patientendaten in automatisierten Verfahren mit der Möglichkeit des Direktabrufes gespeichert, ist diese Möglichkeit nach Abschluss der Behandlung ebenfalls zu sperren. Die Sperrung darf nur zu den gesetzlich geregelten Zwecken aufgehoben werden. Wird beispielsweise ein Patient in ein Krankenhaus aufgenommen, das bereits Daten früherer Behandlungen gespeichert hat, dürfen nur solche Daten entsperrt werden, die in einem engen medizinischen Zusammenhang mit der aktuellen Behandlung stehen.

Damit die Ärzte bei der Aufnahme eines Patienten erkennen können, ob und welche Behandlungen bereits früher durchgeführt wurden, könnte beispielsweise eine Übersicht erstellt werden, welche die wichtigsten Daten wie Name, Behandlungsstation sowie Schlüsselnummer der Diagnose enthält. Stellt der Arzt fest, dass Unterlagen bereits abgeschlossener Behandlungen für die aktuelle Behandlung erforderlich sind, können diese im Archiv angefordert werden.

Archivierung von Patientendaten
Ist die Behandlung abgeschlossen, werden die Patientenakten im Archiv des Krankenhauses abgelegt. Geordnet sind sie nach dem Geburtsdatum und – bei gleichen Geburtsdaten – alphabetisch nach Namen. Dieses Prinzip entspricht nicht den Vorschriften des Landeskrankenhausgesetzes.

Danach sind Patientenakten im Krankenhaus so aufzubewahren, dass sie nur über einen Nachweis zu erschließen sind, zu dem unbefugte Mitarbeiter oder Außenstehende keinen direkten Zugriff haben (§ 19 Abs. 2 Satz 4 LKHG M-V). Bei dem oben geschilderten Verfahren jedoch kann jeder, der das Geburtsdatum und den Namen eines Patienten kennt, auf die entsprechende Akte zugreifen, sofern er Zugang zum Archiv hat. Im vorliegenden Fall war der Zugang von außen nicht besonders geschützt, da sich das Archiv im Erdgeschoss befindet und die Fenster nicht gegen Einbruch gesichert sind.

Ich habe daher vorgeschlagen, eine Übersicht der einzelnen Behandlungen zu erstellen, die Namen, Vornamen und Geburtsdatum der Patienten enthält. Jeder abgeschlossenen Behandlung wird dann eine interne Archivnummer zugeordnet, die Suchkriterium für die Unterlagen ist. Bei diesem Verfahren können die Patientenakten über die Archivnummer erschlossen werden. Dritten, denen diese Nummer nicht bekannt ist, ist es somit nur mit erheblichem Aufwand möglich, bestimmte Akten zu finden.

Systemadministrator als Datenschutzbeauftragter
Im kontrollierten Krankenhaus war die Systemadministratorin zur behördlichen Datenschutzbeauftragten ernannt worden.

Bei dieser Konstellation liegt jedoch eine Interessenkollision mit ihren anderen Aufgaben vor. Soll sie beispielsweise in ihrer Funktion als Datenschutzbeauftragte Arbeitsvorgänge oder Anordnungen aus dem Arbeitsbereich der Systemadministration prüfen, müsste sie sich selbst kontrollieren. Ich habe daher empfohlen, einen Datenschutzbeauftragten zu bestellen, der die in § 20 DSG M-V vorgeschriebenen Bedingungen erfüllt.

Die Krankenhausleitung hat sich für die Hinweise bedankt und die erforderlichen Maßnahmen veranlasst.

2.12.4 Patienten- und Betreuungsverfügungen

Ein Internetverlag bietet allen Interessierten an, eine so genannte Vorsorgeakte in einer Datenbank anzulegen. Darin kann gespeichert werden, ob und bei welcher Stelle jemand eine Patienten-, Betreuungs- oder Organverfügung oder eine Vorsorgevollmacht hinterlegt hat. Mit einer solchen Verfügung kann jeder bestimmen, was mit ihm geschehen soll, wenn er wegen seines Gesundheitszustandes selbst keine Entscheidungen mehr treffen kann. Der Verlag hat sich bei seinem Angebot von dem Gedanken leiten lassen, dass die beste Verfügung nichts nutzt, wenn nicht bekannt ist, dass und wo sie existiert.

Der Datenbestand über Angaben zur Vorsorge kann über das Internet von berechtigten Stellen wie Krankenhäusern oder Vormundschaftsrichtern abgefragt werden. Tritt der Vorsorgefall ein, kann die Verfügung bei der Stelle, die sie aufbewahrt, angefordert werden. Hinterlegt werden diese Verfügungen häufig bei Rechtsanwälten oder Notaren.

Eine Rechtsanwaltskanzlei, die den Internetverlag vertritt, fragte mich, ob nach den landesrechtlichen Regelungen Krankenhäuser Patientenverfügungen erhalten können, die mit einer Betreuungsverfügung verbunden sind.

Nach dem Landeskrankenhausgesetz (LKHG M-V) dürfen Patientendaten nur erhoben und gespeichert werden, soweit dies für die Aufgabenerfüllung des Krankenhauses erforderlich ist, ein Gesetz dies vorschreibt oder erlaubt oder der Patient im Einzelfall eingewilligt hat (§ 15 Abs. 1 LKHG M-V). Betreuungswünsche sind jedoch für die Behandlung im Krankenhaus nicht erforderlich und dürfen deshalb dort nicht erhoben und gespeichert werden. Deswegen habe ich empfohlen, die Verfügungen gegebenenfalls so voneinander zu trennen, dass sie einzeln versandt werden können. Ist dies nicht möglich, müssen die Aussagen der Betreuungsverfügung vor dem Versand unkenntlich gemacht werden, so dass das Krankenhaus nur die Patientenverfügung lesen kann.

Allerdings konnte ich nicht prüfen, ob und welche technischen und organisatorischen Maßnahmen bei der Datenübermittlung über das Internet getroffen worden sind, weil der Internetverlag keine öffentliche Stelle unseres Landes ist. Der Anwaltskanzlei habe ich daher empfohlen, sich an die zuständige Aufsichtsbehörde des Landes zu wenden, in dem

der Verlag seinen Sitz hat. Dort muss dann geprüft werden, ob die Maßnahmen ausreichend sind und dem Stand der Technik entsprechen.

2.12.5 Datenübermittlung vom Krankenhaus an Dritte

Der Datenschutzbeauftragte eines Krankenhauses hat mich gefragt, ob der Bundesverband für Rehabilitation und Interessenvertretung Behinderter (BDH) und der Behindertensportverband vom Krankenhaus Adressen von Patienten ohne deren vorherige Zustimmung erhalten dürfen. Beide Verbände wollten die ehemaligen Patienten schriftlich auf ihr Leistungsangebot aufmerksam machen und sie weiter betreuen.

Die Adressen sind Patientendaten und unterliegen somit den datenschutzrechtlichen Bestimmungen des Landeskrankenhausgesetzes (§§ 14 ff. LKHG M-V). Patientendaten dürfen an Dritte nur übermittelt werden, soweit dies im Sinne von § 17 LKHG M-V erforderlich ist oder wenn der Patient eingewilligt hat. Da das Leistungsangebot der Verbände jedoch nicht auf eine ärztliche Mit- oder Nachbehandlung im Anschluss an den Aufenthalt im Krankenhaus gerichtet ist, wäre die Weitergabe der Adressen nur mit der Einwilligung der Patienten zulässig.

Allerdings könnten Patienten durchaus an dem Angebot interessiert sein. Um den Kontakt zwischen den Verbänden und den interessierten Patienten in datenschutzgerechter Weise herzustellen, kann das so genannte Adressmittlungsverfahren verwendet werden. Dazu übergeben die Verbände dem Krankenhaus die Schreiben über ihre Leistungsangebote mit der Bitte, die Adressen der Patienten einzutragen und die bereits frankierten Schreiben zu versenden. Der Patient kann dann frei entscheiden, ob er die Angebote nutzen möchte.

Das Krankenhaus wird künftig entsprechend meiner Empfehlungen verfahren.

2.12.6 Erhebung von Patientendaten im Krankenzimmer

Patienten haben wiederholt berichtet, dass in Krankenhäusern die ärztliche Schweigepflicht und die datenschutzrechtlichen Vorschriften nicht im gesetzlich geforderten Umfang beachtet werden. Sie beschwerten sich beispielsweise darüber, dass Anästhesisten zur Vorbereitung von Operationen oder Stationsärzte zur ärztlichen Dokumentation Daten

von Patienten am Krankenbett erheben. Dabei können andere Patienten im Krankenzimmer die Gespräche mithören und erlangen Kenntnis von mitunter sensiblen Daten aus der Intimsphäre des Befragten.

Damit die Krankenhäuser die Rechte der Patienten künftig besser wahren, habe ich sie auf Folgendes hingewiesen:

Das Arzt-Patienten-Gespräch sollte vertraulich geführt werden. Deshalb ist den Patienten anzubieten, das Gespräch außerhalb des Krankenzimmers in Räumen mit wenig Patienten- und Besucherverkehr zu führen. Sollte der Patient ein Gespräch am Krankenbett wünschen, ist von ärztlicher Seite darauf zu achten, dass andere Personen im Krankenzimmer den Inhalt der Unterhaltung nicht mithören können. Dies kann beispielsweise durch eine angemessene Lautstärke oder durch das selbständige Ausfüllen von Datenerhebungsbögen durch den Patienten realisiert werden.

Auch bei der weiteren Verarbeitung der Daten ist darauf zu achten, dass nur die Personen, die an der Behandlung und Pflege beteiligt sind, im jeweils erforderlichen Umfang Kenntnis davon nehmen können.

Bei Visiten sollte am Krankenbett nur das unbedingt Notwendige mit dem Patienten besprochen werden. Intensive Diskussionen des medizinischen Falles sollten der Vor- bzw. Nachbereitung der Visite vorbehalten bleiben.

Das ärztliche Personal konnte die Argumentation nachvollziehen und wird künftig in der vorgeschlagenen Weise verfahren.

2.12.7 Bürokratie bei Patientenbeschwerden?

Ein Mitarbeiter des Sozialministeriums unseres Landes hat mir mehrere Fälle geschildert, in denen Patienten lange auf eine Antwort warten mussten, wenn sie sich bei der Ärztekammer, der Kassenärztlichen oder der Kassenzahnärztlichen Vereinigung über eine ärztliche Behandlung beschwert hatten. Ein Grund für die Verzögerung war nach seiner Meinung, dass die Patienten regelmäßig gebeten worden sind, erst noch den behandelnden Arzt von der Schweigepflicht zu entbinden, bevor ihr Fall überhaupt bearbeitet wurde. Der Mitarbeiter des Sozialministeriums bat mich um eine Stellungnahme, ob eine Schweigepflichtentbindung in jedem Fall erforderlich sei.

Dazu habe ich ihm Folgendes mitgeteilt:

Ist aus einer Beschwerde erkennbar, dass der Patient den Kontakt der Stelle, die seine Beschwerde bearbeitet, mit dem behandelnden Arzt nicht wünscht, darf sie keine personenbezogenen Daten des Patienten übermitteln. Sofern eine Beschwerde dann nicht bearbeitet werden kann, ist dies dem Patienten zu erläutern, und er sollte auf seine weiteren rechtlichen Möglichkeiten hingewiesen werden.

Beschwerden von Patienten über ihre ärztliche Behandlung können nach meiner Auffassung dann ohne eine zusätzliche Erklärung bearbeitet werden, wenn der Patient selbst sein Krankheitsbild schildert, den behandelnden Arzt nennt und konkret beschreibt, was ihm an der ärztlichen Behandlung missfallen hat. Mit einer solchen Schilderung erteilt er der Beschwerdestelle den Auftrag, den Sachverhalt aufzuklären. Sofern der Patient dazu keine allgemeine medizinische Frage hat, sondern erkennbar ist, dass seine Frage auf ein Detail seiner Behandlung zielt, wird er damit rechnen, dass die Beschwerdestelle den behandelnden Arzt um eine Stellungnahme bittet. Im Grunde muss die Beschwerdestelle sogar dem behandelnden Arzt mitteilen, worüber sich der Patient beschwert hat, damit der Arzt weiß, in welchem Umfang er medizinische Sachverhalte offenbaren darf. Dies darf eben nur im Rahmen des von dem Patienten geschilderten Sachverhaltes geschehen. Liegen diese Voraussetzungen vor, entbindet der Patient den behandelnden Arzt gegenüber der Beschwerdestelle auch ohne eine weitere Erklärung von der strafrechtlich bewehrten Schweigepflicht. Insofern gibt er eine so genannte konkludente Einwilligung ab.

Mitunter können Beschwerden nur dadurch beantwortet werden, dass auch Angaben anderer behandelnder Ärzte, die der Patient nicht genannt hat, einbezogen werden müssen. Dies kann sich zum Beispiel aus der Stellungnahme des befragten Arztes ergeben. In diesen Fällen ist eine vom Patienten unterschriebene Erklärung erforderlich, durch die er diese Ärzte von der Schweigepflicht entbindet. Von einer konkludenten Einwilligung kann die Beschwerdestelle hier nicht ausgehen, weil der Patient nicht weiß, dass und welche anderen Behandlungen mit beurteilt werden müssen.

Bevor jedoch wegen einer Beschwerde Patientendaten übermittelt werden, ist stets zu prüfen, ob dies überhaupt erforderlich ist. Beschwert sich ein Patient beispielsweise über für ihn ungünstige Sprechzeiten, kann der Arzt allgemein zur Praxisorganisation befragt werden. Die Übermittlung von Patientendaten ist dafür unzulässig, weil der Arzt sie für diese allgemeine Frage nicht benötigt.

Der Mitarbeiter des Sozialministeriums hat meine Stellungnahme an die Beschwerdestellen weitergegeben, damit Patienten künftig zügiger eine Antwort erhalten können.

2.12.8 Wohin mit den ärztlichen Unterlagen bei Praxisaufgabe?

Mitte des Jahres 2002 war Pressemeldungen zu entnehmen, dass in naher Zukunft besonders in den neuen Bundesländern vermehrt niedergelassene Ärzte ihre Praxis aufgeben werden. Aus datenschutzrechtlicher Sicht ist in solchen Fällen von Interesse, was mit den Patientenunterlagen geschieht.

Nach ihrer Berufsordnung sind Ärztinnen und Ärzte in Mecklenburg-Vorpommern verpflichtet, Aufzeichnungen und Untersuchungsbefunde eines Patienten zehn Jahre aufzubewahren, nachdem dessen Behandlung abgeschlossen ist. Geben sie ihre Praxis auf, müssen sie dafür sorgen, dass alle Unterlagen „in gehörige Obhut“ gegeben werden (§ 10 Abs. 4 BOÄ).

Dies ist relativ einfach wenn der Arzt einen Nachfolger für seine Praxis findet. In diesem Fall kann er dem Nachfolger die ärztlichen Aufzeichnungen in einem versiegelten Umschlag übergeben. Die Patienten können dann entscheiden, ob sie sich von dem Nachfolger behandeln lassen und die vorhandenen Unterlagen zur weiteren Nutzung freigeben. Wählt ein Patient jedoch einen anderen Arzt, erhält dieser die Unterlagen.

Gibt es aber keinen Nachfolger, muss der Arzt eine andere Lösung zur Aufbewahrung der Unterlagen finden. Dabei ist zu gewährleisten, dass Patienten auch nach Schließung der Praxis ihre Krankenunterlagen innerhalb der Aufbewahrungsfristen einsehen und Kopien erhalten können. Die Vergangenheit hat jedoch gezeigt, dass Patientenakten nicht immer so aufbewahrt werden, wie dies im Interesse der Patienten erforderlich ist.

Ich habe die Sozialministerin unseres Landes auf diesen Sachverhalt aufmerksam gemacht und angefragt, wer sich bei fehlender Praxisnachfolge der ärztlichen Unterlagen und Patientendokumentationen annimmt. Mir wurde mitgeteilt, dass die zur Aufbewahrung der ärztlichen Aufzeichnungen in der Berufsordnung getroffenen Regelungen ausreichen. Wie der Arzt seiner berufsrechtlichen Verpflichtung im Einzelnen nachkommt, bleibt ihm überlassen. Findet der Arzt keinen Praxisnachfolger, kann er die Unterlagen beispielsweise auch einem anderen zur Aufbewahrung bereiten Arzt treuhänderisch übergeben. Sollte dies nicht möglich sein, kommt auch die Verwahrung durch ein kommerzielles Unternehmen in Betracht. Entscheidet sich ein Arzt für diese Variante, so kann er sich an die Ärztekammer Mecklenburg-Vorpommern wenden, die ihm dann eine entsprechende private Stelle empfehlen wird.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zu diesem Thema beraten. Im Ergebnis hat der Vorsitzende die Gesundheitsministerkonferenz gebeten, sich dafür einzusetzen, dass nach der Schließung von Arztpraxen die betroffenen Patienten weiter Zugang zu ihren Daten haben und ein sorgsamer Umgang mit diesen gewährleistet ist.

Die Sozial- und Gesundheitsminister des Bundes und der Länder haben ihre Erfahrungen zur weiteren Aufbewahrung der Patientenunterlagen bei der Schließung von Arztpraxen ausgetauscht. Die Mehrheit der Länder ist der Auffassung, dass die in den jeweiligen Berufsordnungen getroffenen Regelungen, die Unterlagen zehn Jahre aufzubewahren verbunden mit der Verpflichtung, sie bei Praxisaufgabe in „gehörige Obhut“ zu geben, ausreichen. Eine entsprechende Umfrage unter den Ländern ergab, dass wegen der geringen Anzahl von Fällen der Praxisaufgabe bisher keine Erfahrungen vorliegen. Dies sei zumindest ein Indiz dafür, dass die berufsrechtlichen Vorgaben durch die betroffenen Ärzte beachtet werden. Gleichwohl wollen die Minister die weitere Entwicklung beobachten und bei Bedarf Handlungsoptionen erarbeiten.

2.13 Personalwesen

2.13.1 Personalverwaltungssystem für Lehrer

Der Lehrerhauptpersonalrat des Ministeriums für Bildung, Wissenschaft und Kultur unseres Landes hat mich Mitte des Jahres 2002 darum gebeten, den Entwurf einer Dienstvereinbarung zur Anwendung des Personalverwaltungssystems PERSYS-REDESIGN zu prüfen. Es handelt sich hierbei um eine modifizierte Version des Personalverwaltungssystems PERSYS (siehe Zweiter Tätigkeitsbericht, Punkt 2.13.3), mit dem in den Schulämtern und im Ministerium die Personaldaten der Lehrer verarbeitet werden sollen.

Ich habe die Unterlagen geprüft und dem Lehrerhauptpersonalrat empfohlen, einzelne Regelungen ändern zu lassen. Nach einem knappen Jahr lag allerdings immer noch keine unterzeichnete Dienstvereinbarung vor und auch das erforderliche Sicherheitskonzept (§ 22 Abs. 5 DSG M-V) fehlte. Der Personalrat war deshalb nicht in der Lage zu beurteilen, ob die Daten sicher und ordnungsgemäß verarbeitet werden. Er bat um weitere Beratung zu den datenschutzrechtlichen Aspekten des Entwurfes der Dienstvereinbarung. Dabei stellte sich heraus, dass PERSYS-REDESIGN schon seit längerer Zeit in Betrieb ist. Aus diesem Grund habe ich die Personaldatenverarbeitung der Lehrer in einem Schulamt und im Ministerium für Bildung, Wissenschaft und Kultur kontrolliert und Folgendes festgestellt:

Lange vor der Einführung von PERSYS-REDESIGN hat das Ministerium für Bildung, Wissenschaft und Kultur eine Verwaltungsvorschrift erlassen, durch die es den Schulämtern wesentliche personalrechtliche Befugnisse übertragen hatte. Das Personalverwaltungssystem wird jedoch vom Ministerium administriert. Dort wird festgelegt, wie die Datenverarbeitung abzulaufen hat. Die Schulämter können nur sehr begrenzt die Verarbeitung der Daten ihrer Lehrer beeinflussen, obwohl sie nach der Verwaltungsvorschrift die verantwortliche Stelle sind. Sie haben beispielsweise auch keinen Einfluss darauf, welcher Mitarbeiter des Ministeriums welche Zugriffsrechte für die Daten erhält.

Darüber hinaus war nicht eindeutig geklärt, auf welcher rechtlichen Grundlage die Daten im Schulamt und im Ministerium verarbeitet werden. Öffentliche Stellen dürfen Daten zu Dienst- und Arbeitsverhältnissen verarbeiten, wenn dies erforderlich ist oder wenn eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung es erlaubt (§ 35 Abs. 1 DSG M-V). Auf eine Dienstvereinbarung könnte prinzipiell zwar verzichtet werden, allerdings müsste dann jeder einzelne Verarbeitungsschritt darauf geprüft werden, ob er erforderlich ist. Eine Dienstvereinbarung vereinfacht das Verfahren wesentlich, weil mit ihr unter anderem festgelegt werden kann, wer zu welchem Zweck und in welchem Um-

fang auf Daten zugreifen und sie verarbeiten darf. Da Personalverwaltungssysteme eine umfassende Auswertung der Daten ermöglichen, sollten solche komplexen Datenverarbeitungssysteme nur auf der Grundlage entsprechender Vereinbarungen mit dem Personalrat eingeführt werden.

Weil die personalrechtlichen Befugnisse der Schulämter bei der automatisierten Verarbeitung der Daten nicht umgesetzt worden waren und auch unklar war, auf welcher Rechtsgrundlage Daten verarbeitet werden, habe ich die Datenverarbeitung gegenüber dem Ministerium für Bildung, Wissenschaft und Kultur beanstandet.

In meinem Kontrollbericht habe ich Empfehlungen zum Personalverwaltungssystem gegeben, die zu datenschutzrechtlichen Verbesserungen führen sollen. So muss eindeutig geregelt werden, für welchen Teil der automatisierten Personaldatenverarbeitung das Ministerium und für welchen Teil das Schulamt verantwortlich ist. Darüber hinaus habe ich vorgeschlagen, in der Dienstvereinbarung festzulegen, welcher Mitarbeiter auf welche Datenauswertungen zugreifen darf. Dadurch sollen die inhaltlich nicht näher spezifizierten Lese- und Schreibrechte ersetzt werden.

Eine abschließende Stellungnahme des Ministeriums für Bildung, Wissenschaft und Kultur liegt mir bisher nicht vor. Allerdings wurde mir signalisiert, dass die Empfehlungen umgesetzt werden sollen.

2.13.2 Zu viele Mitarbeiterdaten im Internet

Ein Universitätsangehöriger informierte mich, dass ein Institut seine Mitarbeiter mit einer kurzen Aufgabenbeschreibung, der dienstlichen Telefonnummer, der E- Mail-Adresse sowie einem Foto im Internet vorstellt. Die Mitarbeiter hatten bisher in die Veröffentlichung ihrer Daten nicht eingewilligt, und der Petent wollte nun von mir wissen, ob die Vorgehensweise der Universität rechtens sei.

Genauso wie andere Institutionen ist auch die Universität daran interessiert, ihr Angebot sowie die Ansprechpartner einem breiten Interessentenkreis zugänglich zu machen. Wird dazu das Internet genutzt, wird leicht gegen datenschutzrechtliche Bestimmungen verstoßen, weil immer noch nicht hinreichend bekannt ist, welche Informationen veröffentlicht werden dürfen.

Bei der Veröffentlichung von Mitarbeiterdaten im Internet ist § 35 Landesdatenschutzgesetz zu beachten. Danach können diese Daten veröffentlicht werden, wenn Art oder Ziel ihrer Aufgabe oder der Dienstverkehr es erfordern. Hierunter fällt auch die Information, welcher Mitarbeiter der richtige Ansprechpartner für Anliegen der Bürger ist. Die uneingeschränkte Veröffentlichung von Telefonverzeichnissen und Geschäftsverteilungsplänen mit den Namen aller Mitarbeiter ist hingegen unzulässig. Demzufolge kommen für eine Veröffentlichung im Internet lediglich folgende Personenkreise in Betracht: die obere Leitungsebene, wissenschaftliches Personal (dies gilt nicht für wissenschaftliche Hilfskräfte) sowie Mitarbeiter mit Außenkontakten, die als offizielle Ansprechpartner fungieren. Sollen darüber hinaus weitere Mitarbeiter im Internet vorgestellt werden, so ist dies nur mit deren Einwilligung zulässig und nur dann, wenn die Veröffentlichung zur Aufgabenerfüllung erforderlich ist.

Der Umfang der veröffentlichten Daten darf sich dabei nur auf Name, Funktion und Tätigkeitsbereich, dienstliche Haus-, Post- und E-Mail-Adresse sowie dienstliche Telefon- und Faxnummern erstrecken. Weitergehende Daten oder Fotos dürfen nur in das Internet eingestellt werden, wenn der jeweilige Mitarbeiter einwilligt.

Aufgrund meiner Hinweise hat die Universitätsleitung alle Fakultäten angewiesen, künftig die datenschutzrechtlichen Vorschriften bei Veröffentlichungen im Internet zu beachten. Ausführliche Informationen gibt die Orientierungshilfe „Datenschutzfragen zur Präsentation von öffentlichen Stellen im Internet“, die kostenlos in meiner Behörde erhältlich ist oder aus dem Internet unter www.lfd.m-v.de heruntergeladen werden kann.

2.13.3 Namensschilder im Krankenhaus

Eine Krankenschwester hat sich an mich gewandt, weil ihr Arbeitgeber alle Mitarbeiter angewiesen hatte, im Dienst ein Schild mit Vor- und Zunamen sowie einem Foto zu tragen. Sie sprach sich vor allem deshalb dagegen aus, weil sie in der psychiatrischen Abteilung arbeitet und befürchtete, dass durch das Schild Patienten leicht in der Lage wären, ihre Anschrift zu ermitteln und sie in ihrer privaten Sphäre zu belästigen.

Im Krankenhaus ist es üblich, dass das Pflegepersonal an der Berufskleidung Namensschilder trägt. Bei Krankenschwestern ist in der Regel der Vorname ersichtlich, damit Patienten sie ansprechen können. Datenschutzrechtlich ist es zunächst unbedenklich, wenn das Pflegepersonal im Dienst Namensschilder tragen soll. Das Personal eines Krankenhauses arbeitet im öffentlichen Bereich, so dass es für die Patienten auch ansprechbar sein muss.

Gleichwohl hat der öffentliche Arbeitgeber das Informationsrecht der Patienten gegen das individuelle Schutzbedürfnis der Beschäftigten abzuwägen. Dabei hat er zu beachten, dass Mitarbeiterdaten nur in dem erforderlichen Umfang weitergegeben werden dürfen. Ich habe dem Krankenhaus empfohlen, die einander gegenüberstehenden Interessen der Patienten und der Beschäftigten sorgfältig abzuwägen und es gerade im psychiatrischen Bereich den Beschäftigten selbst zu überlassen, ob sie auf das Schild nur ihren Vornamen oder ihren Vor- und Zunamen eintragen lassen. Das Krankenhaus wird künftig meine Hinweise berücksichtigen. Die Krankenschwester habe ich über meine Empfehlung informiert.

2.13.4 Bericht zur Gleichstellung von Frau und Mann

Ein Markt- und Sozialforschungsinstitut erhielt von der Gleichstellungsbeauftragten unseres Landes den Auftrag, einen Bericht zur Gleichstellung der in der Landesverwaltung beschäftigten Personen zu fertigen. Der Geschäftsführer des Institutes hat mich Anfang des Jahres 2003 gebeten zu prüfen, ob die für den Bericht vorgesehene Datenverarbeitung zulässig sei. Dazu legte er mir den Vertrag zwischen dem Institut und der Gleichstellungsbeauftragten sowie den Katalog der zu verarbeitenden Daten vor.

Die erforderlichen Daten soll das Landesbesoldungsamt liefern. Das Institut benötigt ausschließlich pseudonymisierte Daten der Beschäftigten. Eine Anonymisierung war nicht möglich, weil zeitliche Entwicklungen in der geschlechtsspezifischen Beschäftigungsstruktur festgestellt werden sollen. Dazu müssen die Datensätze zu den einzelnen Personen in bestimmten Zeitabständen verglichen werden.

Der vom Landesbesoldungsamt zu übermittelnde Datensatz enthält darüber hinaus überwiegend so genannte skalierte Daten. So kann auch aus Merkmalen, die selten vorkommen, kein Beschäftigter identifiziert werden. Beispielsweise soll anstelle der konkreten Zahl der Kinder angegeben werden, ob der Beschäftigte keine Kinder (Schlüsselziffer 0), ein bis zwei Kinder (Schlüsselziffer 1) oder mehr als zwei Kinder (Schlüsselziffer 2) hat. Auch bei der Dauer des Beschäftigungsverhältnisses wird lediglich erfasst, ob sie kurzzeitig (unter drei Jahre – Schlüsselziffer 1), von mittlerer Dauer (drei bis unter sechs Jahre – Schlüsselziffer 2) oder langzeitig (über sechs Jahre – Schlüsselziffer 3) ist.

Im Ergebnis konnte ich feststellen, dass die wesentlichen datenschutzrechtlichen Bestimmungen berücksichtigt worden waren. Besonders die Tatsache, dass nur pseudony-

misierte und überwiegend skalierte Daten für den Bericht verarbeitet werden, entspricht den Prinzipien der Datensparsamkeit und der Datenvermeidung. Allerdings fehlt bisher eine datenschutzrechtliche Vorschrift, die es dem Landesbesoldungsamt gestattet, die Daten für diesen Zweck zu übermitteln. Das Landesbesoldungsamt verarbeitet die Daten im Auftrag der Personalakten führenden Dienststellen. Deshalb habe ich der Gleichstellungsbeauftragten empfohlen, dass diese Stellen bestimmen müssten, ob und wie die Daten für die Berichterstattung verwendet werden. Sie könnten beispielsweise den Auftrag an das Landesbesoldungsamt erweitern und festlegen, dass es die erforderlichen Daten übermitteln soll. Die Empfehlung wurde umgesetzt.

2.13.5 Einsichtsrecht in die eigene Personalakte

Eine Petentin hat mich gefragt, ob ihr Arbeitgeber sie vertrösten dürfe, wenn sie ihre Personalakte einsehen möchte. Meines Erachtens gab es dafür keinen Grund. Für Mitarbeiter des öffentlichen Dienstes regeln § 13 Bundesangestelltentarif-Ost und § 102 Landesbeamtengesetz das Recht auf Einsicht in die eigene Personalakte. In der Personalaktenrichtlinie Mecklenburg-Vorpommern vom 14. Oktober 1994 sind detailliertere Regelungen dazu getroffen. Diese Rechtsvorschriften sagen aber nichts darüber aus, zu welchem Zeitpunkt die Einsicht zu gewähren ist.

Aus dem Sinn und Zweck des Akteneinsichtsrechtes folgt jedoch, dass der Arbeitnehmer das Recht auf Einsicht in die Personalakte zu jeder für den Arbeitgeber zumutbaren Zeit ausüben kann, wenn dabei die betrieblichen Interessen gewahrt werden. Die Personalakte kann damit während der Dienststunden und in angemessenen Abständen eingesehen werden. Nur wenn die Akte nicht sofort verfügbar ist, muss der Arbeitnehmer eine zeitliche Verzögerung hinnehmen. Der Arbeitgeber darf den Zeitpunkt der Einsicht nicht ohne zwingenden Grund hinausschieben. Die Dauer der Einsicht richtet sich nach dem Wunsch des Arbeitnehmers.

Ich habe die Petentin über ihre Rechte informiert.

2.13.6 Kontrolle der privaten Nutzung eines Diensttelefons

Eine Petentin hat von ihrem Arbeitgeber, einem Landkreis, ein Handy zur dienstlichen Nutzung erhalten. Der Arbeitgeber kontrollierte, ob die damit geführten Gespräche dienstlich begründet waren. Er wählte dazu die in der Abrechnungsliste verzeichneten Telefonnummern und fragte die sich meldenden Personen nach ihrem Namen. Ferner wollte er von ihnen wissen, ob sie sich erinnern können, welchen Zweck das geführte Gespräch hatte. Dies war aus datenschutzrechtlicher Sicht unzulässig.

Nach § 35 Landesdatenschutzgesetz kann der Arbeitgeber im Rahmen seiner Kontrollbefugnis dienstliche Telefongespräche lediglich stichprobenartig überprüfen. Er darf dabei klären, ob die Gespräche tatsächlich dienstlichen Bezug gehabt haben. Die Details dieser Kontrollen sind in einer Dienstvereinbarung zu regeln.

Eine Dienstvereinbarung ist insbesondere auch deshalb erforderlich, weil mit Handys technische Einrichtungen genutzt werden, die eine Verhaltens- oder Leistungsüberwachung der Beschäftigten ermöglichen. Die schutzwürdigen Interessen der Beschäftigten sind bei der Überprüfung von dienstlichen Telefongesprächen gewahrt, wenn der Personalrat seine Möglichkeiten der Mitbestimmung nach § 70 Abs. 1 Nr. 2 Personalvertretungsgesetz Mecklenburg-Vorpommern durch Abschluss einer solchen Dienstvereinbarung wahrnimmt.

Eine Nachfrage bei den angerufenen Gesprächsteilnehmern darf nur das letzte Mittel sein, um den Anlass des Gespräches zu klären. In jedem Fall muss zunächst der Beschäftigte über den Zweck der fraglichen Telefonate Auskunft geben. Erst wenn der Mitarbeiter den dienstlichen Grund seines Telefongespräches nicht erklären kann oder wenn der Arbeitgeber weitere begründete Zweifel hat, ob das Gespräch dienstlich veranlasst war, sollte ein Anruf beim auf der Liste verzeichneten Gesprächspartner erwogen werden.

Ich habe der Petentin die Rechtslage mitgeteilt. Sie wollte diese Angelegenheit selbst mit ihrem Arbeitgeber erörtern.

2.14 Bildung, Kultur, Wissenschaft und Forschung

2.14.1 Pseudonymisierung bei Arzneimittelstudien

Außerhalb des gesetzlich vorgegebenen Verfahrens der Zulassung von Arzneimitteln lassen Pharmaunternehmen auch ihre bereits zugelassenen Produkte in so genannten Anwendungsbeobachtungen oder Arzneimittelstudien prüfen. Solche Anwendungsbeobachtungen oder Studien werden unter anderem von Ärzten in Krankenhäusern im Auftrag der Unternehmen durchgeführt. Zu diesem Zweck werden den Unternehmen pseudonymisierte Daten des Patienten übermittelt, dem die Arzneimittel verabreicht worden sind. Anonymisierte Daten sind dafür nicht geeignet, weil mitunter die Ärzte zu weiteren medizinischen Details des Anwendungsfalles von den Unternehmen befragt werden. Diese Details können die Ärzte nur ermitteln, wenn sie in der Lage sind festzustellen, zu welchem Patienten die Falldaten gehören.

Der Datenschutzbeauftragte eines Krankenhauses berichtete mir, dass häufig die Initialen des Patienten und das Geburtsjahr oder auch das Geburtsdatum als Pseudonym genutzt werden. Er fragte, ob dies datenschutzrechtlich zu akzeptieren sei.

Der Begriff des Pseudonymisierens ist in § 3 Abs. 4 Satz 2 Nr. 9 Landesdatenschutzgesetz definiert. Danach sind Daten dann pseudonym, wenn sie so verändert worden sind, dass ohne Kenntnis der Zuordnungsfunktion die Einzelangaben über persönliche und sachliche Verhältnisse nicht mehr oder nur mit unverhältnismäßig hohem Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Das Bindeglied zwischen personenbezogenen und pseudonymisierten Daten ist somit die Zuordnungsfunktion. Sie kann im einfachen Fall eine Tabelle sein, in der beispielsweise jedem von einem Krankenhaus aufgenommenen Patienten eine laufende Nummer zugewiesen wird. Personen, die keinen Zugriff auf diese Tabelle haben und nur das Pseudonym kennen, können den Patienten daraus nicht bestimmen. Es ist aber auch möglich, Pseudonyme zu bilden, aus denen nur dann eine Person wieder bestimmt werden kann, wenn neben der Zuordnungsfunktion auch die Merkmale bekannt sind, aus denen das Pseudonym vorher einmal berechnet worden ist. Diese Pseudonyme werden mit mathematischen Verfahren erstellt. Dabei spielen auch kryptographische Algorithmen eine entscheidende Rolle.

Oftmals sind einfache Pseudonymisierungsverfahren bei Patientendaten durchaus ausreichend. Eine Pseudonymisierung mit Patienteninitialen und Geburtsdaten entspricht jedoch nicht den datenschutzrechtlichen Anforderungen. Aus diesen Daten könnte bei sel-

tenen Buchstabenkombinationen der Initialen und mit Nutzung öffentlich zugänglicher personenbezogener Daten, beispielsweise aus Telefon- oder Einwohneradressbüchern, relativ einfach eine Person bestimmt werden. Die Pharmaunternehmen erhalten ja nicht nur die Initialen des Patienten, sondern zusätzlich auch Angaben zum Krankenhaus und damit zum Ort, an dem die Studie durchgeführt worden ist. Dadurch ist der mögliche Personenkreis, der für eine Recherche in Frage kommen würde, weiter eingrenzbar. In aller Regel freilich werden die Unternehmen kein Interesse daran haben, einen Patienten aus einem Pseudonym zu bestimmen; aber aus datenschutzrechtlicher Sicht geht es immer auch darum, Missbrauchspotential möglichst von vornherein auszuschließen oder zumindest zu reduzieren. Dies ist, wie dargestellt, auch mit einfachen Mitteln möglich.

Dem Krankenhaus habe ich deshalb empfohlen, auf Initialen zu verzichten und nur tatsächlich pseudonymisierte Daten an die Pharmaunternehmen zu übermitteln. Weil aber die Unternehmen häufig die Pseudonymisierung mit Initialen bei der Auftragsvergabe vorgeben, habe ich auch der Ärztekammer und insbesondere ihrer Ethikkommission empfohlen, ihren Einfluss geltend zu machen und darauf hinzuwirken, dass datenschutzkonforme Pseudonymisierungen genutzt werden. Die Antwort der Ärztekammer steht noch aus.

Dieses Thema haben die Datenschutzbeauftragten des Bundes und der Länder darüber hinaus mit einem Vertreter des Arbeitskreises der medizinischen Ethikkommissionen diskutiert. Über das Ergebnis der Besprechung in diesem Arbeitskreis werden die Datenschutzbeauftragten noch unterrichtet.

2.14.2 Studentendaten vom Landesprüfungsamt an Universitäten

Das Ministerium für Bildung, Wissenschaft und Kultur unseres Landes hat das Landesprüfungsamt für Heilberufe gebeten, die Universitäten Rostock und Greifswald beim Erstellen der jährlichen Exmatrikulationsstatistik zu unterstützen. Das Landesprüfungsamt für Heilberufe führt unter anderem die staatlichen Prüfungen für Studenten der Humanmedizin und der Pharmazie durch. Es sollte den Universitäten die Prüfungsergebnisse der Studenten zumindest mit Matrikelnummer – also personenbeziehbar – mitteilen. Eine Mitarbeiterin des Amtes fragte mich, ob diese Datenübermittlung zulässig sei.

Personenbezogene Daten dürfen übermittelt werden, wenn dies zur Erfüllung einer in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgabe erforderlich ist und die Daten für den beabsichtigten Zweck genutzt werden dürfen (§§ 14 und 10 DSG M-V).

Eine Universität muss das Prüfungsergebnis eines Studenten beispielsweise dann kennen, wenn dieser sein Studium dort fortsetzt. Weder der Universität noch dem Landesprüfungsamt wäre aber zum Zeitpunkt der Datenübermittlung bekannt, ob dies der Fall sein wird. Somit ist die Übermittlung personenbezogener Daten von Studenten an die Universität für diesen Zweck nicht zulässig. Bevor die Daten übermittelt werden, wäre zu prüfen, ob einzelne Aufgaben nicht ebenso mit anonymisierten Daten erfüllt werden können. Für statistische Zwecke ist beispielsweise nur von Interesse, wie viele Studenten welche Punktwertbereiche oder Examensnoten erreicht haben.

Ich habe dem Ministerium für Bildung, Wissenschaft und Kultur und dem Landesprüfungsamt empfohlen, dass die Universitäten nur die personenbezogenen Daten erheben, die für die Fortführung des Studiums erforderlich sind. Die Daten sind jedoch nicht beim Landesprüfungsamt, sondern direkt bei den Studenten zu erheben, wenn sie sich bei der Universität zurückmelden. Diese Daten können dann unter bestimmten Voraussetzungen auch für statistische Zwecke genutzt werden.

2.14.3 Studentenchipkarten an Hochschulen

Im Vierten Tätigkeitsbericht, Punkt 3.13.1, hatte ich bereits über den Einsatz von Chipkarten für Studenten an Hochschulen informiert. Zum damaligen Zeitpunkt war der Einsatz nur auf freiwilliger Basis möglich, weil das Landeshochschulgesetz keine entsprechende Rechtsgrundlage enthielt. In den vergangenen beiden Jahren haben weitere Hochschulen solche Chipkarten eingesetzt. Studenten und Hochschullehrer fragten deshalb nach, welche datenschutzrechtlichen Vorschriften dabei zu beachten sind.

Mitte des Jahres 2002 trat das neue Landeshochschulgesetz in Kraft. Mit diesem Gesetz wurde den Hochschulen des Landes mehr Gestaltungsspielraum gegeben. Viele Sachverhalte können und müssen sie nun selbst durch Satzungen regeln. Dazu zählt unter anderem die Verarbeitung personenbezogener Daten der Studienbewerber, Studenten und Prüfungskandidaten. Auch die Verwendung von Studentenchipkarten ist nun in einer Satzung auf der Grundlage des Landesdatenschutzgesetzes (DSG M-V) zu normieren. So ist beispielsweise zu bestimmen, ob die Nutzung der Chipkarte obligatorisch oder freiwillig ist. In der Satzung müssen dann die weiteren Vorschriften über mobile Datenverarbeitungssysteme (§ 36 DSG M-V) umgesetzt werden.

Eine Hochschule hat mir inzwischen mitgeteilt, dass die Chipkarte dort auf freiwilliger Basis eingeführt werden soll. Studenten, die die Karte nicht nutzen möchten, können alle

Leistungen auf herkömmliche Weise erhalten und ihren Verpflichtungen wie bisher nachkommen. Alle Studenten wurden darauf hingewiesen und umfassend darüber aufgeklärt, welche Daten auf dem Chip gespeichert sind, welche Sicherheitsmechanismen eingerichtet sind und für welche Zwecke die Karte genutzt werden kann. Die Chipkarte soll den bisherigen Studentenausweis, den Bibliotheksausweis und die Mensakarte ersetzen. Mit ihr können sich die Studenten zum Folgesemester zurückmelden, aktuelle Studien- und gegebenenfalls BAföG-Bescheinigungen ausdrucken lassen, ihre Heimat- und Semesteranschrift ändern, Bücher aus der Bibliothek entleihen oder ihr Essen in der Mensa bezahlen. Geplant ist weiterhin, dass sie sich damit zu Prüfungen anmelden und ihre Prüfungsergebnisse abfragen können. Auf dem Chip sind nur die Matrikel- und die Bibliotheksnummer sowie die persönliche Identifizierungsnummer (PIN) gespeichert. Die Karte ist damit im Wesentlichen ein Zugangsschlüssel für in Dateien gespeicherte Daten. Über die im Chip gespeicherte Matrikelnummer können die dazugehörenden Datenbestände an der Hochschule erschlossen werden. Die fünfstellige PIN soll sicherstellen, dass keine unberechtigten Personen auf die Datenbestände des Studenten zugreifen. Der Karteninhaber kann seine PIN jederzeit an den in der Hochschule aufgestellten Terminals verändern. Die PIN wird nur auf der Karte gespeichert.

Auf der Kartenoberfläche sind der Name, der Vorname und das Passbild aufgedruckt, um die Chipkarte auch als Ausweis nutzen zu können. Außerdem befindet sich auf ihr ein Barcode, der die Bibliotheksnummer enthält, weil die Leihvorgänge in der Bibliothek darüber abgewickelt werden.

Ich habe den Hochschulen angeboten, sie bei der Erarbeitung der Satzungen zur Verarbeitung personenbezogener Daten zu unterstützen. Dieses Angebot wurde angenommen; die Beratungen dazu finden noch statt.

2.14.4 Sprachen-Portfolio

Eltern haben mir das vom Ministerium für Bildung, Wissenschaft und Kultur unseres Landes herausgegebene Heft „Mein Sprachen-Portfolio“ zugesandt und um datenschutzrechtliche Prüfung gebeten. Sie störten sich vor allem daran, dass der Lehrer den Schülern aufgegeben hatte, es auszufüllen und vorzulegen. Da den Unterlagen nicht zu entnehmen war, zu welchem Zweck und auf welcher Rechtsgrundlage diese Daten erhoben werden, und bei den Eltern der Eindruck entstanden ist, dass die Schüler verpflichtet sind, dieses Heft zu führen, habe ich das Ministerium für Bildung, Wissenschaft und Kultur um entsprechende Informationen gebeten.

Das Portfolio soll die fremdsprachliche Entwicklung der Schüler in den Klassenstufen 5 und 6 widerspiegeln. Es ist ein Angebot für Schüler, auf diese Weise ihre Sprachenkompetenz sowie die Fortschritte beim Lernen selbständig zu kontrollieren und zu dokumentieren. Jeder soll sein Passfoto einkleben und eintragen, welche Sprachen er spricht und wie er seine Sprachkenntnisse und -fähigkeiten einschätzt. Der Lehrer soll lediglich begleitend tätig werden, indem er Hinweise und Hilfen beim Ausfüllen gibt, beispielsweise zum behandelten Unterrichtsstoff oder zum erwünschten Lernziel. Die Schule verarbeitet die im Sprachen-Portfolio erhobenen Daten nicht und übermittelt sie auch nicht an Dritte. Den Schülern ist freigestellt, ob sie das Angebot annehmen.

Da die Freiwilligkeit der Teilnahme aus den Unterlagen nicht zu erkennen war, habe ich dem Ministerium für Bildung, Wissenschaft und Kultur empfohlen, Schüler und Erziehungsberechtigte ausdrücklich darauf und auf den Zweck des Heftes hinzuweisen. Das Ministerium ist meiner Empfehlung gefolgt und hat einen entsprechenden Hinweis erarbeitet.

2.14.5 Familien-Interna in Schülerarbeiten?

Immer wieder fragen Eltern oder Schüler, ob für Hausarbeiten oder Aufsätze Daten aus dem persönlichen Umfeld preisgegeben werden müssen. Beispiele hierzu sind bereits in meinem Dritten Tätigkeitsbericht, Punkt 3.15.2., dargestellt.

Nun bat mich ein Petent um eine datenschutzrechtliche Bewertung des folgenden Falles:

Schüler einer 11. Klasse sollten im Russischunterricht eine Hausarbeit zum Thema „Ich, mein Leben und meine Pläne für die Zukunft“ schreiben. Der Fachlehrer hatte dazu inhaltliche Schwerpunkte vorgegeben, die besonders stark die Privatsphäre der Schüler, der Eltern und der Geschwister berührten. Beispielsweise sollten der Geburtsort, mögliche Umzüge, die Konfession der Schüler, aber auch Berufe und Tätigkeiten der Eltern und Geschwister sowie deren Interessen und ihre persönlichen Beziehungen zu den Familienmitgliedern beschrieben werden. Der Petent befürchtete, dass die Familien hier möglicherweise „ausspioniert“ werden.

Es spricht nichts dagegen, lebensnahe Themen für schulische Arbeiten zu vergeben. Allerdings muss dabei die Privatsphäre der Schüler sowie ihrer Eltern und Verwandten respektiert werden. Im Zusammenhang mit der Aufgabenstellung sollte den Schülern daher erklärt werden, dass sie keine wahren Schilderungen, sondern auch eine fiktive wählen können. Entscheidet sich ein Schüler für eine wahre Schilderung und schreibt beispiels-

weise über seine Eltern und Geschwister, müsste er nach den allgemeinen datenschutzrechtlichen Bestimmungen sogar deren Einwilligung einholen, um ihre Daten zu verarbeiten. In der Praxis lässt sich aber nur schwer nachvollziehen, ob die formalen Voraussetzungen für eine solche Nutzung der Daten von Eltern und Verwandten vorliegen. Deshalb habe ich vorgeschlagen, generell auf solche Beschreibungen zu verzichten.

Neben der Wahl zwischen wahrer oder fiktiver Beschreibung könnte den Schülern auch angeboten werden, über eine historische Person oder eine Person des öffentlichen Lebens (Wissenschaftler, Künstler, Politiker) zu schreiben.

Ich habe der Schulleitung vorgeschlagen, meine Hinweise im Lehrerkollegium zu besprechen, damit diese bei künftigen Aufgabenstellungen berücksichtigt werden. Der Direktor hat sich für meine Hinweise bedankt und diese mit dem Fachlehrer für Russisch ausgewertet. Darüber hinaus wurden alle Lehrer mit den datenschutzrechtlichen Bestimmungen sowie mit meinen Empfehlungen vertraut gemacht.

Den Petenten habe ich über das Ergebnis informiert.

2.14.6 Entwicklung eines Sozialberichtssystems für einen Landkreis

Ein Forschungsinstitut erhielt von einem Landkreis den Auftrag, ein Berichtssystem zu entwickeln, das die aktuelle soziale Situation in den Amtsbereichen und Gemeinden abbildet. Die daraus gewonnenen Erkenntnisse sollen die politisch Verantwortlichen unterstützen, Strategien der Hilfe und Selbsthilfe für sozial benachteiligte Personen zu entwickeln.

Der Leiter des Institutes hat mich um Beratung gebeten, damit das Projekt den datenschutzrechtlichen Anforderungen gerecht wird.

Das Berichtssystem ist so konzipiert, dass in bestimmten Zeitabständen Daten über die persönliche Situation von Sozialhilfeempfängern erhoben und verarbeitet werden. Die Veränderungen der sozialen Verhältnisse sollen jederzeit dem Datensatz eines Betroffenen zugeordnet werden können, um die Entwicklung zu dokumentieren. Die Daten werden regelmäßig statistisch ausgewertet und ohne Bezug auf Einzelpersonen in Berichten dargestellt.

Ich habe vorgeschlagen, dass die Ämter des Landkreises die Daten pseudonymisieren, bevor sie an das Institut oder die Stelle übermittelt werden, die den Sozialbericht erstellt. Dieser Vorschlag wurde wie folgt umgesetzt: Praktikanten, die ohnehin für die Datenaufbereitung vorgesehen waren, unterstützen die Mitarbeiter der Sozialämter bei dieser zusätzlichen Aufgabe. Sie werden mit Dienstverträgen an das jeweilige Sozialamt arbeitsrechtlich gebunden. Damit unterliegen sie dem Sozialgeheimnis (§ 35 Erstes Buch Sozialgesetzbuch – SGB I), und der Leiter des Amtes kann die Datenaufbereitung umfassend kontrollieren. Die Praktikanten sind mit weiteren oder späteren Verarbeitungen nicht befasst.

Die pseudonymisierten Datensätze werden vor der Übermittlung durch Mitarbeiter des Landratsamtes noch bearbeitet und geprüft, um zu verhindern, dass aus einzelnen Daten eine Person bestimmbar ist. So wird zunächst die Gemeindekennziffer entfernt. Außerdem wird geprüft, ob eine konkrete Angabe in allen Datensätzen weniger als drei Mal auftritt, gegebenenfalls wird sie dann skaliert. Wenn beispielsweise die Anzahl der Kinder erfasst wird und es im Landkreis nur eine Person/Familie mit sechs Kindern gibt, so wäre sie aus dieser konkreten Angabe bestimmbar. Denn zumindest in der unmittelbaren Umgebung dieser Person oder Familie ist dies bekannt. Das Merkmal muss daher verändert werden, um eine Identifizierung auszuschließen. So könnte anstelle der konkreten Anzahl der Kinder nur die Tatsache „mehr als vier Kinder“ erfasst werden, sofern dieser Sachverhalt auf eine hinreichend große Zahl von Betroffenen zutrifft.

Die pseudonymisierten und geprüften Datensätze gibt eine verantwortliche Person des Landratsamtes für den Sozialbericht frei. Erst nach dieser Freigabe werden die Daten an das Institut übermittelt.

Neben den Daten von Sozialhilfeempfängern werden noch zufällig ausgewählte Bewohner des Landkreises nach ihren Lebensumständen befragt. Deren Adressdaten werden aus öffentlich zugänglichen Quellen gewonnen, wie Telefon- oder Einwohneradressbüchern. Die Betroffenen werden auf die Freiwilligkeit, den Zweck der Befragung und die Datennutzung hingewiesen. Auch diese Daten werden im Bericht so dargestellt, dass daraus keine Person bestimmt werden kann.

Mit der Umsetzung meiner Empfehlungen stand dem Einsatz des Sozialberichtssystems aus datenschutzrechtlicher Sicht nichts mehr im Wege. Das Sozialministerium unseres Landes hat dieses Projekt genehmigt.

2.14.7 Kopie des Rentenausweises beim Theaterbesuch?

Ein Rentner wollte in einer Vorverkaufsstelle eine ermäßigte Theaterkarte kaufen. Als er seinen Rentenausweis vorlegte, wunderte er sich, dass die Verkäuferin diesen kopierte. Auf seine Frage wurde ihm mitgeteilt, dass dieses Verfahren mit der Verwaltung des Theaters vereinbart worden sei. Der Petent bat mich, den Sachverhalt datenschutzrechtlich zu prüfen.

Personenbezogene Daten dürfen nur erhoben werden, wenn sie zur rechtmäßigen Aufgabenerfüllung der verarbeitenden Stelle erforderlich sind (§ 9 DSG M-V). Erforderlich sind die Daten immer dann, wenn die konkrete Aufgabe ohne sie nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllt werden kann.

Diese Voraussetzung war hier nicht erfüllt. Das Theater wollte die Ausweiskopien lediglich statistisch auswerten und im Anschluss vernichten. Dieser Zweck hätte erfüllt werden können, wenn die Vorverkaufsstelle die Anzahl der verkauften ermäßigten Eintrittskarten in einer Liste vermerkt hätte. Daher ist es unzulässig, beim Kauf einer ermäßigten Eintrittskarte den entsprechenden Nachweis zu kopieren und diesen mit der Abrechnung an das Theater zu übermitteln.

Über die statistische Verwendung hinaus wollte das Theater mit Hilfe der Kopien sicherstellen, dass nur berechtigte Theaterbesucher eine ermäßigte Karte nutzen. Doch auch dazu ist diese Verfahrensweise nicht geeignet. Nur bei der Einlasskontrolle kann geprüft werden, ob der Besucher berechtigt ist, eine ermäßigte Eintrittskarte zu nutzen. Dies habe ich dem Theater mitgeteilt und empfohlen, künftig keine Kopien mehr zu verlangen.

Das Theater teilte mir mit, es würde für die nächste Spielsaison ein neues Vorverkaufssystem eingesetzt, bei dem keine Ausweise kopiert werden. Das Ergebnis habe ich dem Petenten mitgeteilt.

2.15 Wirtschaft und Gewerbe

2.15.1 Sparkassenkunden und die US-Quellensteuer

Eine Sparkasse hat Anfang des Jahres 2002 alle Kunden, für die sie ein Wertpapierdepot führte, angeschrieben und ihnen einen Fragebogen zugeschickt. Die Fragen sollten beantwortet werden, um Empfänger von Erträgen aus US-amerikanischen Wertpapieren identifizieren zu können. Hintergrund war, dass die Finanzverwaltung der Vereinigten Staaten von Amerika umfangreiche Vorschriften zur Besteuerung dieser Erträge (US-Quellensteuer) erlassen hat. Aus diesen Vorschriften leitete die Sparkasse ab, dass sie verpflichtet sei, die Daten zu erheben.

In dem Fragebogen sollten die Kunden unter anderem angeben, ob sie US-Bürger sind oder ein Einwanderungsvisum besitzen, ob sie sich im laufenden Jahr über einen längeren Zeitraum (mindestens 31 Tage) in den USA aufgehalten haben oder ob sie einen Ehepartner haben, der US-Bürger ist und mit dem sie gemeinsam in den USA steuerpflichtig sind. Sofern sie aus einem anderen Grund der US-amerikanischen Steuerpflicht unterliegen, wäre dies von ihnen näher zu erläutern. Die Kunden wurden außerdem gebeten, in die Verarbeitung ihrer Daten einzuwilligen.

Ein Kunde wunderte sich über das ihm zugegangene Schreiben und den Fragebogen, weil er zwar ein Wertpapierdepot, aber keine US-Wertpapiere besaß. Er fragte mich, ob die Datenerhebung in diesem Fall zulässig sei.

Ich habe die verantwortlichen Mitarbeiter der Sparkasse gebeten, mir mitzuteilen, warum diese Daten nicht nur von den Kunden erhoben werden, die auch tatsächlich ein Depot mit US-Wertpapieren besitzen, und welchen Stellenwert die Einwilligung hat.

Der Vorstand der Sparkasse teilte mir mit, dass er sich für das geschilderte Verfahren entschieden hatte, da alle angeschriebenen Kunden selbst prüfen sollten, ob ihre Wertpapiere der US-Quellensteuer unterliegen. Eine gezielte Auswahl der Personen, die solche Wertpapiere halten, wäre mit einem erheblichen Aufwand verbunden gewesen, den die Sparkasse nicht leisten könne. Dass die Angaben freiwillig waren, ging nach Meinung des Vorstandes aus dem Anschreiben hervor, in dem um „Mithilfe“ gebeten wurde. Wenn die Daten nicht vorlägen, hätte dies Nachteile für die Kunden, weil dann ihre Erträge aus den Wertpapiergeschäften mit einem Steuersatz von 30 Prozent belegt würden. Diese Steuer müsste an die US-amerikanischen Finanzbehörden abgeführt werden. Liegen hingegen die Daten vor, so dass gegebenenfalls die Identität des Wertpapierinhabers gegenüber den

US-amerikanischen Behörden offenbart werden könnte, würde sich die Steuer erheblich verringern oder sogar ganz entfallen. Sofern ein Kunde sich beispielsweise über einen längeren Zeitraum in den USA aufgehalten hat, sei er berechtigt, ein bestimmtes amerikanisches Steuerformular auszufüllen, was sich auch auf die Höhe der Steuer auswirkt. Zur Einwilligungserklärung bemerkte der Vorstand, dass er im Interesse der Kunden verpflichtet sei, die Daten zu erheben; deshalb sei es gerechtfertigt, sie zu erbitten. Eine Rechtsgrundlage für die Datenerhebung existiert nicht.

Vor dem Hintergrund dieser Ausführungen habe ich der Sparkasse empfohlen, besser über die Datenerhebung aufzuklären und ausdrücklich darauf hinzuweisen, dass sie für die Betroffenen freiwillig ist. Die Kunden sollten darüber informiert werden, dass die Daten nur erforderlich sind, wenn sie US-Wertpapiere deponiert haben oder diese kaufen werden und wenn sie von der US-Quellensteuer befreit werden wollen. Darüber hinaus sollte die Sparkasse diejenigen Kunden, die bereits den Fragebogen ausgefüllt an die Sparkasse geschickt hatten, auf ihr Recht hinweisen, dieser Datenverarbeitung zu widersprechen. Bei einem Widerspruch muss die Sparkasse die Daten unverzüglich löschen.

Der Vorstand der Sparkasse teilte mir mit, dass er meine Hinweise umsetzt. Das Anschreiben und die Einwilligungserklärung wurden überarbeitet; beide Dokumente entsprechen nun den datenschutzrechtlichen Vorschriften. Alle Depotinhaber, die der Sparkasse bereits ihre Daten zur Verfügung gestellt hatten, wurden erneut angeschrieben, über die Datenerhebung ausführlich aufgeklärt und auf ihr Widerspruchsrecht hingewiesen.

2.15.2 Schwarzvermietern auf der Spur

Ein Petent hat mir einen Beitrag der OSTSEE-ZEITUNG zugeschickt, dem zu entnehmen war, dass ein Bürgermeister über den Energie- und Wasserverbrauch sowie über die Abwassermenge die Nutzung von Urlaubsquartieren berechnet hatte. Er wollte auf diese Weise prüfen, ob alle Anbieter von Urlaubsquartieren die Kurtaxe ihrer Feriengäste ordnungsgemäß abgeführt haben, da ein Einnahmeverlust gegenüber dem Vorjahr zu verzeichnen war. Der Einsender des Beitrages meinte, der Bürgermeister könnte dazu in nicht zulässiger Weise personenbezogene Daten der Vermieter verwendet haben.

Der Bürgermeister teilte mir dazu mit, dass er tatsächlich Daten über den Monats- und Jahresverbrauch von Wasser und Energie sowie über die jährliche und monatliche Abwassermenge für die gesamte Stadt vom Zweckverband und vom Energieversorger er-

halten habe. In seine Berechnungen hatte er darüber hinaus Verbrauchsdaten einbezogen, die ihm Bekannte freiwillig überlassen haben.

Dieses Verfahren ist datenschutzrechtlich nicht zu beanstanden, da Zweckverband und Energieversorgungsunternehmen lediglich den Gesamtverbrauch der Gemeinde und nicht den einzelner Haushalte übermittelt haben. Damit waren die Daten nicht personenbezogen und auch nicht personenbeziehbar, so dass darauf auch keine datenschutzrechtlichen Vorschriften anwendbar sind. Auch die Nutzung der personenbezogenen Verbrauchsdaten der Bekannten des Bürgermeisters war datenschutzrechtlich zulässig, da die Daten auf freiwilliger Basis zur Verfügung gestellt worden sind. Dies habe ich dem Petenten mitgeteilt.

2.15.3 Datenverarbeitung in einem Gewerbeuntersagungsverfahren

Ein Ordnungsamt führte gegen ein Ehepaar ein Gewerbeuntersagungsverfahren durch. Dabei beteiligte es unter anderem das Gewerbeaufsichtsamt, die Handwerkskammer, das Finanzamt sowie das Arbeitsamt. Es teilte diesen Stellen mit, dass hier tatsächliche Anhaltspunkte für die gewerberechtliche Unzuverlässigkeit und das Vorliegen eines Strohmannverhältnisses bestünden. Um das Strohmannverhältnis nachzuweisen, holte das Ordnungsamt auch Informationen beim Kreditinstitut der Betroffenen ein. Das Amt teilte dabei mit, dass das Ehepaar hohe Steuerrückstände und hohe Beitragsschulden habe.

Mit der Weitergabe dieser Daten waren die Betroffenen nicht einverstanden. Deshalb hat ihr Rechtsanwalt mich gebeten, den Sachverhalt datenschutzrechtlich zu bewerten.

Die Ausübung eines Gewerbes ist nach § 35 Gewerbeordnung (GewO) zu untersagen, wenn die betroffene Person unzuverlässig und die Untersagung zum Schutz der Allgemeinheit oder der im Betrieb Beschäftigten erforderlich ist.

Um die Zuverlässigkeit eines Gewerbetreibenden prüfen zu können, dürfen die hierfür notwendigen Daten nach § 11 Abs. 1 und 2 GewO beim Betroffenen und unter bestimmten Voraussetzungen auch bei Dritten erhoben werden. Vor einer Gewerbeuntersagung sollen die in § 35 Abs. 4 GewO genannten Stellen, unter anderem die Handwerkskammer, angehört werden. Dabei sind die gegen den Gewerbetreibenden erhobenen Vorwürfe mitzuteilen und die erforderlichen Unterlagen zur Einsichtnahme zu übersenden. Die anzuhörenden Stellen sind – im Gegensatz zu den Stellen, bei denen lediglich die nötigen Daten erhoben werden – über die Einzelheiten des Verfahrens zu informieren, damit sie sich sachgerecht hierzu äußern

können. Der Umfang der zu übermittelnden Daten wird durch den Grundsatz der Verhältnismäßigkeit begrenzt. Daher ist im Einzelfall genau zu prüfen, über welche Informationen die anzuhörende Stelle verfügen muss.

Im vorliegenden Fall ging es um die Prüfung der gewerberechtlichen Zuverlässigkeit sowie die damit verbundene Durchführung eines Gewerbeuntersagungsverfahrens. Das Ordnungsamt hat bei verschiedenen Stellen Auskünfte nach § 11 Abs. 2 GewO eingeholt beziehungsweise diese Stellen nach § 35 Abs. 4 GewO angehört. Den beteiligten Stellen wurden – außer in einem Fall – nicht mehr Daten übermittelt, als diese für die Beantwortung der Anfrage beziehungsweise zur Abgabe einer fachlichen Stellungnahme benötigten.

Die Datenweitergabe an das Kreditinstitut aber war zu weitgehend und mangels Rechtsgrundlage unzulässig. Für das Bestehen eines Strohmannverhältnisses lagen zwar tatsächliche Anhaltspunkte vor, so dass das Ordnungsamt Daten beim Kreditinstitut der Betroffenen erheben durfte. Es hat für diesen Zweck jedoch mehr Daten übermittelt, als erforderlich waren, um den Sachverhalt zu klären. Um zu prüfen, ob ein Strohmannverhältnis besteht, war es keinesfalls notwendig, Einzelheiten aus dem Verfahren gegen die Betroffenen weiterzugeben. Die Mitteilung an das Kreditinstitut, dass die Betroffenen insbesondere wegen hoher Steuerrückstände und hoher Beitragsschulden aus gewerberechtlicher Sicht unzuverlässig seien, gehörte nicht zu den Aufgaben des Ordnungsamtes. Darüber hinaus war auch zu berücksichtigen, dass nach § 11 Abs. 2 Satz 2 GewO bei der Erhebung personenbezogener Daten bei Dritten keine überwiegenden schutzwürdigen Belange der Betroffenen beeinträchtigt werden dürfen. Die Bekanntgabe von sensiblen Daten kann zu schweren Nachteilen wie Verlust der Kreditwürdigkeit und des Ansehens führen. Das hatte die Verwaltung in diesem Fall übersehen.

Der Leiter des Ordnungsamtes hat zugesagt, die schutzwürdigen Interessen von Betroffenen bei derartigen Auskunftsersuchen künftig sorgfältiger zu prüfen und nur noch die erforderlichen Daten zu übermitteln. Die Petenten habe ich über das Ergebnis informiert.

2.15.4 Zu viele Fragen an Mietinteressenten

Ein Interessent für eine Wohnung legte mir den Fragebogen einer kommunalen Wohnungsgesellschaft zur datenschutzrechtlichen Prüfung vor. Er hatte erhebliche Zweifel, ob alle erfragten Daten erforderlich sind, um Interessenten eine geeignete oder gewünschte Wohnung zu vermitteln.

Zwischen der Wohnungsgesellschaft und dem Petenten bestand zu diesem Zeitpunkt noch kein Vertragsverhältnis. Durch die Datenerhebung sollten jedoch Informationen für ein späteres Vertragsverhältnis gewonnen werden. Aber selbst für diesen Zweck erschien mir der Fragebogen zu umfangreich. Insbesondere die Angaben zum Familienstand, zu den Namen der mitziehenden Personen, zum aktuellen Mietverhältnis, zum Arbeitgeber und zur Höhe des Nettoeinkommens waren zu diesem Zeitpunkt meines Erachtens nicht erforderlich. Es dürfte beispielsweise genügen, wenn danach gefragt wird, wie viele Personen die Wohnung nutzen werden oder wie hoch die monatliche Miete maximal sein soll.

Dies habe ich der Wohnungsgesellschaft mitgeteilt und empfohlen, den Fragebogen zu überarbeiten.

Der Geschäftsführer der Wohnungsgesellschaft räumte ein, dass das Formular nicht daraufhin geprüft worden ist, ob die datenschutzrechtlichen Bestimmungen eingehalten werden. Der Antrag sollte lediglich eine Hilfestellung sein, um den passenden Wohnraum zuordnen zu können. Der Fragebogen wurde unter Berücksichtigung meiner Hinweise überarbeitet.

2.15.5 Wohnungsbaugesellschaft übermittelt Eigentümerdaten an Dienstleister

Eine Petentin hatte ein Grundstück von einer kommunalen Wohnungsbaugesellschaft erworben. Kurze Zeit darauf erhielt sie erste Rechnungen von dem Zweckverband für die Wasserversorgung und Abwasserbeseitigung und von dem Energieversorger, obwohl sie sich bei diesen Unternehmen noch nicht als neue Eigentümerin gemeldet hatte. Sie bat mich zu prüfen, woher diese Stellen von den geänderten Eigentumsverhältnissen wussten und ob diese Datenübermittlung rechtswidrig war.

Auf meine Nachfrage bestätigte die Wohnungsbaugesellschaft, dass sie die Daten über die neue Eigentümerin an diese Stellen übermittelt hatte, um damit den Eigentumsübergang ordnungsgemäß abzuwickeln.

Grundsätzlich sind laut Landesdatenschutzgesetz die Daten beim Betroffenen zu erheben, es sei denn, dass eine Rechtsvorschrift eine andere Art der Erhebung erlaubt (§ 9 Abs. 2 DSG M-V). Deshalb müssen der Zweckverband und der Energieversorger die Daten ihrer Kunden bei diesen direkt erheben. Beispielsweise hat sich nach der Satzung des Zweckverbandes der neue Eigentümer eines Grundstückes, das vom Anschluss- und Benutzungszwang für die Wasserversorgung und Abwasserbeseitigung betroffen ist, beim Zweckverband anzumelden. Mit der Anmeldung werden die personenbezogenen Daten erhoben, die zur Abrechnung der Verbrauchswerte erforderlich sind. Dies entspricht dem Grundsatz der Datenerhebung beim Betroffenen.

Die Übermittlung der Daten durch die Wohnungsbaugesellschaft an den Zweckverband und an den Energieversorger war somit nicht erforderlich und deshalb unzulässig. Ich habe der Gesellschaft die Rechtslage mitgeteilt und darauf hingewiesen, dass ich davon ausgehe, dass es sich in diesem Fall um ein Versehen gehandelt hat und die datenschutzrechtlichen Bestimmungen künftig beachtet werden. Die Petentin habe ich über meine rechtliche Bewertung informiert.

2.15.6 Wirtschaftsförderungsgesellschaft holt verdeckte Auskünfte ein

Ein Petent hat mir mitgeteilt, dass er sich von der Wirtschaftsförderungsgesellschaft Mecklenburg-Vorpommern und einer regionalen Gesellschaft beraten lassen hat. Im Nachhinein hat er erfahren, dass beide Stellen ohne seine Einwilligung Auskünfte über ihn bei einer Wirtschaftsauskunftei eingeholt haben. Der Petent wollte von mir wissen, ob dies zulässig ist.

Ich habe die Gesellschaften um eine Stellungnahme zu ihrer Praxis der Datenerhebung gebeten. Die Wirtschaftsförderungsgesellschaft Mecklenburg-Vorpommern vertrat zunächst die Ansicht, dass die Bestimmungen des Landesdatenschutzgesetzes (DSG M-V) für sie nicht gelten. Sie sei keine öffentliche Stelle, sondern eine dem nichtöffentlichen Bereich zuzurechnende Gesellschaft mit beschränkter Haftung (GmbH).

Bevor der eigentliche Sachverhalt geklärt werden konnte, musste ich der Wirtschaftsförderungsgesellschaft Mecklenburg-Vorpommern in einem zeitraubenden Schriftwechsel erklären, dass für juristische Personen und sonstige Vereinigungen des privaten Rechts das Landesdatenschutzgesetz gilt, wenn die Voraussetzungen des § 2 Abs. 2 DSG M-V erfüllt sind. Diese Voraussetzungen sind, dass die juristische Person des privaten Rechts Aufgaben der öffentlichen Verwaltung wahrnimmt und dass andere öffentliche Stellen

Mecklenburg-Vorpommerns die absolute Mehrheit der Anteile an der Gesellschaft besitzen. Beides war erfüllt: Die Wirtschaftsförderung ist eine öffentliche Aufgabe. Die absolute Mehrheit der Anteile an der Wirtschaftsförderungsgesellschaft Mecklenburg-Vorpommern hält unser Land. Somit gelten für die Gesellschaft bestimmte Vorschriften des Landesdatenschutzgesetzes und ergänzend die für nichtöffentliche Stellen des Bundesdatenschutzgesetzes, weil sie mit anderen Wirtschaftsförderungsgesellschaften im Wettbewerb steht (§ 2 Abs. 5 DSG M-V).

In der Sache selbst war die Vorgehensweise der Wirtschaftsförderungsgesellschaft weder bürgerfreundlich noch transparent. Sofern eine Rechtsvorschrift nichts anderes bestimmt, sind personenbezogene Daten beim Betroffenen oder mit seiner Einwilligung bei anderen Stellen zu erheben (§ 9 Abs. 2 DSG M-V). Eine entsprechende Rechtsvorschrift existiert jedoch nicht, denn die Beratung ist freiwillig. Folglich können Daten bei Wirtschaftsauskunfteien nur erhoben werden, wenn der Betroffene eingewilligt hat.

Der Geschäftsführer der Wirtschaftsförderungsgesellschaft hat erst nach langwierigem Schriftwechsel erklärt, dass er künftig meine Empfehlung beachten wird. Die regionale Wirtschaftsförderungsgesellschaft war dagegen von Anfang an aufgeschlossener und erklärte, Daten bei Wirtschaftsauskunfteien künftig nur mit Einwilligung der betroffenen Person einzuholen. Den Petenten habe ich über das Ergebnis informiert.

Alle anderen regionalen Wirtschaftsförderungsgesellschaften in unserem Land habe ich ebenfalls nach ihrer Praxis bei Beratungen gefragt und sie auf die notwendige Einwilligung des Betroffenen hingewiesen, wenn Daten über ihn bei Wirtschaftsauskunfteien oder anderen Stellen erhoben werden sollen. Diese Gesellschaften haben mir mitgeteilt, dass sie entsprechend verfahren.

2.16 E-Government

2.16.1 Gesetzliche Grundlagen

Bundesrecht
Am 1. Februar 2003 ist das Dritte Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften in Kraft getreten (BGBl. I S. 3322). Es regelt die elektronische Kommunikation mit den Bundesbehörden.

Die Empfehlungen der Datenschutzbeauftragten zum damaligen Entwurf für ein Elektronik-Anpassungsgesetz (siehe Punkt 3.17.2 des Fünften Tätigkeitsberichtes) sind dabei leider nur zum Teil berücksichtigt worden. So ist nach dem neuen § 3a Abs. 1 des Verwaltungsverfahrensgesetzes des Bundes (VwVfG) die Übermittlung elektronischer Dokumente zulässig, „soweit der Empfänger hierfür einen Zugang eröffnet“. Die Begründung zum Gesetzentwurf verlangt zwar, dass der Bürger ausdrücklich einwilligen muss, wenn er Dokumente in elektronischer Form erhalten möchte. Es wäre aber besser gewesen, eine Regelung im Gesetz selbst vorzusehen.

Positiv zu werten ist hingegen, dass die Verwaltung gemäß § 3a Abs. 2 Satz 2 VwVfG prinzipiell verpflichtet wird, elektronische Dokumente mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. Unverständlich ist jedoch, dass gerade in einem so sensiblen Bereich wie der Steuerverwaltung Abstriche an den Voraussetzungen für die Signatur zugelassen werden (siehe Punkt 2.16.3).

Landesrecht
Der Landtag von Mecklenburg-Vorpommern hat am 10. Dezember 2003 das Gesetz zur Förderung der elektronischen Kommunikation im Verwaltungsverfahren verabschiedet. Er hat dabei den Entwurf der Landesregierung vom 23. September 2003 (LT-Drs. 4/799) unverändert angenommen. Das Gesetz orientiert sich an dem oben genannten Bundesgesetz. Die Bürger unseres Landes können daher auch mit ihren Landes- und Kommunalbehörden elektronisch kommunizieren, sofern diese einen entsprechenden Zugang eröffnet und öffentlich bekannt gemacht haben.

Das neue Gesetz enthält eine Regelung, die eine öffentliche Zustellung auch durch Bereitstellung im Internet ermöglicht (§ 108 Abs. 2 Satz 1 des Landesverwaltungsverfahrensgesetzes – VwVfG M-V). Diese Form der öffentlichen Zustellung bedeutet im Gegensatz zu der klassischen Bekanntmachung durch Aushang eine weltweite Veröffent-

lichung personenbezogener Daten, deren weitere Verbreitung im Internet auch durch eine spätere Löschung gemäß § 108 Abs. 2 Sätze 5 und 6 VwVfG M-V nicht mehr verhindert werden kann.

Neu sind auch Regelungen im Landesmeldegesetz. So erlaubt dessen § 34 Abs. 1a eine Melderegisterauskunft über das Internet, wenn eine Person mit Vornamen, Nachnamen, Geschlecht und Staatsangehörigkeit „eindeutig" bestimmt wird. Man denke nur an eine Wortfolge wie „Klaus Meier, männlich, deutsch"! Das Beispiel verdeutlicht, dass ein solches Verfahren keine zweifelsfreie Identifizierung zulässt. Verwechselungen sind wahrscheinlich, was beispielsweise bei der Suche nach Schuldnern oder Unterhaltspflichtigen zu erheblichen Nachteilen für unbeteiligte Personen führen kann. In diesem Zusammenhang habe ich entsprechende Empfehlungen gegeben.

Das Innenministerium unseres Landes beabsichtigt, diese Anregungen zu prüfen, wenn das Landesmeldegesetz zur Anpassung an das Melderechtsrahmengesetz novelliert wird. Es ist jedoch zu hoffen, dass schon vorher Wege gefunden werden, systembedingte Personenverwechslungen bei der Melderegisterauskunft über das Internet zu vermeiden.

2.16.2 Empfehlungen zum datenschutzgerechten E-Government

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in ihrer Entschließung vom Oktober 2000 bereit erklärt, Entwicklungen um das Thema E-Government konstruktiv zu begleiten. Einen ersten Empfehlungskatalog zum Datenschutz für eine serviceorientierte Verwaltung veröffentlichten die Datenschutzbeauftragten bereits im Dezember 2000 (siehe Fünfter Tätigkeitsbericht, Punkt 3.17.1).

Im Dezember 2002 legten sie eine weitere Broschüre zum Thema E-Government vor, die mit Hilfe externer Sachverständiger des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie der Universitäten Kassel und Göttingen erarbeitet wurde. Im Mittelpunkt der Broschüre stehen konkrete, praxisorientierte Empfehlungen, die dazu beitragen sollen, dass schon während der Entwicklung von E-Government-Lösungen die Anforderungen an Datenschutz und Datensicherheit im Blick bleiben. Die detaillierten Hinweise können helfen, datenschutzgerechte und datenschutzfreundliche Verfahren zu entwickeln. Die Empfehlungen werden durch eine Zusammenstellung wichtiger technischer und organisatorischer Maßnahmen ergänzt. Dem Leser wird ein ganzer „Baukasten" mit einzelnen Maßnahmen vorgestellt, die unter anderem die Themen Verschlüsselung und elek-

tronische Signatur, Schutzprofile nach den Common Criteria, datenschutzgerechtes Web-Angebot, Sicherheitskonzept, Revision oder Selbstdatenschutz betreffen.

Um den Verwaltungschefs, den IT-Organisatoren, den Verfahrensentwicklern, den Personalvertretungen und den behördlichen Datenschutzbeauftragten den Einstieg in die komplizierte Materie zu erleichtern, sind im letzten Teil der Broschüre beispielhafte, von der jeweils zuständigen Datenschutzaufsicht geprüfte Lösungen für einzelne E-Government-Anwendungen aus dem gesamten Bundesgebiet dargestellt. Für jede Anwendung sind Ansprechpartner benannt, die sich bereit erklärt haben, potentiellen Nachnutzern ihre Erfahrungen bei der datenschutzgerechten Ausgestaltung des eigenen Verfahrens weiterzugeben.

Ich gehe davon aus, dass bei den E-Government-Planungen in unserem Land (siehe Punkt 2.16.4) die Empfehlungen der Broschüre berücksichtigt werden. Nur wenn eine sichere und vertrauliche Kommunikation zwischen Verwaltung und Bürgern sowie ein angemessener Schutz personenbezogener Daten gewährleistet ist, wird die notwendige Akzeptanz für E-Government-Anwendungen beim Bürger und bei der Verwaltung zu erreichen sein.

Die Broschüre „Datenschutzgerechtes E-Government – Handlungsempfehlungen“ ist kostenlos in meiner Dienststelle zu erhalten. Der Text ist in elektronischer Form aus dem Internetangebot meines niedersächsischen Kollegen abrufbar (http://www.lfd.niedersachsen.de).

2.16.3 Die elektronische Signatur

Die Verwaltung kann viele Dienstleistungen nur dann erbringen, wenn der „Kunde“ (z. B. Bürger, Unternehmen, Behörden) mit einer rechtsverbindlichen Unterschrift seine Identität nachweist und seinen ausdrücklichen Willen erklärt, die Dienstleistung in Anspruch zu nehmen. Will die Verwaltung Dienstleistungen in elektronischer Form anbieten, ist ein elektronisches Pendant zur eigenhändigen Unterschrift erforderlich. Diesem Zweck dient die elektronische Signatur. Die technischen Details zur Ausgestaltung elektronischer Signaturen regelt das Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG). Die Vorgaben werden durch die Signaturverordnung (SigV) konkretisiert. Den weiteren rechtlichen Rahmen für den Einsatz der elektronischen Signatur habe ich bereits in meinem Fünften Tätigkeitsbericht unter Punkt 3.17.2 erläutert.

Das Signaturgesetz sieht drei Arten elektronischer Signaturen vor, die sich durch ihre Beweiskraft und die jeweils erforderlichen Sicherheitsanforderungen unterscheiden:

- Unter der (einfachen) elektronischen Signatur versteht das SigG „...Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen“. Diese recht niedrigen Anforderungen wären beispielsweise schon dann erfüllt, wenn einem elektronischen Dokument die eingescannte Unterschrift des Verfassers beigefügt wird. Solche Signaturen sind freilich nicht gegen Fälschungen geschützt und haben daher einen sehr geringen Beweiswert.

- Etwas höheren Sicherheitsanforderungen genügt die fortgeschrittene elektronische Signatur. Einerseits ist mit ihr die Identität des Unterzeichners prüfbar. Andererseits lässt sich feststellen, ob das unterschriebene Dokument nachträglich verändert wurde. Um diese Art der elektronischen Unterschrift zu leisten, benötigt der Unterschreibende in der Regel eine spezielle Software, wie sie beispielsweise bei der elektronischen Steuererklärung genutzt wird.

- Erst die qualifizierte elektronische Signatur erfüllt die Voraussetzungen, um als rechtsverbindliche Unterschrift anerkannt zu werden. Die Erzeugung dieser Signatur muss den besonders hohen, im SigG beschriebenen Sicherheitsanforderungen genügen. Neben der entsprechenden Software sind Speichermedien erforderlich, in denen der geheime Signaturschlüssel des Nutzers abgelegt wird (in der Regel Chipkarten). In einem so genannten qualifizierten Zertifikat wird dieser Signaturschlüssel dem Eigentümer eineindeutig zugeordnet und die Identität des Signaturschlüssel-Inhabers bestätigt. Die Anbieter der Zertifizierungsdienste, die für qualifizierte elektronische Signaturen erforderlich sind, können sich von der Regulierungsbehörde für Telekommunikation und Post (RegTP) akkreditieren lassen. Dazu wird geprüft, ob die Anbieter alle Anforderungen des SigG und der SigV erfüllen. Die daraus resultierende qualifizierte elektronische Signatur mit Anbieterakkreditierung ist ein Sonderfall der qualifizierten elektronischen Signatur, der die höchsten Sicherheitsanforderungen erfüllt. Die zugehörigen Zertifikate müssen beispielsweise noch 30 Jahre nach Ablauf der Gültigkeit online prüfbar sein.

Die elektronische Signatur ist eine besonders wichtige technisch-organisatorische Maßnahme, um sicherzustellen, dass elektronische Daten vom richtigen Absender kommen (Authentizität) und während der Übermittlung nicht verändert wurden (Integrität). Sie ist daher eine Basiskomponente für den elektronischen Rechts- und Geschäftsverkehr, ins-

besondere in E-Government-Anwendungen (siehe dazu auch Punkt 2.16.4). Da der technische Aufwand zur Erzeugung von qualifizierten elektronischen Signaturen höher ist als bei den technisch weniger anspruchsvollen Signaturarten, besteht insbesondere in der öffentlichen Verwaltung die Tendenz, sich auch bei der Verarbeitung besonders schutzbedürftiger Daten lediglich mit der fortgeschrittenen elektronischen Signatur zu begnügen.

Ein Beispiel hierfür ist die Abgabenordnung (AO). § 87a Abs. 3 AO legt fest, dass die für Anträge, Erklärungen oder Mitteilungen an die Finanzbehörden angeordnete Schriftform in bestimmten Fällen durch die elektronische Form ersetzt werden kann. In diesen Fällen ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur zu versehen. Die Übermittlungsvorschriften der AO werden unter anderem in der Steuerdaten-Übermittlungsverordnung (StDÜV) konkretisiert. Sie regelt die elektronische Übermittlung der für das Besteuerungsverfahren erforderlichen Daten, etwa Steuererklärungen oder Freistellungsaufträge. Für den Geltungsbereich der StDÜV lässt § 87a Abs. 6 AO zu, bis zum 31. Dezember 2005 lediglich eine so genannte qualifizierte elektronische Signatur mit Einschränkungen zu verwenden. Dabei handelt es sich aber keinesfalls um eine qualifizierte elektronische Signatur, wie zunächst vermutet werden könnte. Tatsächlich führen diese Einschränkungen dazu, dass lediglich das Sicherheitsniveau einer fortgeschrittenen elektronischen Signatur erreicht wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat diese Übergangsregelung in einer Entschließung vom März 2003 kritisiert (siehe Anlage 15). Die Datenschutzbeauftragten befürchten, dass für die Anwender die Transparenz beim Umgang mit elektronischen Signaturen verloren geht, wenn neben den im SigG festgelegten weitere Signaturverfahren mit geringerer Sicherheit geschaffen werden. Der sichere und verlässliche elektronische Rechts- und Geschäftsverkehr könnte dadurch in Frage gestellt werden. Die Konferenz spricht sich deshalb dafür aus, dass die Finanzbehörden Steuerbescheide und sonstige Dokumente ausschließlich qualifiziert signiert versenden und unterschiedliche Qualitäten und Anwendungsverfahren für elektronische Unterschriften vermeiden. Sie fordert die Bundesregierung auf, solche E-Government-Projekte zu fördern, die qualifizierte elektronische Signaturen einsetzen.

Die Gesellschaft für Informatik e. V. (GI) vertritt in ihrem Memorandum zur Förderung des elektronischen Rechts- und Geschäftsverkehrs vom 3. April 2003 eine vergleichbare Auffassung. Sie fordert, für alle gesellschaftlichen und wirtschaftlichen Bereiche eine einheitliche bundesweite Infrastruktur für **eine** elektronische Signatur bereitzustellen. In Frage kommt nach Auffassung der GI nur die qualifizierte elektronische Signatur mit Anbieterakkreditierung, „...weil nur sie für alle Anwendungen rechtlich zulässig ist, die für

alle Anwendungen ausreichende nachgewiesene Sicherheit nach dem Stand der Technik aufweist und die für viele Anwendungen geforderte langfristige Prüfbarkeit bietet."

Diese Empfehlung gilt uneingeschränkt auch für E-Government-Projekte in unserem Land. Die elektronische Signatur spielt in der E-Government-Strategie der Landesregierung eine zentrale Rolle (siehe Punkt 2.16.4). Signaturverfahren werden jedoch von Bürgern und Mitarbeitern der Verwaltung nur dann akzeptiert, wenn sie einem hohen Sicherheitsstandard genügen und einfach bedienbar sind. Der Akzeptanz dieser modernen und datenschutzfreundlichen Technologie wäre es sicher nicht dienlich, wenn der Anwender aus vielen unterschiedlichen Signaturarten die für jede Anwendung passende erst heraussuchen müsste. Deshalb sollte vorzugsweise die qualifizierte elektronische Signatur genutzt werden.

2.16.4 E-Government im Land

Ende November 2003 hat eine interministerielle Arbeitsgruppe das Arbeitspapier „E-Government in Mecklenburg-Vorpommern" vorgelegt. Der so genannte Masterplan beschreibt die Strategie der Landesregierung zur Modernisierung der öffentlichen Verwaltung. Geplant ist, möglichst viele Verwaltungsleistungen online so bereitzustellen, dass sie der Bürger auch in den Kommunen nutzen kann. Um den Anforderungen insbesondere bei ressortübergreifenden Themen gerecht zu werden, müssen große Teile der Landesverwaltung neu organisiert und der IT-Einsatz neu geregelt werden. Der Masterplan enthält dazu Grundsätze für die Organisation, das IT-Controlling, die Weiterentwicklung der IT-Infrastruktur, die Standardisierung, die Planung und die Mittelbewirtschaftung. Das Papier bezieht sich zwar in erster Linie auf Dienstleistungen der Landesverwaltung, schließt jedoch den Nutzen für die kommunale Ebene nicht aus.

Der Masterplan benennt 75 potentielle E-Government-Projekte, welche die Effizienz der Verwaltung steigern, die behördenübergreifende Information und Kommunikation verbessern und den Kundenkontakt vereinfachen sollen. Als wesentliche Voraussetzung hierfür werden so genannte Basiskomponenten gefordert, beispielsweise Verschlüsselungs- und Signaturverfahren, die elektronische Schriftgutverwaltung, die virtuelle Poststelle oder elektronische Bezahlsysteme. Wichtige ressortübergreifende Projekte sind unter anderem ein zentrales Personaldaten-Verwaltungssystem, der Datenaustausch zwischen polizeilicher Vorgangsbearbeitung und staatsanwaltschaftlicher Datenverarbeitung sowie ein so genanntes DataWarehouse Land, in dem eine autorisierte Datenbasis, zum Beispiel Finanz-, Wirtschafts-, Arbeitsmarkt- und demographische Daten, für operative Auswer-

tungen zur Verfügung gestellt wird. Beispiele für ressortspezifische Projekte sind das Auskunftsverfahren zum Elektronischen Grundbuch, die elektronische Melderegisterauskunft für Polizeibehörden, das Schulberichtssystem oder die IT-unterstützte Antragstellung nach dem Bundeserziehungsgeldgesetz.

Die Umsetzung des Masterplanes erfordert neben neuen Organisationsformen auch eine neue Qualität der automatisierten Verarbeitung personenbezogener Daten. Um die Möglichkeiten der elektronischen Information, Kommunikation und Transaktion umfassend zu nutzen, müssen Daten mehr denn je auf zentralen Servern gespeichert und in behördenübergreifenden Netzen verarbeitet werden. Nicht mehr einzelfallbezogen angelegte Aktenstücke bestimmen dann die Struktur der Datenhaltung, sondern zentrale oder verteilte Datenbestände, auf die unterschiedliche Stellen zugreifen können. Ob Daten zweckgebunden genutzt werden und ob auch bei der elektronischen Datenverarbeitung die Trennung zwischen Legislative, Exekutive und Judikative erhalten bleibt, wäre nicht mehr ohne weiteres offensichtlich und nachvollziehbar. Denn es würde prinzipiell möglich, alle Daten über den Einzelnen auf den berühmten Knopfdruck hin an beliebiger Stelle für beliebige Zwecke zusammenzuführen.

Aber auch unter den Bedingungen des E-Government muss sichergestellt sein, dass jeder selbst bestimmen kann, wer was wann bei welcher Gelegenheit über ihn weiß. Mehr denn je hat diese grundlegende Forderung aus dem Volkszählungsurteil des Bundesverfassungsgerichts ihre Gültigkeit und Berechtigung. Um Risiken für das Recht auf informationelle Selbstbestimmung zu minimieren, sind neue Konzepte für Datenschutz und Datensicherheit erforderlich. Unter anderem vor diesem Hintergrund hat unser Gesetzgeber gefordert, den Landesbeauftragten für den Datenschutz „... über Verfahrensentwicklungen im Zusammenhang mit der automatisierten Verarbeitung personenbezogener Daten rechtzeitig und umfassend zu informieren“ (§ 33 Abs. 5 DSG M-V). Ich halte es für sehr bedenklich, dass ausgerechnet die Landesregierung dieser Verpflichtung bei einem so bedeutenden Projekt bisher nicht nachgekommen ist.

Völlig unerklärlich ist, dass datenschutzrechtliche Fragen im Masterplan bisher nur eine untergeordnete Rolle spielen. Auf Seite 37 wird lediglich darauf hingewiesen, dass sich das so genannte strategische IT-Controlling auch auf den Datenschutz beziehen muss. Einige Seiten danach wird wenigstens der Schutz der Persönlichkeitsrechte von Mitarbeitern der Verwaltung gefordert. Schließlich wird empfohlen, Fragen der IT-Sicherheit und des Datenschutzes in die Fortbildung der Mitarbeiter einzubeziehen. Neben diesen Selbstverständlichkeiten bleibt das Recht des Bürgers auf sorgsamen Umgang mit seinen Daten völlig unerwähnt. Ausdrücklich zu begrüßen ist jedoch, dass Verschlüsselung und elek-

tronische Signatur wesentliche Basiskomponenten für die elektronische Abwicklung der Geschäftsprozesse der Verwaltung sein sollen.

Bei den weiteren Planungen zur Modernisierung der öffentlichen Verwaltung unseres Landes sollte den datenschutzrechtlichen Aspekten die erforderliche Aufmerksamkeit gewidmet werden. Hinweise zur datenschutzgerechten Ausgestaltung von E-Government-Projekten sind unter Punkt 2.16.2 zu finden. Bereits in meinem Fünften Tätigkeitsbericht habe ich im Abschnitt 3.17 detaillierte Empfehlungen zu rechtlichen und technischen Datenschutzfragen bei derartigen Vorhaben gegeben. Ich erkläre nochmals ausdrücklich meine Bereitschaft, die Modernisierung der Verwaltung datenschutzrechtlich zu begleiten.

2.17 Internetnutzung in der öffentlichen Verwaltung

2.17.1 Sichere Internetnutzung durch die Landesregierung

Im Berichtszeitraum kontrollierten meine Mitarbeiter die sicherheitstechnischen und datenschutzrechtlichen Aspekte der Internetzugänge aller Landesministerien. Ziel dieser Kontrollen, die sich auch auf die Kommunikation mit den nachgeordneten Bereichen erstreckte, war es festzustellen, ob ausreichende Maßnahmen zum Schutz personenbezogener Daten getroffen wurden. Es wurde auch geprüft, ob sich aus der Zusammenarbeit der Ministerien auf diesen Gebieten Synergieeffekte zur Verbesserung des Datenschutzes ergeben können.

Alle Ministerien nutzen zur Datenkommunikation mit Behörden in ihrem Zuständigkeitsbereich sowie mit den anderen Ressorts das Landesdatennetz (Corporate Network der Landesregierung – CN; siehe Fünfter Tätigkeitsbericht, Punkt 3.18.1). Bis auf das Ministerium für Bildung, Wissenschaft und Kultur sind alle Ressorts über die zentralen Sicherheitseinrichtungen des Corporate Network (z. B. Firewall und Viruswall) an das Internet angeschlossen (zur Prüfung des Ministerium für Bildung, Wissenschaft und Kultur siehe Fünfter Tätigkeitsbericht, Punkt 3.14.1).

Die Kontrollen haben gezeigt, dass die IT-Verantwortlichen in den Ministerien für die Gefahren sensibilisiert sind, die sich aus der Kopplung der Netze ihres Bereiches mit dem Internet ergeben. In allen Ressorts war ein ausreichender Grundschutz für das hauseigene Netz realisiert. Darüber hinaus waren in jedem Ressort Lösungen zu finden, die zumindest bestimmte Teilaspekte der IT-Sicherheit mustergültig behandeln. Die jeweiligen Maßnahmen unterschieden sich jedoch beträchtlich, wie die folgenden Beispiele belegen:

So schreibt beispielsweise § 22 Abs. 5 DSG M-V für jedes automatisierte Verfahren zur Verarbeitung personenbezogener Daten ein Sicherheitskonzept vor. Darin ist festzulegen, welche technischen und organisatorischen Maßnahmen zum Schutz der Daten zu treffen sind. Das Justizministerium verfügt beispielsweise über ein sehr gutes Sicherheitskonzept. Es ist umfassend, übersichtlich aufgebaut und spiegelt auch den Umsetzungsstand der darin beschriebenen Maßnahmen wider. Auch die Sicherheitskonzepte des Wirtschafts- und des Finanzministeriums sind positiv zu erwähnen. Es gab jedoch auch Konzepte, die nicht dem Stand der Technik entsprachen. So wurden in einigen Fällen nur die Sicherheitsziele beschrieben und die einzelnen Sicherheitsmaßnahmen lediglich sehr grob umrissen dargestellt.

Sicherheitskonzepte sind in erster Linie Arbeitsmittel für diejenigen, die für IT-Sicherheit und Datenschutz zuständig sind. Wenn dieses Werkzeug nicht die erforderliche Qualität aufweist, können Sicherheitslücken in den eigenen IT-Systemen leicht übersehen werden. In einem Fall führten Mängel im Sicherheitskonzept beispielsweise dazu, dass der Überblick über die Netzstruktur und die vereinbarten Sicherheitsmaßnahmen fehlte. Normalerweise nutzt jedes Ressort, wenn es mit einer anderen Behörde kommunizieren will, die zentrale Firewall des CN. Dies gilt auch für die Kommunikation zwischen den Ministerien. Auf diese Weise können die verschiedenen Sicherheitsanforderungen der Ministerien erfüllt werden und eventuelle Störungen bleiben auf jeweils ein Teilnetz beschränkt. In dem besagten Fall muss eine Behörde mit zwei Ministerien elektronisch kommunizieren können. Nach den oben genannten Grundsätzen müsste die Verbindung über eine Firewall geführt werden. Da in einem der beteiligten Ressorts aber der Überblick über die Netzstruktur und die vereinbarten Sicherheitsmaßnahmen fehlte, wurde eine direkte Verbindung ohne Filtermechanismen geschaffen, was zu erheblichen Sicherheitsrisiken führt.

In einem anderen Fall führte ein ungenügendes Sicherheitskonzept dazu, dass erhebliche Sicherheitslücken entstanden, weil versehentlich aktive Inhalte wie Java, JavaScript und ActiveX genutzt werden konnten. Bei ordnungsgemäßer Arbeit mit einem Sicherheitskonzept hätte dies auffallen müssen, da die genannten Inhalte weder an der zentralen noch an der eigenen Firewall oder an den Arbeitsplätzen abgeschaltet beziehungsweise gefiltert wurden.

Sicherheitskonzepte können ihre Wirksamkeit nur dann vollständig entfalten, wenn sie in einen Sicherheitsprozess eingebunden werden. Zu einem solchen Prozess gehört unter anderem, dass geplante Sicherheitsmaßnahmen vollständig realisiert werden, die Wirksamkeit dieser Maßnahmen regelmäßig geprüft wird und Schwachstellen umgehend beseitigt werden. Ein Beispiel für die vorbildliche Etablierung dieses Sicherheitsprozesses liefert das Finanzministerium. Weil Durchsetzung und Kontrolle von Sicherheitsmaßnahmen immer auch eine Aufgabe der Hausleitung sein müssen, ist im Finanzministerium auch die Hausspitze in diesen Prozess eingebunden.

Revisionsfähigkeit von Datenverarbeitungssystemen ist eine zentrale Forderung des Landesdatenschutzgesetzes (§ 21 Abs. 2 Nr. 5). In Revisionen sollten auch externe Prüfer einbezogen werden, da sie mitunter auch solche Schwachstellen finden, die das hauseigene Personal aufgrund von Gewöhnungseffekten nicht mehr bemerkt. Außerdem kann man auf diese Weise externes Know-how nutzbar machen, das in der eigenen Behörde nicht immer vorhanden ist. Bei den Kontrollen war festzustellen, dass externe Revisionen bis-

her nur in einigen Ressorts stattgefunden haben. Ein positives Beispiel hierfür ist das Landwirtschaftsministerium, in dem regelmäßig externe Prüfer tätig sind. Allerdings müssen die Ergebnisse von Revisionen auch Eingang in den IT-Sicherheitsprozess finden. Ich habe bei meinen Prüfungen in mehreren Fällen IT-Sicherheitsprobleme gefunden, die andere externe Prüfer bereits vor geraumer Zeit nachgewiesen hatten.

Um die Verfügbarkeit personenbezogener Daten sicherzustellen (§ 21 Abs. 2 Nr. 3 DSG M-V), sollten sich alle IT-Verantwortlichen intensiv mit Fragen der Datensicherung und -wiederherstellung befassen. Schon bei Einzelplatzrechnern oder Netzen mit sehr wenig Arbeitsstationen kann es erforderlich sein, hierfür geeignete Notfallpläne zu entwickeln und zu trainieren. Auch in diesem Punkt war die Spannbreite der Qualität der vorliegenden Dokumente sehr groß. Ein sauber aufgebautes und regelmäßig gepflegtes Notfallkonzept war beispielsweise im Umweltministerium zu finden.

Alles in allem ist der Schutzbedarf der in den einzelnen Ministerien verarbeiteten Daten sehr ähnlich. Bei den meisten Anwendungen ist von einem mittleren Schutzbedarf auszugehen. Alle Ressorts nutzen jedoch auch einige Anwendungen mit höheren Sicherheitsanforderungen, beispielsweise die Personaldatenverarbeitung oder andere ressortspezifische Fachverfahren. Da offenbar im gesamten Bereich der Landesregierung größtenteils gleiche technische und organisatorische Maßnahmen erforderlich sind, sehe ich erhebliche Synergieeffekte, die zu einem weitgehend einheitlichen Datenschutz- und IT-Sicherheitsniveau in der gesamten Landesverwaltung führen können und darüber hinaus ein erhebliches Einsparungspotential in sich bergen. In folgenden Bereichen sollten meines Erachtens die Möglichkeiten der ressortübergreifenden Koordinierung besser genutzt werden:

- Zu einem weitgehend einheitlichen Datenschutzniveau bei der Nutzung von Internetdiensten im gesamten Bereich der Landesregierung führt insbesondere die Angleichung der (schon) vorhandenen beziehungsweise die Erarbeitung vergleichbarer Regelungen in allen Ressorts. Deshalb habe ich der Landeskoordinierungsstelle für Informations- und Kommunikationstechnik (LKSt) empfohlen, die im Amtsblatt M-V 2000 S. 1090 veröffentlichten „Empfehlungen zur Nutzung der elektronischen Post in den Ministerien und der Staatskanzlei des Landes Mecklenburg-Vorpommern“ zu überarbeiten und sie allen Ressorts als Basis für einheitliche Regelungen zur Verfügung zu stellen. Als Muster sollte die Dienstvereinbarung dienen, die das Sozialministerium in enger Zusammenarbeit mit mir erarbeitet hat. Diese Musterdienstvereinbarung ist in meinem Internetangebot unter http://www.lfd.m-v.de/musterve/mdv_intn.html zu finden.

- Wegen der vergleichbaren Sicherheitsanforderungen müssten die Sicherheitskonzepte der Ressorts sehr ähnlich aufgebaut sein. Es bietet sich deshalb an, für den gesamten Bereich der Landesregierung einmalig ein einheitliches Sicherheitsrahmenkonzept zu erstellen. Ressortspezifische Besonderheiten könnten dieses Rahmenkonzept ergänzen, so dass jedes Ressort seinen Sicherheitsbedarf beschreiben kann.

- Mit der Bildung einer ressortübergreifenden Arbeitsgruppe zur regelmäßigen Prüfung der Landesfirewall ist bereits ein erster Schritt zur Zentralisierung von Revisionsaufgaben gemacht worden. Meines Erachtens ist es sinnvoll, diese Arbeitsgruppe auch mit weiteren ressortübergreifenden Revisionsaufgaben zu beauftragen.

Dieser Aufgaben sollte sich die LKSt oder das nach dem Masterplan E-Government im Innenministerium neu zu schaffende Referat „IT in der Landesverwaltung“ kurzfristig annehmen.

2.17.2 Pilotversuch für sichere E-Mail in der Landesregierung

Im November 2001 beschloss der interministerielle Ausschuss für Informations- und Kommunikationstechnik (IMA-IT), Verschlüsselungs- und Signaturverfahren zu testen, die gewährleisten sollen, dass vertrauliche Daten auch dann ausreichend geschützt sind, wenn sie innerhalb der Landesverwaltung per E-Mail übermittelt werden (siehe Fünfter Tätigkeitsbericht, Punkt 3.17.3). Im Jahre 2002 führte die Landeskoordinierungsstelle Informations- und Kommunikationstechnik (LKSt) einen entsprechenden Pilotversuch durch. Am Test beteiligten sich acht Ressorts sowie einige Firmen als Technologielieferanten und Dienstleister.

Während des Versuches wurde festgestellt, dass die getesteten Produkte prinzipiell in der Landesverwaltung eingesetzt werden können. Es traten nur noch kleinere Schwierigkeiten auf, welche die Projektgruppe durchweg als technisch lösbar eingestuft hat. So konnten beispielsweise nicht alle Programme mit allen Schlüsselzertifikaten arbeiten, und es gab mitunter Installationsfehler.

Um digitale Signatur und Verschlüsselung in der Landesverwaltung einzuführen, sind jedoch noch wesentliche organisatorische Fragen zu klären. Hier ist der interministerielle Ausschuss für Organisationsfragen gefordert. Dieser verweist bislang jedoch nur auf ein Papier der Innenministerkonferenz, welches sich in sehr allgemeiner Weise mit dem Thema befasst. Die Ausführungen dieses Papiers sind nicht konkret genug, um festzulegen, wel-

che Art von Signatur jeweils eingesetzt werden soll (siehe Punkt 2.16.3) und welche Arbeitsplätze mit welcher Technik auszurüsten sind.

Neuerdings gewinnen die Ergebnisse des Pilotversuches jedoch offenbar wieder an Bedeutung. Im Masterplan „E-Government in Mecklenburg-Vorpommern“ der Landesregierung (siehe Punkt 2.16.4) werden Signatur und Verschlüsselung als Basiskomponenten für E-Government-Projekte eingestuft. Für das nach diesem Masterplan neu zu bildende Referat „IT in der Landesverwaltung“ im Innenministerium sollte es daher vordringliche Aufgabe sein, die Entwicklung dieser Basiskomponenten voranzutreiben und die dafür erforderlichen technischen und organisatorischen Voraussetzungen zu schaffen.

2.17.3 Sicherheit durch graphische Firewalls

Firewalls sind Systeme aus Hard- und Software, die der Trennung zweier (oder mehrerer) Netze mit unterschiedlichen Sicherheitsanforderungen dienen. Sie filtern die Kommunikation zwischen den Netzen und geben nur die zugelassenen Daten weiter. Unzulässige Kommunikationsversuche werden blockiert, protokolliert und – je nach Schwere des Verstoßes und Ausstattung der Firewall – auch an die Systemadministration gemeldet.

Die Kommunikation in Netzen basiert auf unterschiedlichen technischen Regeln, den so genannten Protokollen. Eine wichtige Rolle beim „Surfen“ im Internet spielen beispielsweise die Protokolle HTTP (Hypertext Transport Protocol) , TCP (Transmission Control Protocol) und IP (Internet Protocol). Mittels HTTP werden verschiedene Arten von Daten transportiert, darunter formatierte Texte, Bilder und Musik, aber auch kleine Programme, zum Beispiel in den Sprachen Java und JavaScript.

Entsprechend vielfältig sind die Angriffsformen. Manche Angriffe basieren auf unzulässigen IP-Adressen, andere auf speziell formatierten Adressen im HTTP, wieder andere auf Manipulationen mit Java- oder JavaScript-Programmen. Mit HTTP können auch mit Viren, Würmern oder anderer schädlicher Software verseuchte Programme und Dokumente übertragen werden.

Klassische Firewalls untersuchen die ein- und ausgehenden Netzwerkpakete und geben die zulässigen Pakete praktisch unverändert an das zu schützende Netz weiter. Daraus resultieren beispielsweise folgende grundlegende Schwächen:

- Wenn man nur nach Protokollen und Verkehrsrichtung filtert, können immer noch die übertragenen Inhalte auf den Clientrechnern zu Schäden führen. Das bekannteste Problem dieser Kategorie ist die Übertragung schädlicher Software wie Viren und Würmer. Selbst wenn die Firewall nach bekannter schädlicher Software sucht, ist kein vollständiger Schutz zu erreichen. Es wird immer eine zeitliche Lücke zwischen dem ersten Auftreten eines schädlichen Programmes und der Verfügbarkeit von Analysemitteln geben. In diesem Zeitraum ist jede klassische Firewall mit Inhaltsfilterung verwundbar.

- Verschlüsselte Datenübertragungen lassen sich an einer Firewall nicht auswerten. In einem verschlüsselten Datenstrom können jedoch unerwünschte Daten wie die oben erwähnten schädlichen Programme enthalten sein.

- Versucht man, den Umfang der Filterung zu erhöhen, steigt damit auch die Komplexität des Firewallsystems. Damit kann dieses System selbst auch mehr sicherheitskritische Fehler enthalten, die zu einer Kompromittierung des Gesamtsystems beitragen können.

- Weil die vom Internet gelieferten Inhalte erst auf den Rechnern der Nutzer interpretiert werden, können Sicherheitslücken in der dort installierten Software trotz der Firewall zu IT-Sicherheitsproblemen führen. In der Vergangenheit haben sich beispielsweise Browser, vor allem der Internet-Explorer, wiederholt als anfällig für diese Art von Bedrohungen erwiesen.

- Auch andere Software, die nicht sofort mit der Internetnutzung in Verbindung gebracht wird, kann die IT-Sicherheit beeinträchtigen. Dazu gehört neben den Betriebssystemen der Clients beispielsweise auch die Office-Software. Die in moderner Office-Software vorhandenen Makrosprachen eignen sich zum Schreiben von Viren, Würmern und Trojanischen Pferden. Deshalb muss die Software aller Clients ständig aktualisiert werden. Dies ist mit hohem Aufwand verbunden.

Das heißt nun aber nicht, dass klassische Firewalls nutzlos wären. Als Mittel des Grundschutzes sind sie nach wie vor unverzichtbar. Die Beratungs- und Kontrollpraxis zeigt jedoch, dass in vielen Fällen zusätzliche Maßnahmen erforderlich sind. Als sehr wirkungsvoll haben sich so genannte graphische Firewalls erwiesen (siehe auch Fünfter Tätigkeitsbericht, Punkt 3.18.4).

Eine graphische Firewall basiert auf einem System aus einer herkömmlichen Firewall, einem speziellen Internet-Zugangsrechner und einer weiteren, sehr einfach aufgebau-

ten Firewall, die den Internet-Zugangsrechner vom zu schützenden Netz abschottet. Auf dem Internet-Zugangsrechner ist eine spezielle Serversoftware installiert, die mit Clientprogrammen aus dem internen Netz ferngesteuert wird. Zwischen Internet-Zugangsrechner und den Clients wird ein einfaches Kommunikationsprotokoll benutzt, welches lediglich Tastatur- und Mauseingaben nach außen und Bildschirmausgaben nach innen transportiert. Damit gelangen keine potentiell gefährlichen Inhalte wie Java-, JavaScript-, Makro- und andere Programme mehr in das interne Netz. Solche Inhalte werden ausschließlich auf dem Internet-Zugangsrechner interpretiert und können nur dort zu Schäden führen. Deshalb sollten dort keine schutzwürdigen Daten verarbeitet werden.

Die Firewall zwischen dem Internet-Zugangsrechner und dem internen Netz kann verhältnismäßig einfach installiert und gepflegt werden, weil sie nur ein einziges Protokoll überwachen muss; überdies brauchen nur ausgehende Verbindungen zugelassen werden. Der Internet-Zugangsrechner sollte zwar regelmäßig gepflegt werden, jedoch sind hier niedrigere Standards als beim internen Netz einzuhalten, da hier nur wenige oder keine schutzwürdigen Daten zu finden sind.

Die äußere Firewall sollte eine dem Stand der Technik entsprechende Firewall mit Filterung auf der Anwendungsebene (Application Level Gateway) oder einer vergleichbaren Technik sein. Der Betrieb eines solchen Systems kann jedoch auch einem Dienstleister übertragen werden.

Graphische Firewalls lassen sich auf der Basis verschiedener Software einrichten. In meiner Behörde betreibe ich ein solches System mit Linux und einem so genannten VNC-Server auf dem Internet-Zugangsrechner (VNC = Virtual Network Computing). Nutzerakzeptanz und Sicherheitsniveau dieser Lösung sind recht hoch; der Pflegeaufwand ist relativ niedrig, insbesondere verglichen mit dem einer klassischen Firewall.

Von diesen Vorteilen konnte ich mittlerweile mehrere Behörden überzeugen. Einige testen diese Technik bereits oder haben Pilotversuche geplant.

2.17.4 Schulen am Netz

An immer mehr Schulen nutzen Lehrer und Schüler das Internet. Sie recherchieren für den Unterricht, erstellen eine Homepage für ihre Schule oder veröffentlichen die Schülerzeitung – die Möglichkeiten sind vielfältig. Im Internet geben sie aber nicht nur persönliche Daten über sich preis, sondern häufig auch über andere Personen. Dabei besteht die Gefahr, dass sich dritte Personen diese Angaben aneignen und missbrauchen.

Unterstützung bei der datenschutzgerechten Nutzung des Internet gibt die Orientierungshilfe „Datenschutz und Internet in der Schule“. Sie veranschaulicht Schulleitern, Lehrern und Schülern zum einen den rechtlichen Rahmen, den sie zu beachten haben, wenn sie in der Schule einen Internetzugang bereitstellen, surfen, mailen, Homepages betreiben oder Internetaktivitäten protokollieren. Zum anderen zeigt sie auf, wie leicht zugänglich und manipulierbar Daten werden, wenn man sie ohne angemessene Sicherheitsvorkehrungen in das Internet einstellt, und welche Gefahren für den eigenen Computer aus dem Internet drohen.

Folgende Themen werden behandelt:

- personenbezogene Daten und Datenschutz
- Voraussetzungen für die Verarbeitung personenbezogener Daten durch die Schule
- Gefährdungen für Daten im Internet und mögliche Schutzmaßnahmen
- Verantwortlichkeit und Nutzerordnung für den Internetzugang in der Schule
- Protokollierung der Internetzugriffe
- Anforderungen an eine datenschutzgerechte Schul-Homepage
- private Nutzung des Internet in der Schule

Die Orientierungshilfe kann kostenlos in meiner Behörde angefordert oder aus meinem Internetangebot unter http://www.lfd.m-v.de/informat/intschul/oh_intsc.pdf heruntergeladen werden.

2.18 Vertrauenswürdige Hard- und Software

2.18.1 Gütesiegel für datenschutzfreundliche Produkte

Ein süddeutsches Softwareunternehmen bietet ein datenschutzrechtlich vorbildliches Verfahren zur Speicherung medizinischer Daten in einem zentralen Archiv an. Im Sommer 2003 erhielt das Produkt ein Datenschutz-Gütesiegel vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein. Damit wird die Datenschutzfreundlichkeit dieses Speicherverfahrens „amtlich dokumentiert". Ich wurde gefragt, ob dieses Siegel auch in Mecklenburg-Vorpommern gültig ist. Die Firma bezog sich dabei auf die Regelung in § 5 Abs. 2 unseres Landesdatenschutzgesetzes, nach der Produkte vorrangig eingesetzt werden sollen, „... deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem Prüfverfahren festgestellt wurde...".

Leider musste ich dem Unternehmen mitteilen, dass das in Schleswig-Holstein vergebene Gütesiegel bei uns bisher nicht anerkannt wird. Die Landesregierung hat bis heute nicht die Rechtsverordnung erlassen, die Inhalt, Ausgestaltung und Berechtigung zur Durchführung eines entsprechenden Prüfverfahrens in unserem Land regeln soll.

Bereits im August 2002 hatte mir das Innenministerium mitgeteilt, dass für diese Verordnung kein dringlicher Bedarf bestehen würde. Ein Jahr später, im Sommer 2003, war die Situation unverändert. Auf meine erneute Frage teilte mir der Innenminister mit, dass er nach wie vor keinen praktischen Bedarf für die Verordnung sähe. Ohnehin solle zunächst das Ergebnis einer Gesetzesfolgenabschätzung der Hochschule Speyer zur entsprechenden Regelung im Bundesdatenschutzgesetz (§ 9a) abgewartet werden. Darüber hinaus würde ein einheitliches Vorgehen in allen Bundesländern angestrebt und daher abgewartet, welche Standards der Bund setzen wird.

Ich halte diese abwartende Haltung für bedenklich. Ein Blick über die Landesgrenzen zeigt sehr deutlich, dass Hersteller von Hard- und Softwareprodukten großes Interesse an der Prüfung ihrer Produkte haben. In Schleswig-Holstein gibt es beispielsweise schon seit Anfang 2002 die Möglichkeit, die Datenschutzfreundlichkeit derartiger Produkte prüfen und durch das oben genannte Gütesiegel bestätigen zu lassen. Viele Hersteller haben mittlerweile erkannt, dass insbesondere Produkte der Informations- und Kommunikationstechnik einen Wettbewerbsvorteil haben, wenn Datenschutz nachweisbar realisiert wurde. Die Liste der Produkte mit dem Gütesiegel aus Schleswig-Holstein wächst daher ständig (siehe auch unter http://www.datenschutzzentrum.de/ guetesiegel/register.htm).

Solange in unserem Land keine entsprechende Verordnung existiert, sind wir in Mecklenburg-Vorpommern vom datenschutzrechtlichen Fortschritt in diesem Bereich abgekoppelt. Wir nutzen nicht die Chance, unsere im Vergleich zu anderen Datenschutzgesetzen fortschrittliche Regelung sowohl in die Verbesserung des technischen Datenschutzes in den öffentlichen Stellen unseres Landes als auch in Impulse für die einheimische Wirtschaft umzusetzen. Wir sind auch nicht in der Lage, Prüfungsverfahren anderer Bundesländer anzuerkennen und somit die Herstellung und Verbreitung datenschutzfreundlicher Produkte voranzutreiben.

Weder die Ergebnisse der oben genannten Studie noch die Aktivitäten des Bundesgesetzgebers lassen inhaltlich Neues erwarten. Schleswig-Holstein verfügt über eine entsprechende Regelung, die sich in der Praxis bewährt hat und daher als Vorbild für eine in unserem Land zu erlassende Verordnung genutzt werden sollte.

2.18.2 Anwender können Datenschutzanforderungen selbst definieren

Seit November 2002 stellt der Bundesbeauftragte für den Datenschutz in seinem Internetangebot ein so genanntes Schutzprofil (Protection Profile) zur Verfügung (http://www.bfd.bund.de/technik/protection_profile.html). In einem Schutzprofil können Nutzer bereits vor der Entwicklung eines IT-Produktes ihre Anforderungen an dessen Funktion und Vertrauenswürdigkeit beschreiben. Sie können somit die eigenen Sicherheitsanforderungen genau definieren. Schutzprofile basieren auf dem Regelwerk der Common Criteria, einem internationalen Standard für die Prüfung und Bewertung der Sicherheit von Informationstechnik. Das fertige Produkt kann daher in einem international anerkannten, förmlichen Verfahren geprüft werden. Die Übereinstimmung zwischen den Sicherheitsanforderungen und den im Produkt tatsächlich vorhandenen Sicherheitsfunktionen wird mit einem weltweit gültigen Zertifikat bestätigt. Somit können weitere potentielle Nutzer des Produktes auf die Qualität und ordnungsgemäße Funktion der Sicherheitsmechanismen vertrauen, ohne dass sie die Details der Umsetzung von Sicherheitsanforderungen kennen müssen.

Ausgangspunkt für die Bereitstellung dieses Schutzprofils war, dass Nutzer moderner IT-Anwendungen kaum noch nachvollziehen können, ob und in welchem Umfang personenbezogene Daten übertragen und gespeichert werden. Mit Hilfe des Schutzprofils können sie bereits vor der Entwicklung eines IT-Produktes im Detail festlegen, welche Informationen unter welchen Voraussetzungen zwischen welchen Hardwarekomponenten übermittelt werden dürfen.

Das Schutzprofil geht davon aus, dass mit jeder Lese- oder Schreiboperation und mit jedem Sende- und Empfangsvorgang Informationsflüsse zwischen verschiedenen Datenorten initiiert werden. Der Begriff Datenort steht dabei für alle in der Praxis vorkommenden Addressierungsmöglichkeiten und bezieht sich sowohl auf Adressen lokaler Speichermedien wie Dateien, Laufwerke oder Bildschirme als auch auf E-Mail-Adressen, Datenbanken oder andere entfernte, adressierbare Einheiten. Der künftige Nutzer des zu entwickelnden IT-Systems ordnet jedem Informationsfluss individuelle Sicherheitseigenschaften zu. Für jeden als schutzbedürftig klassifizierten Informationsfluss werden so genannte Informationsflussregeln definiert. Mit diesen Regeln wird vorab festgelegt, ob ein Informationsfluss zulässig ist und wie die Daten dann bei der Übertragung zu schützen sind (z. B. verschlüsseln, signieren, anonymisieren, pseudonymisieren). IT-Produkte, die nach den Vorgaben dieses Schutzprofils entwickelt wurden, können dann anhand dieser Regeln selbst dahin gehend überprüft werden, ob Informationen fließen dürfen und welche Sicherheitsvorkehrungen dabei zu realisieren sind. Mit Blick auf diese Eigenschaften erhielt das Schutzprofil die Bezeichnung „Benutzerbestimmbare Informationsflusskontrolle“.

Für den Datenschutz ist dieses Schutzprofil von besonderer Bedeutung, weil auch datenschutzrelevante Aspekte wie Vertraulichkeit, Integrität und Authentizität in der Sprache der Common Criteria beschrieben werden können. Auch das gesetzlich normierte Gebot der Zweckbindung kann mit dem Konzept des Schutzprofils sehr detailliert umgesetzt werden. Somit lassen sich vielfältige datenschutzrechtliche Anforderungen an IT-Produkte bereits während der Produktentwicklung berücksichtigen.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (siehe Abschnitt 4) hatte bereits im Jahr 2000 begonnen, das oben genannte Schutzprofil zu entwickeln (siehe Fünfter Tätigkeitsbericht, Punkt 3.18.5). Nach Abschluss der vorbereitenden Arbeiten stellte dann das Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI) dieses Schutzprofil im Auftrag des Bundesbeauftragten für den Datenschutz und mit Unterstützung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) fertig. Die Firma T-Systems ISS GmbH prüfte anschließend das Schutzprofil nach den Vorgaben der Common Criteria. Mit der Erteilung des Zertifikates durch das BSI und der Übergabe der Unterlagen an den Bundesbeauftragten im November 2002 steht das Schutzprofil nun allen interessierten Nutzern zur Verfügung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung vom 27./28. März 2003 die Anwendung des Schutzprofils empfohlen, damit auch die Nutzer von Informationstechnik beurteilen können, ob IT-Systeme oder -Pro-

dukte vertrauenswürdig und datenschutzgerecht sind (siehe Anlage 12). Die Datenschutzbeauftragten appellieren an die Hersteller, entsprechende Produkte zu entwickeln beziehungsweise vorhandene Produkte anhand bereits bestehender oder gleichwertiger Schutzprofile zu modifizieren. Sie treten weiterhin dafür ein, dass die öffentliche Verwaltung vorrangig solche Produkte einsetzt.

2.18.3 Sicherheit auf Kosten des Datenschutzes?

Im Herbst 2002 veröffentlichte die Fachpresse Berichte, wonach neuartige Kontrollmöglichkeiten bei Personalcomputern entwickelt werden. Zahlreiche Bürger befürchteten, dass künftig Dritte festlegen und kontrollieren können, welche Hard- und Softwarekomponenten auf Computern benutzt werden dürfen.

Seit Anfang 2002 hatte die Fachpresse regelmäßig über die Aktivitäten einer von der Firma Intel geführten Initiative namhafter Hard- und Softwarehersteller berichtet. Unter dem Namen Trusted Computing Platform Alliance (TCPA) hatten sich etwa 200 Firmen mit dem Ziel zusammengeschlossen, die Spezifikation für einen Sicherheitschip (Trusted Platform Modul – TPM) zu entwickeln. Dieser Chip ergänzt die klassische PC-Architektur und führt zahlreiche Funktionen aus, die das Vertrauen in die Sicherheit des PC stärken sollen (z. B. kryptographische Funktionen, Unterstützung des sicheren Bootens, Initialisierungs- und Management-Funktionen). Für die Nutzung dieser Funktionen ist ein besonderes BIOS und ein Betriebssystem mit speziellen Treibern erforderlich, das über eine kryptographisch gesicherte Schnittstelle (Trusted Platform Support Service – TSS) zum Sicherheitschip verfügt. In diesem Zusammenhang wurde stets das Softwareprojekt Palladium von Microsoft erwähnt, das Basis für die Arbeiten an einem vertrauenswürdigen Betriebssystem sein soll.

Die öffentliche Diskussion um diese Technologien wurde jedoch in vielen Fällen durch spekulative Darstellungen verzerrt. So war zunächst nicht auszuschließen, dass die neuartigen Sicherheitsfunktionen durch lückenlose Kontrolle der Hardware, des Betriebssystems und der Anwendungssoftware erkauft werden sollen und somit Dritte jede Aktivität auf solchen Personalcomputern vollständig überwachen können. Unsicherheiten wurden dadurch geschürt, dass sich selbst renommierte IT-Sicherheitsfachleute mitunter sehr polemisch zu den Plänen der TCPA und der Firma Microsoft äußerten. TPM-Anwendungen wurden zu Unrecht vielfach mit einem datenschutzunfreundlichen System zur Lizenz- und Urheberrechtskontrolle (Digital Rights Management – DRM) gleichgesetzt.

Eine differenziertere Betrachtung zeigte dann jedoch, dass die TCPA-Technologie nicht von vornherein negativ zu bewerten ist, sondern durchaus auch für den Datenschutz Vorteile mit sich bringen kann. So können beispielsweise private Schlüssel und sensitive Daten besser geschützt werden, als durch jedes andere bislang am Markt verfügbare Konzept. Durch die mögliche „Versiegelung“ verschlüsselter Daten (die Entschlüsselung ist nur bei einer vorher definierten Konfiguration möglich) können von außen erfolgende Angriffe auf Personalcomputer besser abgewehrt werden. Die Datensicherheit bei der Nutzung von virtuellen LANs, Fernzugriffsmechanismen und drahtlosen Netzen kann erhöht werden. Die TCPA-Spezifikationen sind zudem unabhängig vom jeweiligen Betriebssystem. Durch TCPA-konforme Technik kann der Wunsch nach einer generellen Verschlüsselung übertragener und gespeicherter Daten leichter umgesetzt werden.

Die Befürchtungen der Kritiker sind allerdings nicht von der Hand zu weisen. Die TCPA-Technologie kann tatsächlich missbräuchlich genutzt werden. So könnte beispielsweise eine Infrastruktur mit externen Kontrollinstanzen aufgebaut werden, mit der die Nutzung von Software und das Abspielen digitalisierter Unterhaltungsmedien lückenlos kontrolliert wird (DRM-Systeme). Welche Rolle dabei das jetzt als „Next-Generation Secure Computing Base“ (NGSCB) bezeichnete Palladium spielen könnte, ist noch unklar. In neueren Veröffentlichungen bestätigt Microsoft den Zusammenhang zwischen solchen Systemen und NGSCB allerdings (http://www.microsoft.com/resources/ngscb/documents/ngscb_tcp.doc). DRM-Systeme werden dort als wichtige Anwendung für NGSCB genannt.

Um die Entwicklungen um TCPA und Palladium aus datenschutzrechtlicher Sicht bewerten zu können, hat der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (siehe Punkt 4) die Datenschutzaspekte der TCPA-Spezifikationen untersucht. Im Ergebnis hat die 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 2003 eine Entschließung verabschiedet (siehe Anlage 11). Sie begrüßt alle Aktivitäten, die der Verbesserung des Datenschutzes dienen und insbesondere zu einer manipulations- und missbrauchssicheren sowie transparenten IT-Infrastruktur führen. Sie erkennt auch die berechtigten Forderungen der Softwarehersteller an, dass kostenpflichtige Software nur nach Bezahlung genutzt werden darf. Die Datenschutzbeauftragten fordern aber die Hersteller von Informations- und Kommunikationstechnik gleichzeitig auf, Hard- und Software so zu entwickeln und herzustellen, dass Anwender die ausschließliche Kontrolle über die von ihnen genutzte Informationstechnik haben, dass alle zur Verfügung stehenden Sicherheitsfunktionen transparent sind und dass die Nutzung von Hard- und Software und der Zugriff auf Dokumente auch weiterhin möglich ist, ohne dass Dritte davon Kenntnis erhalten.

Detaillierte Informationen zu den datenschutztechnischen Aspekten von TCPA und NGSCB/Palladium sind einem Vermerk meines brandenburgischen Kollegen zu entnehmen (www.lda.brandenburg.de/material/tcpa.pdf).

2.18.4 Automatisches Software-Update

Softwarehersteller bieten in zunehmendem Maße an, komplette Softwarepakete oder einzelne Updates auf die Rechner ihrer Kunden im Rahmen so genannter Online-Updates über das Internet zu laden und automatisch zu installieren. Dabei versuchen die Hersteller jedoch immer öfter, unbemerkt auf die Personalcomputer bei Firmen, Behörden und Privatnutzern zuzugreifen, um Konfigurationsdaten – die in der Regel personenbezogene Daten enthalten – auszulesen.

Diese Update-Verfahren sind mit erheblichen Risiken verbunden. Ohne dass der Nutzer dies bemerkt, werden personenbezogene Daten an Softwarehersteller übermittelt, die im derzeit praktizierten Umfang zumindest aus technischen Gründen nicht erforderlich sind. Darüber hinaus bewirken Online-Updates Änderungen an der Software der Zielrechner, die dann meist ohne die erforderlichen Tests und Freigabeverfahren genutzt werden. Ferner ist nicht immer sichergestellt, dass andere Anwendungen problemlos weiter funktionieren. Das – unbemerkte – Update wird dann auch nicht als Fehlerursache erkannt.

Vor dem Hintergrund der zunehmenden Gefahr von Viren und anderer Schadsoftware ist es sehr wichtig, dass die Sicherheit und die Aktualität von System- und Anwendungssoftware stets gewährleistet sind. Dies erfordert in der Tat regelmäßige Updates. Insbesondere privaten Nutzern sollte es aber immer selbst überlassen werden zu entscheiden, ob sie ihre Software automatisch aktualisieren lassen oder ob sie ein Update selbst initiieren möchten. In keinem Fall darf ein Update davon abhängig sein, dass zuvor umfangreiche personenbezogene Daten an den Hersteller übermittelt werden. Anbieter dürfen nur die Konfigurationsdaten erhalten, die für den Update-Vorgang aus technischer Sicht erforderlich sind.

Öffentliche Stellen dürfen Online-Updates in keinem Fall nutzen, um Softwarekomponenten ohne separate Tests und formelle Freigabe auf Produktionssysteme einzuspielen. Denn alle Änderungen an automatisierten Verfahren zur Verarbeitung personenbezogener Daten oder an den zugrunde liegenden Betriebssystemen sind Wartungstätigkeiten im datenschutzrechtlichen Sinn und dürfen daher nur den dazu ausdrücklich ermächtigten Personen möglich sein. Darüber hinaus dürfen personenbezogene Daten von Nutzern nur mit

der ausdrücklichen Zustimmung der für die Daten verantwortlichen Stelle im Zusammenhang mit derartigen Wartungstätigkeiten übermittelt und verarbeitet werden. Die meisten der derzeit angebotenen Verfahren zum automatischen Software-Update werden diesen aus dem Datenschutzrecht folgenden Anforderungen nicht gerecht.

Um die Produktionssysteme immer auf dem aktuellen Softwarestand zu halten, ist es erforderlich, Updates zunächst auf einen unabhängigen Testrechner zu laden. Dort kann die ordnungsgemäße Funktion der Software geprüft werden. Nach erfolgreichem Test sind die neuen Softwarekomponenten freizugeben und dürfen erst dann zur Nutzung in das Produktionssystem überspielt werden.

Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung vom August 2003 auf die Risiken automatischer Software-Updates hingewiesen (siehe Anlage 20). Sie fordern die Softwarehersteller auf,

- überprüfbare, benutzerinitiierte Update-Verfahren bereitzustellen, die nicht zwingend einen Online-Datenaustausch mit dem Zielrechner erfordern,

- auch weiterhin datenträgerbasierte Update-Verfahren anzubieten, bei denen lediglich die für den Datenträgerversand erforderlichen Daten übertragen werden,

- automatisierte Online-Update-Verfahren nur wahlweise anzubieten und vorhandene so zu modifizieren, dass sowohl der Update- als auch der Installationsprozess transparent und revisionssicher sind,

- Software-Updates nicht davon abhängig zu machen, dass Softwareherstellern ein praktisch nicht kontrollierbarer Zugriff auf die Rechner der Nutzer gewährt wird,

- personenbezogene Daten nur dann abzurufen, wenn der Verwendungszweck vollständig bekannt ist und in die Verarbeitung ausdrücklich eingewilligt wurde und

- in jedem Fall das gesetzlich normierte Prinzip der Datensparsamkeit einzuhalten.

In einem Interview zu Fragen der Sicherheit von Rechnern und Netzwerken („Focus“ vom 20. Oktober 2003) hat Bundesinnenminister Otto Schily die Forderungen der Datenschutzbeauftragten aufgegriffen und folgende Anforderungen an Sicherheitslösungen genannt: „Die Anwender müssen selbst entscheiden können, ob sie die neuen Funktionen zur Verbesserung der Computersicherheit nutzen. Ein Sicherheitsmodul muss vollständig deakti-

vierbar und von unabhängigen Institutionen überprüfbar sein. Der Anwender muss die volle Kontrolle über seine Daten behalten. Es versteht sich von selbst, dass keine Daten ohne Wissen des Benutzers ins Internet gesendet werden."

Softwarehersteller sollten die Forderungen von Datenschützern und Politikern aufgreifen und Update-Verfahren anbieten, die den Erfordernissen des Rechts auf informationelle Selbstbestimmung ausreichend Rechnung tragen.

2.18.5 Geschwätzige Drucker

Im April 2003 meldete die Fachpresse (c't 7/2003, DSB 4/2003), dass die Firma Hewlett-Packard (HP) den Datenschutz verletzt habe. Die für HP zuständige Datenschutzaufsichtsbehörde hatte kritisiert, dass einige HP-Drucker automatisch Verbrauchsdaten an einen Server des Herstellers im Ausland für Zwecke der Statistik übermitteln. Mit Hilfe des Software-Tools „myPrintMileage" wurden die Bezeichnung, der Typ und die Seriennummer des Druckers, die Anzahl der Druckjobs und der Seiten, der Typ, die Produktnummer, die Kapazität und der Füllstand der Tintenpatrone sowie weitere technische Informationen übermittelt. Da auch die IP-Adresse des Absenders übermittelt wurde, war es möglich, über die bei der Produktregistrierung erhobenen Daten einen Personenbezug herzustellen. Die nach dem Bundesdatenschutzgesetz erforderliche Einwilligung der Nutzer lag nach der Bewertung der Aufsichtsbehörde nicht vor, weil die entsprechende Zustimmungsklickbox bei der Installation der Druckersoftware an einer für den Nutzer nicht sichtbaren Stelle mit „ja" vorbelegt war. Im Ergebnis war festzustellen, dass auch in diesem Fall (siehe dazu auch Punkt 2.18.4 Automatisches Software-Update) personenbezogene Daten der Nutzer ohne deren Wissen übermittelt wurden.

HP zeigte sich einsichtig und entschuldigte die unzulässige Datenübermittlung mit dem Hinweis, man habe die entsprechenden Regelungen der deutschen Datenschutzbestimmungen übersehen. Die Einwilligungserklärung wurde so geändert, dass der Anwender bewusst der Übermittlung zustimmen muss.

Leider ist der beschriebene Fall kein Einzelfall. Auch andere Druckerhersteller versuchen, sich unbemerkt personenbezogene Daten der Nutzer für verschiedene Zwecke übermitteln zu lassen. Da sie insbesondere mit Tintenpatronen viel Geld verdienen, suchen sie beispielsweise Wege, ihre Produkte möglichst einfach unter´s Volk zu bringen. Etwas „Besonderes" hat sich die Firma Dell einfallen lassen. Die seit Mitte 2003 angebotenen Tintenstrahldrucker werden mit dem so genannten Dell Ink Management System ausge-

stattet. Nach Herstellerangaben dient die intelligente Software im Dell-Druckertreiber zur Überwachung des Druckers und zur Benachrichtigung bei niedrigem Tinten-Füllstand. Dell wirbt mit dem integrierten Online-Einkaufssystem, das eine direkte Verbindung zur Dell-Website für den schnellen, einfachen Tinteneinkauf herstellt und die Lieferung der Tinte direkt an die Haustür ermöglichen soll. Dass auch Dell dabei unbemerkt Konfigurations- und Verbrauchsdaten abruft, erfährt der Kunde nicht ohne weiteres.

Ich halte diese Entwicklung für sehr bedenklich. Sie kann dazu führen, dass für den Anwender nicht mehr nachvollziehbar ist, wer über welche Daten zu seiner Person verfügt und zu welchem Zweck diese verwendet werden. Die im Punkt 2.18.4 genannten Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gelten auch hier uneingeschränkt. Die Hersteller sollten ihre Produkte demnach so ausgestalten, dass die Nutzer die ausschließliche und vollständige Kontrolle über ihre Informationstechnik haben und Zugriffe auf personenbezogene Daten nur nach vorheriger Information und mit Einwilligung in jedem Einzelfall möglich sind. Darüber hinaus müssen sie sicherstellen, dass alle zur Verfügung stehenden Funktionen für Anwender transparent sind und die Nutzung von Hard- und Software auch weiterhin möglich ist, ohne dass Dritte davon Kenntnis erhalten und Nutzungsprofile anlegen können.

2.18.6 Überwacht Windows XP seine Nutzer?

Seit neue Personalcomputer vorzugsweise mit dem Betriebssystem Windows XP von Microsoft ausgestattet werden, haben sich Anfragen besorgter Bürger bei mir gehäuft. Viele befürchten, dass im Zusammenhang mit der so genannten Produktaktivierung des Betriebssystems personenbezogene Daten über das Internet an die Firma Microsoft übermittelt werden.

Microsoft hat in das Betriebssystem Windows XP eine Aktivierungsfunktion integriert. Nach Ablauf einer Testphase wird der Nutzer aufgefordert, die erworbene Software per Telefon oder über das Internet zur weiteren Verwendung freischalten zu lassen. Ohne Freischaltung kann das Betriebssystem nicht weiter genutzt werden. Nach der Freischaltung hat der Nutzer zusätzlich die Möglichkeit, sich als Anwender bei Microsoft registrieren zu lassen, um beispielsweise regelmäßig Produktinformationen zu erhalten.

Nutzer von Windows XP können tatsächlich nicht ohne weiteres nachvollziehen, welche Daten bei der Aktivierung und bei der Registrierung an Microsoft übertragen wurden.

Unter dem Druck der Öffentlichkeit beauftragte die Microsoft Deutschland GmbH daher die TÜV Informationstechnik GmbH aus Essen (TÜViT), die Produktaktivierung zu prüfen. Die Mitarbeiter des TÜViT konnten dazu auf den vollständigen Quellcode von Windows XP zugreifen. Darüber hinaus haben sie das Microsoft Activation Center, das die telefonischen Aktivierungen in Deutschland durchführt, geprüft.

Im Ergebnis hat der TÜViT keine Anhaltspunkte dafür gefunden, dass bei der Aktivierung personenbezogene Daten über das Internet übertragen werden. Microsoft erhält lediglich die so genannte Installations-ID (Produkt-ID und Hardware-ID). Die Aktivierung kann somit als anonym bezeichnet werden. Erst bei der freiwilligen Nutzerregistrierung werden die im Assistenten angegebenen persönlichen Daten übermittelt. Dies gilt entsprechend für die telefonische Registrierung.

Trotz der „Unbedenklichkeits-Bescheinigung“ des TÜViT sind Bedenken berechtigt. Das Betriebssystem verfügt über weitere Funktionen, die zu einer ungewollten Kontaktaufnahme und zur Übermittlung von Daten an Microsoft führen können. Eine dieser Funktionen betrifft das so genannte WindowsUpdate. Bei entsprechender Konfiguration der Einstellungen wird der Rechner automatisch mit aktuellen Software-Updates über das Internet versorgt. Die damit zusammenhängenden Risiken habe ich ausführlich im Punkt 2.18.4 beschrieben. Darüber hinaus hat Microsoft das Betriebssystem mit einer Benachrichtigungs-Komponente versehen, die bei Programmabstürzen versucht, über das Internet eine entsprechende Meldung an Microsoft zu senden. Welche Daten dabei übermittelt werden, hat Microsoft nicht mitgeteilt.

Selbst so scheinbar simple Funktionen wie die interne Uhr des PC werfen Fragen auf. Windows XP verfügt über einen Synchronisationsmechanismus, mit dem die interne Uhr automatisch über eine Internetverbindung zu Microsoft abgeglichen wird. Auch hier ist nicht transparent, ob bei dieser Synchronisation weitere Daten übermittelt werden.

Ein letztes Beispiel soll verdeutlichen, wie intensiv Windows XP versucht, „nach Hause zu telefonieren“. Der Windows XP Media Player, eine Standardkomponente des Betriebssystems zur Wiedergabe von Musik oder Videos auf dem PC, ist bei der Auslieferung so eingestellt, dass er automatisch Verbindung zu Microsoft aufnimmt. Beim Abspielen von Audio-CDs oder DVDs wird versucht, den Kontakt zu einem Microsoft-Server herzustellen. Die Software fragt eine Datenbank ab, damit der Media Player Künstler und Titel automatisch korrekt anzeigen kann. Der Verdacht, dass auch dabei personenbezogene Daten der Nutzer übermittelt werden, ist bis heute nicht vollständig ausgeräumt.

Ob Funktionen, die automatisch eine Internetverbindung zu Microsoft herstellen, tatsächlich genutzt werden, hängt maßgeblich von der Konfiguration der entsprechenden Parameter des Betriebssystems ab. So ist es durchaus möglich, das automatische Update zu unterbinden, indem der entsprechende Haken auf der zuständigen Registerkarte entfernt wird. Auch die automatische Fehlerbenachrichtigung kann unterbunden werden. Der Nutzer muss „nur“ mit der rechten Maustaste auf „Arbeitsplatz/Eigenschaften“ klicken und die Registerkarte „Systemeigenschaften“ öffnen, im folgenden Register „Erweitert“ die Schaltfläche „Fehlerberichterstattung“ drücken und die Option „Fehlerberichterstattung deaktivieren“ aktivieren. Ähnlich „einfach“ sind auch andere Funktionen auszuschalten.

Hinweise zum datenschutzgerechten Umgang mit diesem neuen Betriebssystem gibt die Orientierungshilfe „Datenschutz bei Windows XP Professional“. Die Empfehlungen sind auf die Professional-Version der Software ausgerichtet, weil diese gegenüber der Home-Version zusätzliche datenschutzrelevante Funktionen enthält.

Neben einem kurzen Vergleich der Vor- und Nachteile des neuen Betriebssystems beschreibt die Orientierungshilfe detailliert, welche Einstellungen gewählt werden sollten, um die oben genannten Risiken zu minimieren. Darüber hinaus gibt sie Hinweise zur Installation und erläutert Sicherheitsaspekte bei der Einbindung von XP-Computern in Netzwerke. Auch weitere Komponenten des Betriebssystems wie Verschlüsselung (Encrypting File System EFS), Systemwiederherstellung (Automated System Recovery ASR) oder Verzeichnisdienst (Active Directory) werden aus datenschutzrechtlicher Sicht beleuchtet. Ein Kapitel mit Sicherheitsempfehlungen, die Voraussetzung für den datenschutzgerechten Einsatz von Windows XP sind, rundet den Inhalt ab.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (siehe Punkt 4) hat über diese Orientierungshilfe beraten und sie zustimmend zur Kenntnis genommen. Sie kann kostenlos aus meinem Internetangebot unter http://www.lfd.m-v.de/informat/dsbeiwxp/oh_wxp.pdf heruntergeladen werden.

2.18.7 Datensicherheit und USB

Seit einiger Zeit werden Personal Computer mit Buchsen für den Universal Serial Bus (USB) ausgestattet. Diese Schnittstellen dienen dem einfachen Anschluss verschiedener Hardwarekomponenten wie Disketten-, DVD- oder CD-ROM-Laufwerken, handlichen Festspeichermedien (so genannte memory sticks) oder Netzwerkhardware. Aufwändige

Installationsprozeduren für Hard- und Software entfallen, da moderne Betriebssysteme die neu angeschlossenen Geräte sofort erkennen und einbinden. Auch wenig qualifizierte Nutzer sind somit in der Lage, Hard- oder Softwarekomponenten in Betrieb zu nehmen. Dabei besteht die Gefahr, dass diese Komponenten ohne die in allen Behörden erforderliche Freigabe nach § 19 Abs. 1 DSG M-V genutzt werden.

Um zu verhindern, dass nicht freigegebene Technik angeschlossen wird und diese neuen Schnittstellen für unzulässige Datenübermittlungen oder für das Einspielen nicht zugelassener Software genutzt werden, muss der Zugriff auf den USB durch technische Maßnahmen ausschließlich auf zugelassene Geräte beschränkt werden. Die bisher empfohlenen Nutzungsbeschränkungen für CD- und Floppy-Laufwerke reichen nicht mehr aus.

Es hat sich allerdings gezeigt, dass Zugriffssperren für USB-Geräte nicht ganz einfach einzurichten sind. Die Entwickler von Betriebssystemen haben oft mehr auf die Funktion der Geräte als auf ausreichenden Zugriffsschutz geachtet. Um insbesondere Administratoren bei der Auswahl und Konfiguration der Zugriffssperren zu unterstützen, hat der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (siehe Punkt 4) die Orientierungshilfe „Datensicherheit bei USB-Geräten“ mit entsprechenden Empfehlungen erarbeitet. Sie bezieht sich auf die Betriebssysteme Windows 2000 und XP sowie Linux.

Unter Windows sind kommerzielle Programme empfehlenswert, mit denen Administratoren die Zugriffsrechte auf USB-Geräte ändern können. Darüber hinaus können Systemverantwortliche auch selbst entsprechende Scripte (kleine Programme, die Administratoren zur Steuerung des Betriebssystems nutzen) schreiben. In der Fachliteratur sind verschiedene Möglichkeiten erläutert.

Bei Linux müssen Administratoren hingegen die Konfiguration der USB-Software anpassen und die Zugriffsrechte der USB-Geräte mit Linux-Bordmitteln überprüfen. Die Orientierungshilfe enthält dazu einige Hinweise. Sie kann von meinem Internetangebot unter http://www.lfd.m-v.de/informat/usb/oh_dsusb.html abgerufen werden.

2.18.8 Drahtlose lokale Netze – immer noch nicht zu empfehlen

Drahtlose lokale Netze nach der Norm IEEE 802.11b (wireless LAN – WLAN) erfreuen sich wachsender Beliebtheit – auch im öffentlichen Bereich. Die Komponenten zum Aufbau solcher Netze sind mittlerweile sehr preisgünstig, und die Hersteller versprechen eine

Übertragungssicherheit, die der drahtgebundener Netze entsprechen soll. Darüber hinaus entfällt die mitunter aufwändige und teuere Verkabelung.

Die Nutzer solcher Netze sollten jedoch Folgendes beachten:

- Die Ausbreitung der Funkwellen lässt sich nur schwer begrenzen. Ohne zusätzliche Schutzmaßnahmen kann der Datenverkehr von Funknetzen daher häufig mit einfachen Mitteln abgehört werden.

- Verfügen Unbefugte über die gleiche Netzwerktechnik, können auch sie am Funkverkehr teilnehmen; berechtigte Teilnehmer müssen also auf geeignete Weise identifiziert werden können.

- Funknetze können verhältnismäßig einfach gestört werden, beispielsweise durch andere Funknetze derselben Norm.

- Der Standort der Teilnehmer ist durch Peilung feststellbar. Somit können prinzipiell Bewegungsprofile erstellt werden.

Nach wie vor können datenschutztechnische Grundanforderungen (Sicherung der Vertraulichkeit, der Integrität und der Verfügbarkeit – § 21 Abs. 2 Nr.1, 2 und 3 DSG M-V) mit den von den Herstellern implementierten Mitteln nicht ausreichend erfüllt werden. Das durch den entsprechenden Standard definierte Sicherheitsniveau hat sich gegenüber dem im letzten Bericht geschilderten Niveau (siehe Fünfter Tätigkeitsbericht, Punkt 3.18.7) nicht verändert. Die von einigen Herstellern zusätzlich implementierten Sicherheitsmaßnahmen bieten keine wesentlichen Verbesserungen. Im Einzelnen stellen die Standards folgende Mechanismen zur Verfügung:

- Das implementierte Verschlüsselungsverfahren WEP (wired equivalent privacy) beruht vor allem auf einem Verschlüsselungsverfahren mit einer effektiven Schlüssellänge von 40 oder 104 Bits. 40 Bit lange Schlüssel sollten nach dem heutigen Stand der Technik überhaupt nicht mehr verwendet werden, da mit handelsüblichen Rechnern sämtliche möglichen Schlüssel innerhalb kurzer Zeit ausprobiert werden können („brute force“ – Angriffe mit roher Gewalt). Beide Varianten weisen zusätzlich gravierende kryptographische Mängel auf (Einzelheiten habe ich bereits im Fünften Tätigkeitsbericht, Punkt 3.18.7, beschrieben). Dies führt dazu, dass Unbefugte mit handelsüblichen Netzwerkkarten und teilweise kostenlos im Internet verfügbarer Software die verwendeten Schlüssel bestimmen können, indem sie den Netzwerkverkehr abhören.

- Die Netzwerknamen (hier SSID – service set identifier) lassen sich angeblich vor Unbefugten verbergen. Dieses Mittel ist jedoch weitgehend wirkungslos, da die SSID trotz eingeschalteter Verschlüsselung regelmäßig im Klartext übermittelt wird. Ein Angreifer kann die SSID somit aus dem Netzwerkverkehr herausfiltern.

- Die MAC-Adressen der Netzwerkkarten sind weltweit eindeutig festgelegt. Viele so genannte Access-Points (zentrale Knotenpunkte in einem WLAN) können somit den Funkbetrieb auf eine festgelegte Menge von Netzwerkkarten beschränken, die anhand ihrer Adresse definiert werden. Leider erweist sich diese Einschränkung als wirkungslos, da man die Adresse von Netzwerkadaptern im laufenden Betrieb verändern kann (siehe Fünfter Tätigkeitsbericht, Punkt 3.18.7).

Obwohl alle bisher genannten Techniken keinem auch nur halbwegs versierten Angreifer standhalten, sollten sie dennoch verwendet werden, um einen Grundschutz zu erreichen und wenigstens Gelegenheitstäter auszuschließen. Im Einzelnen sollte dieser Grundschutz in Anlehnung an die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aus folgenden Maßnahmen bestehen:

- Es sollten SSIDs vergeben werden, die keinen Rückschluss auf den Betreiber zulassen.

- Die bei der Auslieferung der Access-Points standardmäßig festgelegten Konfigurationspasswörter sind zu ändern.

- Die periodische Aussendung der SSIDs muss am Access-Point abgeschaltet werden („SSID verbergen“).

- Die MAC-Adress-Filterung ist zu aktivieren.

- Die WEP-Verschlüsselung ist einzuschalten und möglichst mit 128 Bit Schlüssellänge (104 Bit effektiv) zu betreiben.

- Da die Authentifikation des Clients gegenüber dem Access-Point kryptographisch fehlerhaft implementiert ist, sollte sie abgeschaltet werden.

- WEP-Schlüssel, SSIDs und Zugangspasswörter sollten anhand der anerkannten Passwortregeln (siehe Punkt 2.20.3) vergeben werden. Sie sind regelmäßig zu ändern.

- WEP-Schlüssel sollten darüber hinaus möglichst den gesamten Schlüsselraum ausnutzen. Das bedeutet, dass sie in Form zufällig gewählter Hexadezimalziffern eingegeben werden sollten.

- Access-Points sind so aufzustellen und ihre Antennen so auszuwählen und auszurichten, dass möglichst nur der gewünschte Bereich ausgeleuchtet wird. Die Sendeleistung ist ebenfalls soweit möglich zu reduzieren.

- Außerhalb der regulären Betriebszeiten sollten Access-Points abgeschaltet werden, beispielsweise mit einer Zeitschaltuhr.

- Es sollten statische IP-Adressen verwendet und der zulässige Adressraum im Server möglichst klein eingestellt werden. DHCP-Server (dynamic host configuration protocol), die den Teilnehmern automatisch IP-Adressen zuweisen, sind abzuschalten. Diese Maßnahmen erschweren es möglichen Eindringlingen, gültige IP-Adressen zu bekommen und damit am Netzwerk teilzunehmen.

- Die Firmware der Geräte muss ständig auf dem neuesten Stand sein.

- Access-Points dürfen nicht über die Funkschnittstelle administriert werden, wenn die Kommunikation nicht zusätzlich kryptographisch gesichert ist.

Um personenbezogene Daten in Funknetzen zu verarbeiten, sind aber selbst diese Maßnahmen noch nicht ausreichend. Das Netzwerk ist in diesen Fällen zusätzlich mit kryptographischen Mitteln zu schützen, zum Beispiel mit IPSec. Ferner ist der Einsatz von Personal Firewalls erforderlich. Werden Funknetze mit bestehenden LANs gekoppelt, ist außerdem der Einsatz weiterer Firewalls zu erwägen.

2.19 Biometrische Verfahren

2.19.1 Biometrie in Ausweisen

Weltweit sind die Anstrengungen verstärkt worden, um den Terrorismus wirksam zu bekämpfen. In Deutschland beispielsweise eröffnet das Terrorismusbekämpfungsgesetz die Möglichkeit, neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale in Pässe und Personalausweise deutscher Staatsbürger aufzunehmen (siehe Fünfter Tätigkeitsbericht, Punkt 3.3.5). Das soll die Überprüfung der Echtheit der Dokumente und der Identität von Personen erleichtern. Zulässig wären biometrische Daten des Gesichts, der Finger (Fingerabdruck), der Hand (Handgeometrie und Handlinien) oder der Augen (Iris und Retina) beziehungsweise Kombinationen dieser Merkmale. Ein Bundesgesetz soll regeln, welche biometrischen Merkmale erhoben, wie sie erfasst und gespeichert und auf welche Weise diese Daten genutzt werden dürfen.

Bei biometrischen Merkmalen handelt es sich um personenbezogene Daten, die laut Art. 8 der EG-Datenschutzrichtlinie beziehungsweise § 3 Abs. 9 Bundesdatenschutzgesetz oder § 7 Abs. 2 Landesdatenschutzgesetz besonders schutzbedürftig sind. Derartige Daten können beispielsweise Informationen über die ethnische Herkunft oder den Gesundheitszustand des Betroffenen enthalten. Die Verarbeitung dieser Daten ist daher ein gravierender Eingriff in das grundgesetzlich geschützte Persönlichkeitsrecht. Darüber hinaus eignen sich biometrische Merkmale prinzipiell zur Bildung einheitlicher Personenkennzeichen, die nach dem Volkszählungsurteil (BVerfGE 65,1, -53-) unzulässig sind. Vor diesem Hintergrund muss besonders sorgfältig geprüft werden, ob der Eingriff in das Persönlichkeitsrecht, der mit der Verarbeitung biometrischer Daten zwangsläufig einhergeht, für die Bekämpfung des internationalen Terrorismus tatsächlich geeignet, erforderlich und angemessen ist.

Geeignetheit
Zur Prüfung der Identität Einzelner mit Hilfe biometrischer Verfahren ist es erforderlich, deren bereits erfasste biometrische Merkmale (die so genannten Templates) mit aktuellen, bei der Kontrolle aufgenommenen Merkmalen zu vergleichen. Geeignet sind solche Verfahren nur dann, wenn eine ausreichend hohe Erkennungsleistung garantiert wird. Die Qualität des Vergleichs und damit die Leistungsfähigkeit biometrischer Systeme beschreiben vor allem folgende drei Parameter:

- Die False Rejection Rate (FRR) ist ein Maß für die Zahl der unberechtigt zurückgewiesenen Personen. Das betrifft die Fälle, bei denen der Vergleich der aktuell gemes-

senen Werte mit den Templates ein negatives Ergebnis liefert, obwohl die Daten übereinstimmen müssten.

- Die False Acception Rate (FAR) beschreibt, wie viele Personen fälschlicherweise als Berechtigte erkannt wurden. In diesem Fall hat der Vergleich eine Übereinstimmung geliefert, obwohl die Templates nicht zu den überprüften Personen gehören.

- Die False Enrollment Rate (FER) nennt den Anteil der Personen, bei denen das gewünschte biometrische Merkmal für eine Identitätsprüfung nicht geeignet ist oder nicht in das System eingelesen werden kann.

Darüber hinaus muss ein biometrisches Verfahren ein hohes Maß an Überwindungssicherheit aufweisen. Es darf also nicht möglich sein, das zu prüfende biometrische Merkmal nachzuahmen oder dem System auf irgendeine Weise gefälschte Datensätze zur Prüfung zu präsentieren.

Aus technischer Sicht ist ein biometrisches Verfahren nur dann zur Prüfung der Identität geeignet, wenn möglichst wenig Personen unberechtigt zurückgewiesen werden (FRR klein), möglichst viele unberechtigte Personen abgewiesen werden (FAR klein), das zu prüfende biometrische Merkmal möglichst vieler Personen verarbeitet werden kann (FER klein) und eine angemessen hohe Überwindungssicherheit garantiert ist. Um eine seriöse Aussage über die Leistungsfähigkeit biometrischer Identifikationssysteme zu erhalten, sind umfangreiche Tests erforderlich.

Das Bundeskriminalamt (BKA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) beauftragten das Fraunhofer Institut für graphische Datenverarbeitung Darmstadt (IGD) bereits im April 1999, einen solchen Test durchzuführen. Untersucht wurden so genannte Scanner für Fingerabdruck, Handgeometrie und Iris, Erkennungssysteme für Gesichter und Unterschriften und kombinierte Systeme, die auch die Lippenbewegung und die Stimme zur Identifikation nutzen. An dem Feldversuch beteiligten sich etwa 50 Personen auf freiwilliger Basis. Nach einjähriger Testzeit legte das IGD die Ergebnisse in einer detaillierten Studie vor. Sie zeigte, dass die getesteten biometrischen Systeme noch nicht alltagstauglich und für sicherheitskritische Anwendungen nur sehr eingeschränkt geeignet waren. Neben der schlechten Erkennungsleistung wurde auch die geringe Überwindungssicherheit kritisiert.

Im Juni 2003 präsentierte das BSI den Abschlussbericht eines weiteren Feldversuches (http://www.bsi.de/fachthem/BioFace/BioFaceIIBericht.pdf). Wieder war das IGD beauftragt worden, biometrische Identifikationssysteme zu testen. Im Projekt BioFace wurde

die Erkennungsleistung von Gesichtserkennungssystemen untersucht. Diesmal beteiligten sich 116 Testpersonen, und es stand eine Referenzdatenbank mit Bildern von 50.000 weiteren Personen zur Verfügung. Das Ergebnis des Systemtests war wieder ernüchternd. Im Abschlussbericht heißt es: „Die Erkennungsleistungen sind bei weitem nicht so gut wie sie die Werbung der Systemhersteller ihnen zubilligt. Eine Erkennungsleistung von knapp 50 % ist allenfalls in einem automatisierten Überwachungsszenario ausreichend (immerhin hat man fast die Hälfte der gesuchten Personen ohne menschliche Hilfe detektiert), für eine automatisierte Zutrittskontrolle ist sie jedoch in keiner Weise akzeptabel (mehr als der Hälfte der Zutrittsberechtigten bliebe der Zutritt verwehrt).“ Mit Blick auf die mangelnde Verfügbarkeit der Systeme und die unzureichende Unterstützung der Hersteller ist der Studie weiterhin zu entnehmen: „Mitunter konnten sie (die Hersteller) technische Fragen nicht selbst beantworten, oder zur Inbetriebnahme der Systeme und zur Fehlerbehebung vor Ort mussten Fachleute aus fernen Ländern eingeflogen werden. Insbesondere letzterer Umstand wäre bei der Inbetriebnahme solcher Systeme in deutschen Bundesbehörden aus sicherheitstechnischer Sicht unter Umständen nicht tragbar.“

Nach Ansicht der Tester ist „...die Tauglichkeit der Gesichtserkennungssysteme als (unterstützende) Verifikations- bzw. Identifikationssysteme durch BioFace nicht abschließend beweis- oder widerlegbar ...“. Es gibt also nach wie vor keine verlässlichen Aussagen darüber, inwieweit biometrische Gesichtserkennungssysteme zur Prüfung der Identität geeignet sind. Das BSI weist allerdings darauf hin, dass die Anzahl der Testpersonen nicht groß genug war, um statistisch belastbares Zahlenmaterial zu liefern.

Erforderlichkeit

Bevor neue biometrische Merkmale in Ausweisen gespeichert werden, ist zu klären, ob die vorhandenen nicht bereits ausreichen, um die Identität des Ausweisinhabers auf angemessen sichere Weise zu prüfen. Die Eingriffstiefe in das Recht auf informationelle Selbstbestimmung wäre wesentlich geringer, wenn neue Merkmale nicht erforderlich wären.

Deutsche Ausweise besitzen mit dem Lichtbild des Inhabers bereits ein biometrisches Merkmal. Es gibt auch schon Verfahren, die das Foto mit dem Gesicht des Betroffenen automatisch vergleichen. Allerdings ist bisher nicht geklärt, welche Bildqualität notwendig ist, um beim Vergleich verlässliche Ergebnisse zu erzielen. Unklar ist auch, welchen Einfluss Alterungserscheinungen auf die Erkennungsleistung haben. Die Verwendung neuer biometrischer Merkmale sollte deshalb erst dann erwogen werden, wenn diese technischen Fragen geklärt sind.

Mit der handschriftlichen Unterschrift enthält jeder Ausweis ein weiteres biometrisches Merkmal. Um die Identität des Ausweisinhabers zu prüfen, müsste diese Unterschrift automatisch mit einer bei Kontrollen geleisteten Unterschrift verglichen werden. Auf dem Ausweis sind die für eine Unterschrift charakteristischen dynamischen Merkmale (z. B. Druckverlauf, Schreibpausen) jedoch nicht gespeichert. Ein Vergleich ist daher wenig sinnvoll.

Angemessenheit

Mit biometrischen Merkmalen beziehungsweise mit dem daraus resultierenden Datensatz lassen sich viele unterschiedliche Daten des Betroffenen erschließen und verknüpfen. Damit kämen biometrische Merkmale prinzipiell einem einheitlichen Personenkennzeichen gleich, welches das Bundesverfassungsgericht im so genannten Volkszählungsurteil (BVerfGE 65, 1, -53-) für unzulässig erklärt hat.

Das Terrorismusbekämpfungsgesetz lässt eine bundesweite Datei mit biometrischen Daten bisher nicht zu. Wenn der Aufbau dieser zentralen Datenbank aber nicht dauerhaft ausgeschlossen wird, droht eine neue Überwachungsqualität. Existiert erst einmal eine flächendeckende Infrastruktur zur Erfassung biometrischer Merkmale, so ist zu befürchten, dass im Alltag erfasste biometrische Daten mit zentralen Datenbeständen abgeglichen und sehr weitgehende Bewegungsprofile erstellt werden können. Würden dafür beispielsweise Gesichtserkennungssysteme genutzt, die biometrische Merkmale über eine gewisse Entfernung ohne Mitwirkung der betroffenen Personen erheben, wäre eine heimliche Überwachung durchaus realisierbar.

Schließlich ist auch zu berücksichtigen, dass einige biometrische Merkmale nicht nur zur Identifizierung genutzt werden können, sondern auch weitergehende Auswertungen ermöglichen. So kann beispielsweise unter Umständen auf bestimmte gesundheitliche Zustände geschlossen werden, was die Gefahr der zweckentfremdeten Nutzung biometrischer Daten in sich birgt.

Angesichts der Risiken, die mit dem flächendeckenden Einsatz biometrischer Erkennungssysteme verbunden sind, halte ich ihre Nutzung mit dem Ziel der Bekämpfung des internationalen Terrorismus für unangemessen. Der tiefe Eingriff in das Recht auf informationelle Selbstbestimmung steht meines Erachtens in keinem annehmbaren Verhältnis zu den Missbrauchsmöglichkeiten dieser Technik.

Ich unterstütze nachdrücklich eine zentrale Forderung des Büros für Technikfolgenabschätzung beim Deutschen Bundestag (TAB). In einem Sachstandsbericht zu biometri-

schen Identifikationssystemen vom Februar 2002 fordern die Verfasser unter anderem: „Zur weiteren Abklärung der zukünftigen Entwicklung biometrischer Systeme sollte eine umfassende Technikfolgen-Abschätzung durchgeführt werden. Erforderlich wäre eine systematische, zukunftsorientierte Analyse und Beurteilung der gesellschaftlichen, ökonomischen und rechtlichen Voraussetzungen und Folgen einer weiter zunehmenden Verbreitung biometrischer Verfahren."

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im März 2002 eine Entschließung zum Thema verabschiedet (siehe Anlage 1). Die Datenschutzbeauftragten haben detaillierte Forderungen formuliert für den Fall, dass entgegen bestehender Bedenken biometrische Merkmale in Pässe und Personalausweise aufgenommen werden. Diese Forderungen basieren auf dem „Positionspapier zu technischen Aspekten biometrischer Merkmale in Personalausweisen und Pässen", das der Arbeitskreis „Technische und organisatorische Datenschutzfragen" (siehe Punkt 4) im Auftrag der Konferenz erarbeitet hat. Das Papier kann aus meinem Internetangebot unter http://www.lfd.m-v.de/beschlue/63biomed.html heruntergeladen werden.

2.19.2 Fingerabdruck als Zugang zum Kopierer

Die Verwaltung eines Landkreises wollte ihre Kopiergeräte mit einem Fingerabdrucklesegerät ausstatten, damit nur berechtigte Mitarbeiter Unterlagen kopieren können. Gleichzeitig wollte man die Kopierkosten besser kontrollieren und den einzelnen Kostenstellen zuordnen. Mitarbeiter der Verwaltung fragten mich, ob sie ihren Fingerabdruck dafür speichern lassen müssen. Sie befürchteten, dass nicht sorgsam mit diesen Daten umgegangen wird und im Falle einer Weigerung mit dienstrechtlichen Konsequenzen zu rechnen sei.

Biometrische Verfahren wie der Fingerabdruckvergleich können ein geeigneter Ersatz für eine Zugangskontrolle über ein Verfahren mit persönlicher Identifikationsnummer (PIN) sein. Allerdings werden gegenwärtig im täglichen Leben sehr viele Verfahren der Zugangskontrolle darüber abgewickelt, unter anderem bei der Bank-Card, beim Handy oder beim Zutritt zu bestimmten Räumen. Das PIN-Verfahren hat daher den Nachteil, dass sich die Nutzer oftmals viele verschiedene PINs merken müssen. Deshalb wird die PIN von den Nutzern häufig aufgeschrieben und leider nicht immer sicher verwahrt. Bei der PIN besteht die Gefahr, dass sie unberechtigten Dritten zur Kenntnis gelangt. Dahingegen werden bei biometrischen Verfahren unverwechselbare Körpermerkmale verarbeitet. Bei dem Fingerabdruckverfahren werden beispielsweise vorab charakteristische Verzweigungen der Papillarlinien eines Fingers gespeichert. Sie werden dann mit denen des aufgelegten

Fingers verglichen. Stimmen beide Muster überein, wird der Zugang gewährt. Dabei ist es nicht erforderlich, die biometrischen Daten zentral zu speichern. Hier eignet sich zum Beispiel eine persönliche Chipkarte, mit der die betroffene Person ihren Vergleichs-Fingerabdruck in den Kopierer eingibt. Verfügt die Person über die Chipkarte, ist ein Missbrauch weitgehend ausgeschlossen.

Biometrische Verfahren greifen allerdings zwangsläufig stärker in die Privatsphäre eines Betroffenen ein. Werden darüber hinaus die biometrischen Daten, wie von der Verwaltung des Landkreises vorgesehen, zentral gespeichert, sind aufwändige technische und organisatorische Maßnahmen zu ihrem Schutz erforderlich.

Diese Bewertung habe ich dem Landkreis mitgeteilt und darauf hingewiesen, dass die Nutzung biometrischer Verfahren für diese Anwendung nur auf freiwilliger Basis zulässig ist. Ich habe daher empfohlen, den Mitarbeitern freizustellen, ob sie das Fingerabdruckverfahren oder alternative Verfahren nutzen wollen.

Der Landkreis ist dieser Empfehlung gefolgt. Für Mitarbeiter, die das neue System ablehnen, werden Alternativen angeboten. Sie können die Kopien beispielsweise in der Hausdruckerei in Auftrag geben, oder am Arbeitsplatz werden entsprechende Geräte aufgestellt. Dienstrechtliche Konsequenzen seien nie vorgesehen gewesen, so der Landkreis.

2.20 Technik und Organisation

2.20.1 Computerdiebstahl leicht gemacht

In meinem Fünften Tätigkeitsbericht habe ich unter Punkt 3.7.4 über den Diebstahl eines Computers aus einem Rechnungsprüfungsamt informiert. Unzureichende technische und organisatorische Maßnahmen waren damals die Gründe für eine Beanstandung. Der Oberbürgermeister hatte daraufhin zugesagt, in einem Datenschutzkonzept die erforderlichen Maßnahmen zu dokumentieren und unverzüglich umzusetzen.

Etwa achtzehn Monate später berichtete die Presse über einen erneuten Einbruch in den Gebäudekomplex der Stadtverwaltung. Wieder waren Computer gestohlen worden, auf denen sensible personenbezogene Daten gespeichert waren. Dabei handelte es sich um Daten, die dem Sozialgeheimnis unterliegen und die gemäß § 35 Sozialgesetzbuch Erstes Buch (SGB I) und §§ 67 bis 85a Sozialgesetzbuch Zehntes Buch (SGB X) besonders zu schützen sind.

Eine Kontrolle zeigte, dass keine der Maßnahmen umgesetzt worden war, die der Oberbürgermeister anlässlich des ersten Einbruchs zugesagt hatte. Der Amtsleiter verwies darauf, dass die Haushaltslage der Stadt die erforderlichen Investitionen bisher nicht zugelassen hätte. So wurde weder ein Sicherheitskonzept erstellt noch eine Einbruchmeldeanlage installiert. Selbst die besonders sensiblen Sozialdaten wurden weiterhin unverschlüsselt gespeichert. Darüber hinaus waren die Mitarbeiter völlig unzureichend zu Fragen des Datenschutzes geschult und ließen demzufolge die angemessene Sensibilität beim Umgang mit den schutzbedürftigen Daten vermissen.

Die andauernden, gravierenden Mängel bei der Verarbeitung von Sozialdaten und den damit verbundenen wiederholten Verstoß gegen datenschutzrechtliche Bestimmungen habe ich erneut beanstandet. Bereits während der Kontrolle habe ich Empfehlungen gegeben, wie auch ohne erheblichen Kostenaufwand kurzfristig ein wirksamerer Schutz der verarbeiteten Sozialdaten erreicht werden kann. Insbesondere habe ich Möglichkeiten aufgezeigt, wie die Daten verarbeitet werden können, ohne dass sie dauerhaft auf den Personalcomputern gespeichert werden müssen. Der zuständige Amtsleiter sagte zu, sofort Maßnahmen zu treffen, die einen angemessenen Schutz der personenbezogenen Daten gewährleisten.

Doch schon eine Woche später informierte mich der Oberbürgermeister über einen weiteren Einbruch im gleichen Bereich. Die gerade beschafften Personalcomputer und Bild-

schirme waren gestohlen worden. Und wieder befanden sich sensible Sozialdaten auf den Festplatten der Rechner.

Jetzt erst reagierte die Stadtverwaltung so, wie es schon längst erforderlich gewesen wäre: Sie hat sofort die Beschaffung einer Einbruchmeldeanlage angewiesen. Bis zur Installation der festen wurde eine funkgesteuerte Anlage in Betrieb genommen. Sozialdaten wurden nun entsprechend meiner Empfehlung nur noch auf geschützten, zentralen Servern gespeichert. Die umgehende Auswertung dieser Vorfälle durch den Amtsleiter und spezielle Schulungen durch die behördliche Datenschutzbeauftragte sollen dazu beitragen, die Mitarbeiter zu Datenschutzfragen zu sensibilisieren. Begonnen wurde auch mit der Erarbeitung des Sicherheitskonzeptes und einer Dienstanweisung zum Umgang mit Sozialdaten. Darüber hinaus hat der Oberbürgermeister zugesagt, mich unaufgefordert regelmäßig über den Fortschritt der Umsetzung des Konzeptes zu informieren.

Im Ergebnis bleibt festzustellen, dass hier offensichtlich „am falschen Ende“ gespart worden ist. Durch die fehlenden Sicherungsmaßnahmen sind der Stadt nun insgesamt höhere Kosten entstanden, als sie für die erforderliche Technik hätte investieren müssen. Darüber hinaus wurden insbesondere schutzbedürftige Interessen der betroffenen Personen erheblich beeinträchtigt.

2.20.2 Datenlöschung bei gefundenen Handys

Immer öfter werden in Fundbüros auch Handys abgegeben. In den Speichern dieser Geräte befinden sich mitunter Daten über Familienangehörige, Bekannte und Geschäftspartner, Kurznachrichten und manchmal sogar ganze elektronische Kalender. Meldet sich der Eigentümer nach einer bestimmten Zeit nicht, übergibt das Fundbüro die Gegenstände dem Finder oder versteigert sie. Die Datenschutzbeauftragte einer Kommune hat mich gefragt, was in diesem Fall mit den gespeicherten Daten passieren solle.

Ich habe folgendes Vorgehen empfohlen:

Die im Telefon befindliche Chipkarte, die so genannte SIM-Karte, ist Eigentum des Mobilfunk-Providers. Bevor also der Finder das Telefon bekommt, sollte das Fundbüro dem Provider die Kartennummer mitteilen. Der Provider kann dann in der Regel den Eigentümer des Telefons ermitteln und ihn über den Fund informieren.

Parallel dazu sollte das Fundbüro die Polizei fragen, ob das Telefon als gestohlen gemeldet wurde. Dazu muss die Gerätenummer (IMEI) herangezogen werden. Findet die Polizei den Eigentümer, so müsste sie ihn ebenfalls informieren.

Kann der Eigentümer jedoch nicht ermittelt werden, darf der Finder das Gerät nur dann erhalten, wenn eine Fachwerkstatt zuvor alle Daten gelöscht hat. Die Kosten für diese Dienstleistung sind gering, werden jedoch nicht vom Fundbüro übernommen. Deshalb sollte der Finder schon beim Abgeben bestätigen, dass er im Falle der Annahme des Handys die Löschung der Daten auch bezahlt. Andernfalls darf das Fundbüro das Gerät nicht aushändigen, sondern muss es datenschutzgerecht vernichten, beispielsweise durch mechanische Zerstörung von Tastatur und Elektronik.

2.20.3 Passwort – Sechs Zeichen sind zu wenig

Nutzer dürfen personenbezogene Daten nur dann automatisiert verarbeiten, wenn sie dazu berechtigt sind (§ 22 Abs. 1 DSG M-V). Zu diesem Zweck verlangen Rechner oft die Eingabe einer Nutzerkennung (Identifikation) und eines Passwortes. Das Passwort funktioniert dabei wie ein Ausweis, mit dem der Computer die Identität des Nutzers überprüft. Diese Prüfung heißt Authentifikation. Erst nach erfolgreicher Authentifikation kann ein Nutzer die ihm zugeteilten Rechte ausüben, wie Dateien lesen oder ändern.

Immer wieder versuchen jedoch auch Unberechtigte, auf personenbezogene Daten zuzugreifen, und bedienen sich dabei unterschiedlicher Angriffsmethoden.

So kann ein Angreifer einen interessant erscheinenden Nutzernamen wählen und dann einfach verschiedene Passwörter ausprobieren. Nutzernamen sind in der Regel leicht zugänglich, und viele Nutzer wählen leicht zu erratende Passwörter wie Namen von Familienangehörigen oder Geburtstage aus. Um derartige Angriffe abzuwehren, sperren viele Systeme den Zugriff auf Nutzerkonten, wenn jemand zu oft versucht, sich mit einem falschen Passwort anzumelden.

Des Weiteren könnte ein Eindringling versuchen, in den Besitz der auf dem System gespeicherten Passwörter zu gelangen. Solche Angriffe können erfolgreich sein, wenn die Zugriffsrechte falsch gesetzt sind oder wenn das System andere Sicherheitslücken aufweist. Um den unberechtigten Zugriff auf Passwörter zu erschweren, sollen Passwörter in IT-Systemen verschlüsselt gespeichert werden.

Aber selbst die Verschlüsselung schützt nicht in jedem Fall. Folgendes Szenario verdeutlicht dies: Ein Angreifer wählt beliebige Passwörter aus und verschlüsselt sie mit dem Verfahren, welches das angegriffene System verwendet. Stimmt der gerade berechnete mit einem der gespeicherten Werte überein, ist ein gültiges Passwort gefunden. Dieser Prozess lässt sich automatisieren, indem die Passwortkandidaten aus Wörterverzeichnissen gewählt werden. Selbst Passwörter in exotischen Sprachen sind nicht sicher, da man mit geringem Aufwand Wörterverzeichnisse für jede beliebige Sprache erstellen kann. Dafür sind nicht einmal Sprachkenntnisse erforderlich, weil sich solche Wörterbücher automatisiert erstellen lassen, indem Texte aus dem Internet in Wörter zerlegt und sortiert werden. Um wörterbuchbasierte Angriffe zu verhindern, sind Passwörter empfehlenswert, die keine sinnvollen Wörter ergeben, also auch in keinem Wörterbuch zu finden sind.

Eine weitere Angriffsmöglichkeit besteht darin, Passworte mit „roher Gewalt“ (englisch: brute force) zu brechen. Dazu bildet der Angreifer Wörter einer bestimmten Länge, indem er alle möglichen Kombinationen eines Zeichensatzes verwendet. Anschließend überprüft er diese Zeichenketten wie oben beschrieben.

Um Passwörter mit den bisher aufgezeigten Methoden zu brechen, sind detaillierte Fachkenntnisse erforderlich. Allerdings gibt es – vorzugsweise im Internet – mittlerweile für die meisten Systeme einfach zu bedienende Programme, die auch wenig geübte Angreifer in die Lage versetzen, Passwörter auszuforschen. (Es spricht übrigens nichts dagegen, dass Systemadministratoren solche „Passwortknacker“ einsetzen, um die Sicherheit ihrer Systeme zu analysieren. Dazu sollten sie allerdings immer die Genehmigung ihrer Vorgesetzten einholen, damit solche Analysen nicht als versuchter Einbruch gewertet werden.)

Um Angriffe auf Passworte zu erschweren, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) Regeln zum Umgang mit Passwörtern im IT-Grundschutzhandbuch veröffentlicht. Auch in meinem Internetangebot sind Hinweise zur Passwortsicherheit zu finden (http://www.lfd.m-v.de/informat/pwd/oh_pwd.html). Sie basieren auf der BSI-Veröffentlichung. Diese Passwortregeln enthalten unter anderem Empfehlungen zu folgenden Aspekten:

- Wie muss ein Passwort zusammengesetzt sein?

- Wann ist ein Passwort zu wechseln?

- Unter welchen Bedingungen dürfen Passwörter hinterlegt werden?

- Wie lang muss ein Passwort mindestens sein?

Mit Blick auf die ständig steigende Leistungsfähigkeit moderner Computer haben Mitarbeiter des Hamburgischen Datenschutzbeauftragten untersucht, wie ein Passwort beschaffen sein muss, um einem Brute-Force-Angriff zu widerstehen. Sie haben berechnet, wie viele Passwörter einer bestimmten Länge sich bilden lassen, wenn man dazu jeweils eine bestimmte Auswahl aus Buchstaben in Groß- und Kleinschreibung, Ziffern und Sonderzeichen trifft. Ferner haben sie experimentell ermittelt, wie viele Passwörter man pro Sekunde mit den heute üblichen Rechnern und Programmen prüfen kann. Es zeigte sich, dass ordnungsgemäß gebildete, sechsstellige Passwörter unter bestimmten Umständen bereits mit einem einzelnen modernen Rechner innerhalb von Minuten gebrochen werden können. Der genaue Wert hängt vor allem davon ab, wie viele verschiedene Zeichen im Passwort tatsächlich vorkommen. Daneben spielt auch das verwendete Verschlüsselungsverfahren eine Rolle. Benutzt man mehrere Rechner gleichzeitig zum Brechen von Passwörtern, sinkt die benötigte Zeit mit der Anzahl der Rechner.

Die Tests der Hamburger Kollegen haben gezeigt, dass Passwörter aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen und mindestens acht Zeichen lang sein müssen, um den oben beschriebenen Angriffen standzuhalten. Abzuraten ist von Passwörtern aus Wörtern einer natürlichen Sprache, und zwar auch dann, wenn sie nur geringfügig verändert sind, etwa durch Anfügen oder Voranstellen von Sonderzeichen.

Da bisher immer eine Mindestpasswortlänge von sechs Zeichen empfohlen wurde, habe ich meine im Internet veröffentlichten Passwortregeln entsprechend angepasst. Auch das BSI hat diese Erkenntnisse aufgegriffen und wird sie in der kommenden Ausgabe des Grundschutzhandbuches berücksichtigen.

2.20.4 Was Rechnernamen verraten können

Mitte 2002 informierte mich der Betreiber einer Website über ungewöhnliche Einträge in den Logdateien seines Servers. Die Protokolle enthielten Namen von Beschäftigten einer Universität unseres Landes mit Angaben zu ihrem jeweiligen Arbeitsbereich.

Wer eine Website lesen möchte, muss dem dazugehörigen Webserver bestimmte Daten zur Verfügung stellen. Damit der Server die angeforderte Seite senden kann, benötigt er so genannte Verbindungsdaten. In jedem Fall sind die IP-Adressen des anfordernden Rechners und der gewünschten Seite erforderlich.

Die Verbindungsdaten werden jedoch oft auch für andere Zwecke verwendet. Viele Betreiber von Websites gewinnen aus ihnen Statistiken über die Nutzung ihres Angebotes. Meist wandelt der Website-Betreiber dazu die numerische IP-Adresse des anfordernden Rechners zunächst in einen sprechenden Host-Namen (Rechnernamen) um. Dazu nutzt er einen praktisch überall im Internet erreichbaren Dienst, das Domain Name System (DNS). DNS-Server wandeln nicht nur Host-Namen wie www.datenschutz.mvnet.de in IP-Adressen wie „195.145.109.16“ um und umgekehrt, sondern stellen auch weitere Informationen bereit. Beispielsweise ist nachvollziehbar, welcher Rechner die elektronische Post für eine bestimmte Gruppe von Computern entgegennimmt. Mitunter kann man sogar den Rechnertyp, das Betriebssystem und den Standort des Rechners auslesen. Diese Informationen sollten aber nicht veröffentlicht werden, weil sie für potentielle Angreifer nützlich sein können.

Das Rechenzentrum der Universität hatte die Personalcomputer in vielen Fällen nach ihren Nutzern benannt. Der Host-Name hatte die Form pc-nachname.bereich.fragliche-uni.de. Das führte dazu, dass jeder Nutzer eines so bezeichneten PC beim Abruf einer Website seine „Visitenkarte“ auf dem entsprechenden Webserver hinterlässt. Für diese Offenbarung personenbezogener Daten existiert keine Rechtsgrundlage. Deshalb ist sie nur zulässig, wenn die betroffenen Bediensteten einwilligen. Die Universität hatte eine solche Einwilligung jedoch nicht eingeholt.

Damit die Beschäftigten künftig auf datenschutzgerechte Weise Internetdienste nutzen können, habe ich folgende Alternativen vorgeschlagen:

1. Es sind nachträglich Einwilligungserklärungen der Betroffenen einzuholen, die den Anforderungen des § 8 Landesdatenschutzgesetz entsprechen.

2. Das DNS ist so zu betreiben, dass von außen nur diejenigen Adressen abfragbar sind, die tatsächlich sichtbar sein sollen (z. B. die des Webservers). Falls sich Hosts mit Namen von Bediensteten darunter befinden, ist auch hier die Einwilligung der Betroffenen erforderlich.

3. Personennamen werden in Host-Namen nicht verwendet. Damit sinkt auch der Aufwand bei der Umstrukturierung lokaler Netze.

Die Universität hat sich für die zweite Variante entschieden.

2.20.5 Kryptographie in der Praxis – Handlungsempfehlungen

Bis vor nicht allzu langer Zeit waren kryptographische Verfahren etwas Geheimnisumwittertes, das man nur mit Geheimdiensten oder mit der organisierten Kriminalität in Verbindung brachte. Mit der Verbreitung des Computers und der rasanten Entwicklung seiner Leistungsfähigkeit haben kryptographische Verfahren die Sphäre des Geheimnisvollen jedoch verlassen. Auch der Versuch, Kryptographie zu reglementieren, weil ja auch Straftäter diese Verfahren nutzen können, hat sich als untauglich erwiesen (siehe Dritter Tätigkeitsbericht, Punkt 4.2 und Vierter Tätigkeitsbericht, Punkt 3.16.2). Heute finden kryptographische Verfahren wie Verschlüsselung oder elektronische Signatur gesamtgesellschaftliche Verbreitung. Hard- oder softwarebasierte Kryptographie wird als preiswertes und einfach bedienbares Massenprodukt am Markt für jedermann angeboten.

Die Datenschutzbeauftragten des Bundes und der Länder haben die öffentlichen Stellen vor diesem Hintergrund schon vor einigen Jahren aufgefordert, vorbehaltlos die technischen Möglichkeiten des Einsatzes kryptographischer Verfahren zum Schutz personenbezogener Daten zu prüfen und derartige Lösungen häufiger als bisher einzusetzen. Sie fordern, dass Kryptographie zum Standard in der Informations- und Kommunikationstechnik werden muss, auf deren Einsatz nur dann verzichtet werden sollte, wenn wichtige Gründe dagegen sprechen (Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. Oktober 1999 – Vierter Tätigkeitsbericht, Anlage 15).

Nach wie vor ist jedoch die Auswahl eines kryptographischen Verfahrens keineswegs trivial. Welche kryptographischen Methoden geeignet und welche Produkte für den jeweiligen Einsatzzweck wirksam und wirtschaftlich sind, muss für jeden Einzelfall entschieden werden. Die Datenschutzbeauftragten des Bundes und der Länder wollen insbesondere öffentliche Stellen bei diesen Entscheidungsprozessen unterstützen. Zu diesem Zweck hat eine Arbeitsgruppe des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ (siehe Punkt 4) die „Orientierungshilfe zum Einsatz kryptographischer Verfahren“ erarbeitet.

Die Orientierungshilfe gibt zunächst einen kurzen Überblick über die technischen Grundlagen der Kryptographie und erläutert die verschiedenen mathematischen Prinzipien. Es werden die Szenarien der Informationstechnik beschrieben, für die der Einsatz kryptographischer Verfahren in Betracht kommt. In einem weiteren Abschnitt werden allgemeine Lösungsansätze für Verschlüsselungs- und Signaturverfahren erläutert und Unterschiede zwischen hard- und softwarebasierten Verfahren erklärt. Darüber hinaus findet man konkrete Hinweise für verschiedene IT-Szenarien, so beispielsweise Empfehlungen zur Verschlüsselung sowohl in Landes- als auch in kleineren privaten Netzen. Es wird be-

schrieben, mit welchen Verfahren sich E-Government-Lösungen absichern lassen und unter welchen Voraussetzungen die elektronische Post für rechtsverbindliche Kommunikationsvorgänge genutzt werden kann. Ein umfangreiches Glossar, in dem kryptographisch relevante Begriffe ausführlich erläutert werden, rundet die Orientierungshilfe ab.

Unsere Landesregierung wertet kryptographische Verfahren wie Verschlüsselung und elektronische Signatur zu Recht als Basiskomponenten für E-Government-Projekte im Land (siehe Punkt 2.16.4). Die Empfehlungen der Orientierungshilfe sollten bei der Realisierung dieser Projekte berücksichtigt werden. Auch für Unternehmen der Privatwirtschaft und Privatleute kann dieses Papier nützlich sein.

Die Orientierungshilfe ist aus meinem Internetangebot unter http://www.lfd.m-v.de/informat/krypto/oh_krypt.pdf abrufbar.

2.20.6 Polizeifunk – und immer noch hören alle zu

Das (analoge) Funksystem von Polizei und Rettungskräften ist technisch hoffnungslos veraltet. Vertreter der Gewerkschaft der Polizei (GdP) in Mecklenburg-Vorpommern äußerten sich im Dezember 2002 gegenüber der Presse: „Kollegen stehen in Funklöchern, Fahndungen verknistern im Äther, Gespräche zwischen Leitstellen und Einsatzkräften können abgehört werden."

Die Mängel sind seit vielen Jahren bekannt. Bereits im Oktober 1993 wies die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung darauf hin, dass die Vertraulichkeit der Funkkommunikation von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) gefährdet sei. Die Datenschutzbeauftragten forderten schon damals, den so genannten BOS-Funk zu digitalisieren, um das Abhören des Funkverkehrs zu unterbinden (siehe Erster Tätigkeitsbericht, Punkt 2.21.3).

Auch die Konferenz der Innenminister der Länder (IMK) war sich seit langem einig, dass ein bundesweit einheitliches Digitalfunk-System erforderlich sei. 1996 wurde die Einführung eines solchen Systems, das auf europäischen Standards basieren sollte, beschlossen. Ende 2000 wurde die „Zentralstelle für die Vorbereitung der Einführung eines bundesweit einheitlichen digitalen Sprech- und Datenfunksystems" (ZED) gegründet. Im Mai 2001 unterzeichneten der Bund und zwölf Bundesländer das Verwaltungsabkommen über die ZED. Unser Landtag beriet im September 2001 über den Beitritt des Landes zum ZED-Verwaltungsabkommen. Alle Fraktionen waren sich einig, dass auch Mecklenburg-Vorpommern in diesem Gremium mitarbeiten muss. Im Oktober 2001 lag der erste ausführ-

liche Bericht der ZED vor. Er verdeutlichte unter anderem, dass Ausweichlösungen, etwa die Nutzung öffentlicher Mobilfunknetze (GSM, UMTS), kaum praktikabel und taktisch unvertretbar sind. Als einzig mögliche Alternative wurde ein eigenständiges, digitales Netz angesehen.

Im Bericht wurde herausgestellt, welche Leistungsmerkmale das künftige Netz haben muss:

- rasche und flexible Zusammenschaltung verschiedener Teilnehmer (dynamische Gruppenbildung)

- Kommunikation der Einsatzkräfte untereinander ohne Zwischenschaltung einer Leitstelle (Direct Mode)

- effektive und flexible Alarmierung der Einsatzkräfte (Paging)

- Übermittlung von Daten parallel zur Sprachkommunikation

- Abhörsicherheit durch Ende-Ende-Verschlüsselung

- Kompatibilität zu den BOS-Netzen europäischer Partner

Der Zeitplan der ZED sah vor, das Ausschreibungsverfahren zur Beschaffung der Technik im Juli 2003 durch den Zuschlag der Vergabestelle abzuschließen und die entsprechenden Verträge zu unterzeichnen.

Als technische Lösung kommen nach Bewertung der ZED nur zwei am Markt verfügbare Systeme in Betracht:

- TETRA 25 (Motorola, Rhode & Schwarz und Dolphin)

- TETRAPOL (EADS, MATRA, AEG Mobile Communication und Siemens)

Nach Vorstellung der ZED kommt TETRA 25 den Anforderungen des BOS-Funks unter den konkreten Bedingungen in Deutschland und unter Berücksichtigung der europäischen Entwicklung am nächsten.

Man sollte nun annehmen, dass die Einführung des digitalen BOS-Funks unmittelbar bevorsteht. Doch weit gefehlt! Die Finanzminister der Länder stellten auf ihrer Sitzung im

Juni 2002 fest, dass „eine Finanzierung des Projektes auf der Basis des aus dem Interessenbekundungsverfahren gewonnenen Finanzbedarfs nicht realistisch ist. Zur Senkung der Kosten ist es unabdingbar, einen technischen Mindeststandard festzulegen. Dabei müssen auch die technischen Alternativen (GSM-Netze, UMTS-Netze, WLAN) wieder einbezogen werden." Die IMK beauftragte daraufhin die ZED, nochmals einen Bericht zur Beschreibung der Leistungsmerkmale des BOS-Digitalfunknetzes vorzulegen.

Somit steht die Einführung des digitalen BOS-Funks praktisch wieder am Anfang. Die bisher favorisierte Lösung ist in Frage gestellt. Der Vorsitzende der GdP äußerte im September 2003 gegenüber der Presse, dass „die innere Sicherheit Deutschlands sich ohne digitalen Polizeifunk auf rasanter Fahrt in die Katastrophe befindet". Auch die Datenschützer sehen die Entwicklung mit Sorge, da die Vertraulichkeit der Funkkommunikation nach wie vor nicht gewährleistet ist.

2.20.7 Schulnotenverwaltung – gutes Konzept von Schülern entwickelt

Im Sommer 2003 bat mich eine Schule um Beratung zu einem Schulnoten-Verwaltungs-System, welches Schüler entwickelt hatten. Lehrer sollen die Noten künftig in ein „virtuelles Klassenbuch" eintragen, in das auch Schüler und Eltern einsehen können. Lehrer, Schüler und Eltern können das System auch zu Hause nutzen, denn es ist an das Internet angeschlossen. Da zusätzlich Erläuterungen zu den Leistungen und Durchschnittsnoten hinterlegt sind, brauchen die Lehrer keine zusätzlichen Aufzeichnungen mehr zu führen – auch nicht, um sich Fehlstunden zu notieren. Dieses System basiert auf anerkannten und erprobten Programmsystemen, deren Quellcode öffentlich zugänglich ist (Open Source Software). So werden das Betriebssystem Linux, der Webserver Apache, das Datenbanksystem MySQL und die Netzwerk-Verschlüsselung OpenSSL verwendet.

Die Schüler haben ein wirkungsvolles und datenschutzgerechtes Zugriffsschutzkonzept entwickelt und damit die Vorgabe des Schulgesetzes unseres Landes realisiert (§ 70 Abs. 5 SchulG M-V). So müssen sich Lehrer, Schüler und Eltern dem System gegenüber authentifizieren, bevor sie es nutzen können. Jeder Schüler kann nur die ihn betreffenden Daten lesen. Die Eltern können Schulnoten ihrer Kinder nur einsehen, solange diese minderjährig sind. Benutzt man die Web-Oberfläche des Systems, so werden die Daten ausschließlich verschlüsselt übertragen.

Nur wenige technische Aspekte waren noch zu verbessern. So habe ich empfohlen, auf einen drahtlosen Zugang zum System mittels der Verfahren Infrarot und Bluetooth zunächst zu verzichten, weil die Daten bei der Infrarot-Übertragung nicht verschlüsselt werden und

die Implementation des Bluetooth-Standards häufig mit Sicherheitsmängeln behaftet ist. Ferner habe ich auf die Bestimmungen zur Auftragsdatenverarbeitung von § 4 Landesdatenschutzgesetz hingewiesen, falls der Betrieb des Systems einem Privatunternehmen übertragen werden soll. Darüber hinaus sollten die Nutzer des Verfahrens ihre Start-Passwörter in verschlossenen Briefumschlägen erhalten. Alle Teilnehmer sollten die zugeteilten Passwörter bei der ersten Benutzung ändern.

Insgesamt jedoch zeigte die Schülerarbeit ein erfreulich hohes Sicherheitsniveau, an dem sich so mancher IT-Experte aus Verwaltung und Wirtschaft ein Beispiel nehmen sollte.

2.20.8 Pseudonymisierte Protokolle

Protokolle sind erforderlich, um nachträglich kontrollieren zu können, ob Daten ordnungsgemäß verarbeitet wurden. Das Landesdatenschutzgesetz (DSG M-V) fordert solche Aufzeichnungen (z. B. § 21 Abs. 2 Nr. 5, § 22 Abs. 2 und Abs. 4). Aus Protokollen muss ein Nutzer aber erst dann identifizierbar sein, wenn ein konkreter Missbrauchsverdacht vorliegt. Die meisten bisher am Markt verfügbaren Protokollierungsprogramme sind jedoch nicht in der Lage, derart differenzierte Protokolle zu erzeugen.

Der Fachbereich Informatik der Universität Dortmund hat sich dieses Themas angenommen. Während einer Sitzung des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ (siehe Punkt 4) stellten wissenschaftliche Mitarbeiter des Fachbereiches die Ergebnisse eines Forschungsprojektes vor. Es wurde untersucht, ob Datenverarbeitungsvorgänge so protokolliert werden können, dass zunächst nur pseudonymisierte Daten anfallen und ein Personenbezug erst dann herstellbar ist, wenn der Verursacher von Schutzverletzungen ermittelt werden muss.

Die Arbeiten waren erfolgreich. Die Wissenschaftler haben die Software „Pseudonymization With Conditional Reidentification“ (Pseudo/CoRe) entwickelt. Die Software pseudonymisiert einerseits die standardmäßig erzeugten Protokolldateien (z. B. Syslog). Ein Administrator kann diese Daten dann zwar verwenden, um das Verhalten eines IT-Systems zu analysieren und zu optimieren. Er kann den Nutzern aber keine einzelnen Aktivitäten aus den Protokolldaten zuordnen und somit nicht das individuelle Nutzerverhalten ausforschen. Andererseits ist es möglich, Missbrauchsfälle dennoch aufzudecken. Pseudo/CoRe depseudonymisiert die dafür erforderlichen Protokolldatensätze im Bedarfsfall automatisch. Dazu werden dem System vorab bestimmte Regeln vorgegeben. Diese bestimmen, welche Aktivitäten zulässig und welche als Missbrauchsversuch zu werten sind. Erst wenn

ein hinreichend großer Verdacht für eine Regelverletzung vorliegt, wird der entsprechende Protokolldatensatz mit Hilfe kryptographischer Algorithmen automatisch depseudonymisiert. Die Protokolldaten sind dann personenbeziehbar, so dass Angreifer ermittelt werden können.

Die Funktionsfähigkeit der Software wurde dem Arbeitskreis am Beispiel der Protokollierung von Login-Vorgängen demonstriert. In konventionellen Systemen werden die Login-Daten (etwa Kennung, Datum, Terminalnummer) unverschlüsselt und somit personenbezogen aufgezeichnet. Die Software ersetzt nun die personenbezogenen Merkmale durch kryptographisch erzeugte Pseudonyme. Ein Systemadministrator muss jedoch einen Personenbezug herstellen können, um Angriffe zu verfolgen, bei denen das Passwort erraten werden soll. Vertippt sich ein autorisierter Nutzer beim Eingeben des Passwortes ein- oder zweimal, wird dies nicht weiter untersucht. Für die Depseudonymisierung der Protokolle wurde daher die Regel vorgegeben, dass ein Angriff dann anzunehmen ist, wenn drei fehlerhafte Anmeldeversuche in Folge auftauchen. Nur in diesem Fall werden die Protokolldaten depseudonymisiert und der Administrator informiert. Er kann dann ermitteln, welches Nutzerkonto von welchem Terminal aus angegriffen wurde, und weitere Aktivitäten einleiten.

Die Wissenschaftler der Universität Dortmund haben nachgewiesen, dass die Software praxistauglich ist. So wurden die Syslog- und Web-Server-Audit-Daten eines zentralen Servers (Solaris SUN Ultra Enterprise 4000 mit sechs Ultra SPARC 168 MHz CPUs, 3 GB RAM und drei Platten Arrays mit insgesamt 396 GB) am Zentrum für Kommunikation und Informationsverarbeitung der Universität Dortmund ausgewertet. Während der Arbeitszeit sind von den 1.050 registrierten Nutzern durchschnittlich 25 Nutzer gleichzeitig aktiv. Daraus resultieren knapp 40.000 Audit-Datensätze pro Stunde. Der Durchsatz der Pseudonymisierungs-Software hat sich dabei als völlig ausreichend erwiesen.

Die Software ist bisher nicht am Markt verfügbar. Mit der Implementierung auf einem UNIX-System und dem Nachweis der Funktionsfähigkeit ist das Forschungsprojekt zunächst beendet. Da Pseudo/CoRe nach den gleichen Prinzipien wie Intrusion Detection Systeme (IDS) arbeitet, soll die Zusammenarbeit mit Forschungseinrichtungen intensiviert werden, die sich vorwiegend mit IDS befassen. Solche Systeme sind bereits als Produkte verfügbar. Deshalb ist zu hoffen, dass auch Pseudo/CoRe von derartigen Kooperationsbeziehungen profitiert und zu einem vermarktungsfähigen Produkt weiterentwickelt wird.

Aus datenschutzrechtlicher Sicht ist die Software nachdrücklich zu begrüßen. Es handelt sich um eine datenschutzfreundliche Technologie, die insbesondere geeignet ist, die Zweck-

bindung von Protokolldaten sicherzustellen. Pseudo/CoRe ist darüber hinaus ein Verfahren, dass den Anforderungen des § 5 Abs. 1 DSG M-V nach Datenvermeidung in besonderer Weise genügt, da von vornherein pseudonymisierte Daten verarbeitet werden und nur bei konkretem Missbrauchsverdacht ein Personenbezug herstellbar ist.

Details zur Software und zum gesamten Rahmenprojekt sind im Internetangebot der Universität Dortmund unter http://ls6-www.cs.uni-dortmund.de/pseudocore zu finden.

3. FORTSETZUNG VON THEMEN FRÜHERER TÄTIGKEITSBERICHTE

3.1 Auslegung von Wählerverzeichnissen bei Kommunalwahlen

Bisher wurden vor Wahlen die Wählerverzeichnisse öffentlich ausgelegt. Dadurch konnte jedermann ohne besonderen Anlass auch Namen und Adressen von Einwohnern erfahren, für die eine melderechtliche Auskunftssperre besteht, so dass diese Auskunftssperren praktisch unwirksam wurden.

Seit Ende 2001 können Wahlberechtigte bei Wahlen auf Landesebene nur noch dann das Wählerverzeichnis einsehen, wenn sie glaubhaft machen können, dass das Verzeichnis unrichtig oder unvollständig ist. Mit einer Auskunftssperre versehene Daten sind in jedem Fall von der Einsichtnahme ausgenommen (siehe Fünfter Tätigkeitsbericht, Punkt 4.7).

Am 15. Dezember 2003 ist eine entsprechende Änderung im Kommunalwahlgesetz in Kraft getreten. Danach werden künftig bei Kommunalwahlen ebenso wie bei Landtagswahlen die Wählerverzeichnisse nicht mehr öffentlich ausgelegt.

3.2 Noch immer rechtswidrige Datenerhebungen für die Hochbaustatistik

Seit mehr als vier Jahren werden personenbezogene Daten der Bauherren in formell und materiell rechtswidriger Weise für Zwecke der Hochbaustatistik erhoben. So erhalten die Bauaufsichtsbehörden beispielsweise statistische Einzeldaten der Bauherren, die sie für ihre Arbeit nicht benötigen (z. B. die Baukosten). Im Fünften Tätigkeitsbericht habe ich unter Punkt 3.8.2 die Rechtslage dargelegt und das Innenministerium unseres Landes um schnelle Abhilfe gebeten. Ende 2003 hat mir das Innenministerium mitgeteilt, dass das Ministerium für Arbeit, Bau und Landesentwicklung Mecklenburg-Vorpommern die erforderliche Rechtsverordnung federführend erarbeiten werde. Auf meine Nachfrage zum Zeitplan für den Erlass der Verordnung teilte mir das Bauministerium mit, es könne derzeit nicht beurteilen, wann das Verfahren zur Erstellung der Rechtsverordnung beendet sein wird.

Für mich ist nicht nachvollziehbar, warum sich das Verfahren so in die Länge zieht. Seit Februar 2001 liegt dem Innenministerium ein Entwurf für einen Erlass zur Durchführung der Hochbaustatistik vor, den das Statistische Landesamt mit mir abgestimmt hat. Der Inhalt dieses Entwurfes könnte sofort ohne große Änderungen in die geforderte Rechtsverordnung übernommen werden.

Im Interesse aller Bauherren ist zu hoffen, dass möglichst bald eine Rechtsverordnung verabschiedet wird, die eine datenschutzgerechte Erhebung ihrer Daten sicherstellt.

3.3 Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

Zur Nutzung von Internetdiensten am Arbeitsplatz habe ich schon im Fünften Tätigkeitsbericht unter Punkt 3.17.6 ausführliche Hinweise gegeben. Im März 2002 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Entschließung zu diesem Thema verabschiedet (siehe Anlage 3). Sie fordert darin unter anderem,

- die Arbeitsplätze mit Internetzugang so zu gestalten, dass keine oder möglichst wenige personenbezogene Daten erhoben werden,

- die Beschäftigten umfassend über die Nutzungsbedingungen des Internetzugangs und die Kontrollmöglichkeiten des Arbeitgebers zu informieren,

- die Protokollierung der Internetnutzung durch eine Dienstvereinbarung zu regeln und die dabei anfallenden Daten nicht zur Leistungs- und Verhaltenskontrolle zu verwenden,

- durch organisatorische und technische Maßnahmen sicherzustellen, dass der Arbeitgeber die Inhalte privater E-Mails nicht zur Kenntnis nehmen kann und

- dass der Bundesgesetzgeber endlich ein umfassendes Arbeitnehmerdatenschutzgesetz verabschiedet.

Die Entschließung verweist auf die Orientierungshilfe „ Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ des Arbeitskreises Medien der Datenschutzbeauftragten, welche detailliert die datenschutzrechtlichen Anforderungen an die Internetnutzung am Arbeitsplatz darstellt. Die Orientierungshilfe kann aus meinem Internetangebot unter http://www.lfd.m-v.de/informat/nutzuint/ nutzuint.pdf heruntergeladen werden.

4. ARBEITSKREIS „TECHNISCHE UND ORGANISATORISCHE DATENSCHUTZFRAGEN“ (AK TECHNIK)

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik) tagt als Gremium der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zweimal im Jahr. Er berät die Konferenz zu technischen Fragen des Datenschutzes und unterstützt die Beratungstätigkeit der Datenschutzbeauftragten beispielsweise mit entsprechendem Arbeitsmaterial.

Biometrische Verfahren waren in diesem Berichtszeitraum ein Schwerpunkt der Tätigkeit des AK Technik. Um beurteilen zu können, ob diese Verfahren zumindest aus technischer Sicht zur Bekämpfung des internationalen Terrorismus geeignet, erforderlich und angemessen sind (siehe Punkt 2.19.1), hat der Arbeitskreis im Frühjahr 2002 beim Fraunhofer Institut für graphische Datenverarbeitung in Darmstadt getagt. Die Wissenschaftler des Institutes informierten detailliert über den Stand der Technik und erläuterten die Wirkungsweise sowie Vor- und Nachteile einzelner biometrischer Erkennungssysteme. Im Ergebnis konnte der Arbeitskreis der Konferenz ein „Positionspapier zu technischen Aspekten biometrischer Merkmale in Personalausweisen und Pässen“ vorlegen und eine Entschließung zu biometrischen Merkmalen in Personalausweisen und Pässen vorbereiten (siehe Anlage 1).

Im September 2002 tagte der Arbeitskreis bei der Bundesdruckerei in Berlin. Die Mitarbeiter der Bundesdruckerei stellten verschiedene Einsatzszenarien für biometrische Identifikationssysteme vor und diskutierten mit den Arbeitskreismitgliedern die datenschutzrechtlichen Aspekte möglicher Anwendungen.

In seiner Sitzung im Frühjahr 2003 in Schwerin befasste sich der Arbeitskreis mit der Frage der Vertrauenswürdigkeit von Informationstechnik. Dabei spielten die Entwicklungen um TCPA und Palladium (siehe Punkt 2.18.3) eine zentrale Rolle. In einem detaillierten Positionspapier hat der Arbeitskreis die datenschutzrechtlichen Aspekte dieser Entwicklungen dargestellt. Auf der Basis dieses Papiers hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Entschließung verabschiedet (siehe Anlage 11).

Das Thema Vertrauenswürdigkeit war auch in anderen Zusammenhängen von Bedeutung. So hat der Arbeitskreis eine weitere Entschließung für die Konferenz vorbereitet, welche auf die Risiken automatischer Software-Updates hinweist (siehe Anlage 20). Sie enthält unter anderem Vorschläge, wie die Vertrauenswürdigkeit derartiger Prozesse verbessert werden kann. Die Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre hat im Herbst 2003 in Sydney das Thema aufgegriffen und ebenfalls eine Entschließung verabschiedet (http://www.privacyconference2003.org/commissioners.asp).

Schließlich befasste sich der AK Technik unter dem Stichwort Vertrauenswürdigkeit auch mit den Möglichkeiten der Prüfung und Zertifizierung von Produkten der Informationstechnik. Nach dem Abschluss der Arbeiten an einem so genannten Schutzprofil (siehe Punkt 2.18.2) will der AK Technik für die breite Nutzung dieses Schutzprofils in der öffentlichen Verwaltung werben. Um hierfür geeignete Wege zu finden, wurde zu einer Sitzung des Arbeitskreises ein Mitarbeiter des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eingeladen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt diese Aktivitäten des AK Technik. In einer Entschließung vom März 2003 beispielsweise fordert die Konferenz Anwender von IT-Produkten auf, ihre Sicherheitsanforderungen mit Hilfe dieser Schutzprofile selbst zu formulieren (siehe Anlage 12).

Im Herbst 2003 tagte der Arbeitskreis beim Bundesbeauftragten für den Datenschutz in Bonn. Schwerpunktthema dieser Sitzung war die elektronische Signatur. Vertreter des TeleTrusT Deutschland e. V. und der Regulierungsbehörde für Telekommunikation und Post (RegTP) waren eingeladen, um mit den Arbeitskreismitgliedern über den Stand der Technik in diesem Bereich zu diskutieren (siehe Punkt 2.16.3). Der AK Technik wollte sich auf diese Weise Informationen „aus erster Hand“ verschaffen, um öffentliche Stellen bei ihren E-Government-Projekten auch weiterhin kompetent beraten zu können. Während dieser Sitzung verabschiedete der Arbeitskreis die Orientierungshilfe zum Einsatz kryptographischer Verfahren (siehe Punkt 2.20.5). Das Papier wurde von einer Arbeitsgruppe des AK Technik erstellt und soll öffentliche Stellen ebenfalls mit Blick auf künftige E-Government-Projekte unterstützen.

Alle Publikationen des AK Technik sind in meinem Internetangebot veröffentlicht (http://www.lfd.m-v.de) und stehen auch im gemeinsamen Internetangebot der Datenschutzbeauftragten, dem so genannten Virtuellen Datenschutzbüro, unter http://www.datenschutz.de zum Abruf bereit.

5. ÖFFENTLICHKEITSARBEIT

Zahlreiche Petitionen und Anfragen im Berichtszeitraum belegen, dass es den Bürgerinnen und Bürgern unseres Landes nicht einerlei ist, wie mit ihren persönlichen Daten umgegangen wird. Sie erwarten, dass die öffentlichen Stellen ihre Daten ordnungsgemäß verarbeiten, dass sie nur die Daten angeben müssen, die auch benötigt werden, und sie bitten um Hinweise, wie sie sich in bestimmten Situationen verhalten sollen und sich auch selbst schützen können.

Eine häufig gefragte Informationsquelle sind nach wie vor die Broschüren, Faltblätter und Orientierungshilfen meiner Dienststelle zu ausgewählten datenschutzrechtlichen Themen (Übersicht siehe Punkt 9). Darüber hinaus enthält das Internetangebot (www.lfd.m-v.de) umfangreiche Informationen und auch Materialien zum Herunterladen. Über Links sind die Angebote meiner Kollegen von Bund und Ländern zugänglich. Empfehlenswert für interessierte Internetnutzer ist ebenfalls ein Besuch im so genannten Virtuellen Datenschutzbüro (www.datenschutz.de). Dabei handelt es sich um einen Service von deutschen und ausländischen Datenschützern, die Informationen rund um das Thema Datenschutz bereitstellen. Zum Service gehören Newsticker, Presseverteiler und Suchmaschine sowie die Möglichkeit des Mitdiskutierens in Mailinglists zu vielen Bereichen und das Beantworten der zahlreichen Fragen – ob per FAQ (Frequently Asked Questions) oder individuell per E-Mail.

Die „Tage der offenen Tür“ unseres Landtages sowie die „Mecklenburg-Vorpommern-Tage“ in Wismar und in Greifswald wurden genutzt, um direkt mit Bürgern ins Gespräch zu kommen. Viele Gäste nahmen diese Möglichkeit wahr. Am „Tag der offenen Tür“ im Jahre 2002 präsentierte sich meine Behörde anlässlich der „10 Jahre Datenschutz“ in unserem Bundesland in besonderer Weise. Unter anderem konnten die Besucher ihr Wissen zum Thema Datenschutz bei einem Quiz testen. Neben Informationen in Papierform gab es auch eine CD-ROM mit viel Wissenswertem zu rechtlichen und technischen Datenschutzfragen.

Der Bedarf vieler Institutionen an Vorträgen und anderen Veranstaltungen zu datenschutzrechtlichen Fragen ist nach wie vor sehr groß. Schwerpunktthema in den vergangenen zwei Jahren war das neue Landesdatenschutzgesetz (DSG M-V). So nutzten viele Mitarbeiter der öffentlichen Verwaltung, insbesondere die kommunalen Datenschutzbeauftragten, mein Angebot, sich über ihre Aufgaben und die Neuerungen im DSG M-V zu informieren. Den zwei zentralen Veranstaltungen im Land, die gemeinsam mit dem Landkreistag Mecklenburg-Vorpommern und dem Städte- und Gemeindetag Mecklenburg-Vorpommern organisiert wurden, folgten weitere Informationsveranstaltungen in verschiedenen Städten und Kommunen. Auch aus der Landesverwaltung kamen zahlreiche

Anfragen. Zusammen mit dem Justizministerium unseres Landes führten meine Mitarbeiter beispielsweise eine Tagesveranstaltung für behördliche Datenschutzbeauftragte im Bereich der Justiz durch.

Großen Zuspruch fand die von meiner Behörde herausgegebene Broschüre „Landesdatenschutzgesetz 2002 mit Erläuterungen“. Neben dem Gesetzestext enthält sie detaillierte Hinweise zu den einzelnen Vorschriften, insbesondere auch zum behördlichen Datenschutzbeauftragten, zum Verfahrensverzeichnis, zur Verarbeitung besonders sensibler Daten, zur Datenvermeidung und zu technischen Datenschutzaspekten. Die Broschüre kann kostenlos in meiner Dienststelle angefordert oder als elektronisches Dokument aus meinem Internetangebot heruntergeladen werden.

Ein weiterer Tätigkeitsschwerpunkt war das Thema „E-Government“. Die öffentliche Verwaltung möchte möglichst viele Dienstleistungen auch im Internet anbieten, um so ihre Aufgaben besser und schneller im Interesse der Bürgerinnen und Bürger erfüllen zu können. Die Datenschutzbeauftragten des Bundes und der Länder haben eine Broschüre herausgegeben, die über den richtigen Umgang mit E-Government informiert (siehe auch Punkt 2.16.2). Sie beschreibt die Anforderungen und Risiken und liefert konkrete Empfehlungen sowie einen Katalog beispielhafter datenschutzfreundlicher Lösungen. Die Broschüre richtet sich nicht nur an Entscheidungsträger in der Verwaltung, sondern auch an Bürgerinnen und Bürger sowie Wirtschaftsunternehmen, welche die Angebote des E-Government nutzen (möchten). Die Broschüre „Datenschutzgerechtes E-Government“ kann ebenfalls kostenlos in meiner Behörde bestellt oder der Text im Internet abgerufen werden.

Aber auch zu vielen weiteren Themen führten meine Mitarbeiter Schulungen und Beratungen durch, hielten Vorträge oder gestalteten Diskussionsrunden. Ob technische und organisatorische Datenschutzfragen in der Verwaltung, Personal- und Sozialdatenschutz bei der AWO oder anderen Trägern sozialer Belange – die Palette der Themen war breit. Die Zusammenarbeit mit den Hochschulen des Landes wurde weiter intensiviert. Auch in diesem Berichtszeitraum konnten Informatikstudenten Praktika in meiner Dienststelle absolvieren. Meine Mitarbeiter betreuten Beleg- und Diplomarbeiten und hielten Vorlesungen zu Grundsätzen des Datenschutzes und der Datensicherheit. Da insbesondere Beratungen im Vorfeld neuer Datenverarbeitungsverfahren Mängel vermeiden helfen, werden wir auch weiterhin dem großen Informationsbedarf vor Ort nachkommen.

Künftig werden die Bürgerinnen und Bürger noch mehr Eigenverantwortung zur Wahrnehmung der eigenen datenschutzrechtlichen Belange zeigen müssen. Das setzt allerdings

die Kenntnis über die Verarbeitung der personenbezogenen Daten, also die Transparenz der Verfahren, und auch das Wissen um die rechtlichen Möglichkeiten voraus. In diesem Sinne werde ich auch weiterhin meine Öffentlichkeitsarbeit ausrichten, um so dem Grundrecht auf informationelle Selbstbestimmung in unserem Land angemessen Geltung zu verschaffen.

6. ANLAGEN

1. Anlage: Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7./8. März 2002 in Mainz

Biometrische Merkmale in Personalausweisen und Pässen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eingehend über Geeignetheit, Erforderlichkeit und Angemessenheit der beabsichtigten Einführung biometrischer Merkmale in Ausweisen und Pässen diskutiert. Sie hat ein Positionspapier des Arbeitskreises Technik, das detaillierte Prüfpunkte für die Erprobungsphase einer solcher Maßnahme nennt, zustimmend zur Kenntnis genommen. Für den Fall, dass das Vorhaben trotz noch bestehender Bedenken realisiert werden sollte, hat sie übereinstimmend folgende Anforderungen formuliert:

1. Fälschliche Zurückweisungen berechtigter Personen durch automatisierte Personenerkennungssysteme sind auch bei ständiger Verbesserung der Technik prinzipiell nicht zu vermeiden. Es dürfen deshalb nur Verfahren in Betracht gezogen werden, bei denen die Fehlerquote zumutbar gering ist. In Fehlerfällen muss dafür Sorge getragen werden, dass eine die Betroffenen nicht diskriminierende rasche Aufklärung erfolgt.

2. Zu berücksichtigen ist, dass bei der Anwendung biometrischer Verfahren Zusatzinformationen anfallen können (z. B. Krankheits-, Unfall-, Beschäftigungsindikatoren). Es muss sichergestellt werden, dass die gespeicherten und verarbeiteten Daten keine Rückschlüsse auf zusätzliche personenbezogene Merkmale erlauben.

3. Systeme, die biometrische Daten aus Ausweisen ohne Kenntnis der Betroffenen verarbeiten (sog. passive Systeme), sind abzulehnen.

4. Der Gesetzgeber hat die Verwendung biometrischer Daten in Ausweisen und Pässen grundsätzlich auf die Feststellung beschränkt, dass die dort gespeicherten Daten mit den Merkmalen der jeweiligen Ausweisinhaber und -inhaberinnen übereinstimmen; dies muss erhalten bleiben. Die Verwendung der biometrischen Merkmale für andere öffentliche Zwecke (außer der gesetzlich zugelassenen Verwendung aus dem Fahndungsbestand) wie auch für privatrechtliche Zwecke (Versicherung, Gesundheitssystem) ist auszuschließen. Deshalb hat der Gesetzgeber zu Recht die Einrichtung zentraler Dateien ausgeschlossen. Diese gesetzgeberische Entscheidung darf nicht durch den Aufbau dezentraler Dateien umgangen werden.

5. Die Entscheidung über das auszuwählende biometrische Erkennungssystem verlangt ein abgestimmtes europäisches Vorgehen.

siehe Anlage:
Positionspapier zu technischen Aspekten biometrischer Merkmale in Personalausweisen und Pässen (unter http://www.lfd.m-v.de/beschlue/63biomet.html)

2. Anlage: Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7./8. März 2002 in Mainz

Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikationsdiensten

Mit der rasch wachsenden Nutzung des Internet kommt dem datenschutzgerechten Umgang mit den dabei anfallenden Daten der Nutzerinnen und Nutzer immer größere Bedeutung zu. Die Datenschutzbeauftragten haben bereits in der Vergangenheit (Entschließung der 59. Konferenz „Für eine freie Telekommunikation in einer freien Gesellschaft“) darauf hingewiesen, dass das Telekommunikationsgeheimnis eine unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft ist. Seine Geltung erstreckt sich auch auf Multimedia- und E-Mail-Dienste.

Die Datenschutzbeauftragten betonen, dass das von ihnen geforderte in sich schlüssige System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt, nach wie vor fehlt. Die Strafprozessordnung (und seit dem 01.01.2002 das Recht der Nachrichtendienste) enthält ausreichende Befugnisse, um den Strafverfolgungsbehörden (und den Nachrichtendiensten) im Einzelfall den Zugriff auf bei den Anbietern vorhandene personenbezogene Daten zu ermöglichen. Für eine zusätzliche Erweiterung dieser Regelungen z. B. hin zu einer Pflicht zur Vorratsdatenspeicherung besteht nicht nur kein Bedarf, sondern eine solche Pflicht würde dem Grundrecht auf unbeobachtete Kommunikation nicht gerecht, weil damit jede Handlung (jeder Mausklick) im Netz staatlicher Beobachtung unterworfen würde.

In keinem Fall sind Anbieter von Tele-, Medien- und Telekommunikationsdiensten berechtigt oder verpflichtet, generell Daten über ihre Nutzerinnen und Nutzer auf Vorrat zu erheben, zu speichern oder herauszugeben, die sie zu keinem Zeitpunkt für eigene Zwecke (Herstellung der Verbindung, Abrechnung) benötigen. Sie können nur im Einzelfall berechtigt sein oder verpflichtet werden, bei Vorliegen ausdrücklicher gesetzlicher Voraussetzungen Nachrichteninhalte, Verbindungsdaten und bestimmte Daten (Nutzungsdaten), die sie ursprünglich für eigene Zwecke benötigt haben und nach den Bestimmungen des Multimedia-Datenschutzrechts löschen müssten, den Strafverfolgungsbehörden (oder Nachrichtendiensten) zu übermitteln.

3. Anlage: Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7./8. März 2002 in Mainz

Entschließung zur datenschutzgerechten Nutzung von E-MaiI und anderen Internet-Diensten am Arbeitsplatz

Immer mehr Beschäftigte erhalten die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten und ihrer Kommunikationspartner bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben der dienstlichen die private Nutzung des Internet am Arbeitsplatz gestattet wird. Der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat detaillierte Hinweise hierzu erarbeitet.

Insbesondere gilt Folgendes:

1. Die Arbeitsplätze mit Internet-Zugang sind so zu gestalten, dass keine oder möglichst wenige personenbezogene Daten erhoben werden. Die Nutzung des Internet am Arbeitsplatz darf nicht zu einer vollständigen Kontrolle der Bediensteten führen. Präventive Maßnahmen gegen eine unbefugte Nutzung sind nachträglichen Kontrollen vorzuziehen.

2. Die Beschäftigten sind umfassend darüber zu informieren, für welche Zwecke sie einen Internet-Zugang am Arbeitsplatz nutzen dürfen und auf welche Weise der Arbeitgeber die Einhaltung der Nutzungsbedingungen kontrolliert.

3. Fragen der Protokollierung und einzelfallbezogenen Überprüfung bei Missbrauchsverdacht sind durch Dienstvereinbarungen zu regeln. Die Kommunikation von schweigepflichtigen Personen und Personalvertretungen muss vor einer Überwachung grundsätzlich geschützt bleiben.

4. Soweit die Protokollierung der Internet-Nutzung aus Gründen des Datenschutzes, der Datensicherheit oder des ordnungsgemäßen Betriebs der Verfahren notwendig ist, dürfen die dabei anfallenden Daten nicht zur Leistungs- und Verhaltenskontrolle verwendet werden.

5. Wird den Beschäftigten die private E-Mail-Nutzung gestattet, so ist diese elektronische Post vom Telekommunikationsgeheimnis geschützt. Der Arbeitgeber darf ihren Inhalt grundsätzlich nicht zur Kenntnis nehmen und hat dazu die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen.

6. Der Arbeitgeber ist nicht verpflichtet, die private Nutzung des Internet am Arbeitsplatz zu gestatten. Wenn er dies gleichwohl tut, kann er die Gestattung unter Beachtung der hier genannten Grundsätze davon abhängig machen, dass die Beschäftigten einer Protokollierung zur Durchführung einer angemessenen Kontrolle der Netzaktivitäten zustimmen.

7. Die gleichen Bedingungen wie bei der Nutzung des Internet müssen prinzipiell bei der Nutzung von Intranets gelten.

Die Datenschutzbeauftragten fordern den Bundesgesetzgeber auf, auch wegen des Überwachungspotentials moderner Informations- und Kommunikationstechnik am Arbeitsplatz die Verabschiedung eines umfassenden Arbeitnehmerdatenschutzgesetzes nicht länger aufzuschieben.

siehe Anlage:
Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz (unter http://www.lfd.m-v.de/beschlue/63email.html)

4. Anlage: Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7./8. März 2002 in Mainz

Neues Abrufverfahren bei den Kreditinstituten

Nach der Novelle des Gesetzes über das Kreditwesen soll die zuständige Bundesanstalt die von den Kreditinstituten vorzuhaltenden Daten, wer welche Konten und Depots hat, ohne Kenntnis der Kundinnen und Kunden zur eigenen Aufgabenerfüllung oder zu Gunsten anderer öffentlicher Stellen abrufen können. Dies ist ein neuer Eingriff in die Vertraulichkeit der Bankbeziehungen.

Dieser Eingriff in die Vertraulichkeit der Bankbeziehungen muss gegenüber den Kundinnen und Kunden zumindest durch eine aussagekräftige Information transparent gemacht werden. Die Konferenz fordert daher, dass zugleich mit der Einführung dieses Abrufverfahrens eine Verpflichtung der Kreditinstitute zur generellen Information der Kundinnen und Kunden vorgesehen wird und diese die Kenntnisnahme schriftlich bestätigen. Dadurch soll zugleich eine effektive Wahrnehmung des Auskunftsrechts der Kundinnen und Kunden gewährleistet werden.

Die Erweiterung der Pflichten der Kreditinstitute, Kontenbewegungen auf die Einhaltung gesetzlicher Bestimmungen mit Hilfe von EDV-Programmen zu überprüfen, verpflichtet die Kreditinstitute außerdem zu einer entsprechend intensiven Kontenüberwachung (sog. „know your customer principle“). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass die Überprüfung in einer Weise stattfindet, die ein datenschutzkonformes Vorgehen sicherstellt.

5. Anlage: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 24. Mai 2002

Geplanter Identifikationszwang in der Telekommunikation

Das Bundesministerium für Wirtschaft und Technologie hat einen Entwurf zur Änderung des Telekommunikationsgesetzes veröffentlicht. Der Entwurf hat das Ziel, jeden Anbieter, der geschäftsmäßig Telekommunikationsdienste erbringt, dazu zu verpflichten, Namen, Anschriften, Geburtsdaten und Rufnummern seiner Kundinnen und Kunden zu erheben. Die Kundinnen und Kunden werden verpflichtet, dafür ihren Personalausweis vorzulegen, dessen Nummer ebenfalls gespeichert werden soll. Die beabsichtigten Änderungen sollen in erster Linie dazu führen, auch Nutzerinnen und Nutzer von Prepaid-Karten (also die Erwerberinnen und Erwerber von SIM-Karten ohne Vertrag) im Mobilfunk erfassen zu können. Die erhobenen Daten sollen allein dem Zweck dienen, den Sicherheitsbehörden zum jederzeitigen Online-Abruf über die Regulierungsbehörde für Telekommunikation und Post bereitzustehen. Im gleichen Zuge sollen die Zugriffsmöglichkeiten der Sicherheitsbehörden auf diese Daten dadurch erheblich erweitert werden, indem auf die Kundendateien nach abstrakten Merkmalen zugegriffen werden kann.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen dieses Vorhaben ab. Unter der unscheinbaren Überschrift „Schließen von Regelungslücken“ stehen grundlegende Prinzipien des Datenschutzes zur Disposition. Kritikwürdig an dem geplanten Gesetz sind insbesondere die folgenden Punkte:

- Der geplante Grundrechtseingriff ist nicht erforderlich, um die Ermittlungstätigkeit der Sicherheitsbehörden zu erleichtern. Seine Eignung ist zweifelhaft: Auch die Gesetzesänderung wird nicht verhindern, dass Straftäterinnen und Straftäter bewusst und gezielt in kurzen Zeitabständen neue Prepaid-Karten erwerben, Strohleute zum Erwerb einsetzen, die Karten häufig – teilweise nach jedem Telefonat – wechseln oder die Karten untereinander tauschen. In der Begründung wird nicht plausibel dargelegt, dass mit dem geltenden Recht die Ermittlungstätigkeit tatsächlich behindert und durch die geplante Änderung erleichtert wird. Derzeit laufende Forschungsvorhaben beziehen diese Frage nicht mit ein.

- Der Entwurf widerspricht auch dem in den Datenschutzrichtlinien der Europäischen Union verankerten Grundsatz, dass Unternehmen nur solche personenbezogenen Daten verarbeiten dürfen, die sie selbst zur Erbringung einer bestimmten Dienstleistung benötigen.

- Die Anbieter würden eine Reihe von Daten auf Vorrat speichern müssen, die sie selbst für den Vertrag mit ihren Kunden nicht benötigen. Die ganz überwiegende Zahl der Nutzerinnen und Nutzer von Prepaid-Karten, darunter eine große Zahl Minderjähriger, würde registriert, obwohl sie sich völlig rechtmäßig verhalten und ihre Daten demzufolge für die Ermittlungstätigkeit der Strafverfolgungsbehörden nicht benötigt werden. Das Anhäufen von sinn- und nutzlosen Datenhalden wäre die Folge.

- Die gesetzliche Verpflichtung, sich an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten, würde konterkariert. Gerade die Prepaid-Karten sind ein gutes praktisches Beispiel für den Einsatz datenschutzfreundlicher Technologien, da sie anonymes Kommunizieren auf unkomplizierte Weise ermöglichen. Die Nutzung dieser Angebote darf deshalb nicht von der Speicherung von Bestandsdaten abhängig gemacht werden.

- Mit der Verpflichtung, den Personalausweis vorzulegen, würden die Anbieter zusätzliche Informationen über die Nutzerinnen und Nutzer erhalten, die sie nicht benötigen, z. B. die Nationalität, Größe oder Augenfarbe. Die vorgesehene Pflicht, auch die Personalausweisnummern zu registrieren, darf auch künftig keinesfalls dazu führen, dass die Ausweisnummern den Sicherheitsbehörden direkt zum Abruf bereitgestellt werden und sie damit diese Daten auch für die Verknüpfung mit anderen Datenbeständen verwenden können.

- Auch Krankenhäuser, Hotels, Schulen und Hochschulen sowie Unternehmen und Behörden, die ihren Mitarbeiterinnen und Mitarbeitern das private Telefonieren gestatten, sollen verpflichtet werden, die Personalausweisnummern der Nutzerinnen und Nutzer zu registrieren.

- Die Befugnis, Kundendateien mit unvollständigen oder ähnlichen Suchbegriffen abzufragen, würde den Sicherheitsbehörden eine Vielzahl personenbezogener Daten unbeteiligter Dritter zugänglich machen, ohne dass diese Daten für ihre Aufgaben erforderlich sind. Die notwendige strikte Beschränkung dieser weitreichenden Abfragebefugnis durch Rechtsverordnung setzt voraus, dass ein entsprechender Verordnungsentwurf bei der Beratung des Gesetzes vorliegt.

Der Formulierungsvorschlag des Bundeswirtschaftsministeriums lässt eine Auseinandersetzung mit dem Recht auf informationelle Selbstbestimmung der Kundinnen und Kunden der Telekommunikationsunternehmen weitgehend vermissen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Gesetzgeber auf, auf die geplante Änderung des Telekommunikationsgesetzes zu verzichten und vor weiteren Änderungen die bestehenden Befugnisse der Sicherheitsbehörden durch unabhängige Stellen evaluieren zu lassen.

6. Anlage: Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 24./25. Oktober 2002 in Trier

Entschließung zur systematischen verdachtslosen Datenspeicherung in der Telekommunikation und im Internet

Gegenwärtig werden sowohl auf nationaler als auch auf europäischer Ebene Vorschläge erörtert, die den Datenschutz im Bereich der Telekommunikation und der Internetnutzung und insbesondere den Schutz des Telekommunikationsgeheimnisses grundlegend in Frage stellen.

Geplant ist, alle Anbieter von Telekommunikations- und Multimediadiensten zur verdachtslosen Speicherung sämtlicher Bestands-, Verbindungs-, Nutzungs- und Abrechnungsdaten auf Vorrat für Mindestfristen von einem Jahr und mehr zu verpflichten, auch wenn sie für die Geschäftszwecke der Anbieter nicht (mehr) notwendig sind. Das so entstehende umfassende Datenreservoir soll dem Zugriff der Strafverfolgungsbehörden, der Polizei und des Verfassungsschutzes bei möglichen Anlässen in der Zukunft unterliegen. Auch auf europäischer Ebene werden im Rahmen der Zusammenarbeit der Mitgliedsstaaten in den Bereichen „Justiz und Inneres“ entsprechende Maßnahmen – allerdings unter weitgehendem Ausschluss der Öffentlichkeit – diskutiert.

Die Datenschutzbeauftragten des Bundes und der Länder treten diesen Überlegungen mit Entschiedenheit entgegen. Sie haben schon mehrfach die Bedeutung des Telekommunikationsgeheimnisses als unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft hervorgehoben. Immer mehr menschliche Lebensäußerungen finden heute in elektronischen Netzen statt. Sie würden bei einer Verwirklichung der genannten Pläne einem ungleich höheren Überwachungsdruck ausgesetzt als vergleichbare Lebensäußerungen in der realen Welt. Bisher muss niemand bei der Aufgabe eines einfachen Briefes im Postamt seinen Personalausweis vorlegen oder in einer öffentlichen Bibliothek registrieren lassen, welche Seite er in welchem Buch aufschlägt. Eine vergleichbar umfassende Kontrolle entsprechender Online-Aktivitäten (E-Mail-Versand, Nutzung des World Wide Web), wie sie jetzt erwogen wird, ist ebensowenig hinnehmbar.

Zudem hat der Gesetzgeber erst vor kurzem die Befugnisse der Strafverfolgungsbehörden erneut deutlich erweitert. Die praktischen Erfahrungen mit diesen Regelungen sind von unabhängiger Seite zu evaluieren, bevor weitergehende Befugnisse diskutiert werden.

Die Konferenz der europäischen Datenschutzbeauftragten hat in ihrer Erklärung vom 11. September 2002 betont, dass eine flächendeckende anlassunabhängige Speicherung sämtlicher Daten, die bei der zunehmenden Nutzung von öffentlichen Kommunikationsnetzen entstehen, unverhältnismäßig und mit dem Menschenrecht auf Achtung des Privatlebens unvereinbar wäre. Auch in den Vereinigten Staaten sind vergleichbare Maßnahmen nicht vorgesehen.

Mit dem deutschen Verfassungsrecht ist eine verdachtslose routinemäßige Speicherung sämtlicher bei der Nutzung von Kommunikationsnetzen anfallender Daten auf Vorrat nicht zu vereinbaren. Auch die Rechtsprechung des Europäischen Gerichtshofs lässt eine solche Vorratsspeicherung aus Gründen bloßer Nützlichkeit nicht zu.

Die Konferenz fordert die Bundesregierung deshalb auf, für mehr Transparenz der Beratungen auf europäischer Regierungsebene einzutreten und insbesondere einer Regelung zur flächendeckenden Vorratsdatenspeicherung nicht zuzustimmen.

7. Anlage: Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 24./25. Oktober 2002 in Trier

Elektronisches Fahrgeldmanagement (EFM)

Datenschutzrechtliche Grundanforderungen

1. Transparenz
Die Datenverarbeitung durch das EFM muss transparent sein (§ 6 c Abs. 1 Nr. 2 und 3 BDSG). Dies erfordert die

- Festlegung der Zwecke,

- Beschreibung der einzelnen Datenverarbeitungsvorgänge differenziert nach den jeweiligen für den Fahrgast zutreffenden Geschäftsprozessen und den dabei zu verarbeitenden Daten,

- Angaben der Identitäten und Anschriften der Stellen, die zu den genannten Zwecken personenbezogene Daten verarbeiten und/oder bei denen die jeweiligen Rechtsansprüche geltend gemacht und Verfahrensbeschreibungen gemäß § 4g Abs. 2 Satz 2 BDSG eingesehen werden können,

- Einbeziehung der Unterrichtungspflichten der Kundenvertragspartner. Dazu sollte ein Merk- oder Informationsblatt erstellt werden, in dem der Fahrgast in allgemein verständlicher Form über die vorgesehene Datenverarbeitung – auch durch zentrale Servicestellen oder andere autorisierte Dritte – und über seine Rechte nach §§ 34, 35 BDSG unterrichtet wird.

2. Widerspruchsrecht
Der Verband der Deutschen Verkehrsunternehmen sollte mit seinen Kundenvertragspartnern verabreden, dass der Kunde bei Vertragsabschluss schriftlich erklärt, ob er der Übermittlung oder Nutzung seiner Daten zu Zwecken der Werbung und der Markt- und Meinungsforschung widersprechen möchte oder nicht. Es ist sicherzustellen, dass auch autorisierte Dritte diese Beschränkung beachten.

3. Wahlmöglichkeit
Den Fahrgästen muss nach Information über die vertraglich bedingte Datenverarbeitung eine freie Entscheidung zwischen anonymer Fahrt und besonderen Leistungsangeboten (bspw. best pricing) überlassen bleiben.

4. Datensparsamkeit
Alle Leistungsmerkmale und Geschäftsprozesse sind nach dem Prinzip der Datenvermeidung und Datensparsamkeit (§ 3 a BDSG) zu gestalten. Insbesondere ist auszuschließen, dass kundenbezogene Bewegungsprofile erstellt werden. Das bedeutet:

- Daten für Planungszwecke und zur Optimierung des Angebots sind anonym zu erheben oder zu anonymisieren;

- soweit Daten für besondere Leistungsangebote oder das Reklamationsmanagement benötigt werden, sind diese pseudonym zu erheben und zu speichern, so dass ohne Wissen und Wollen des betroffenen Fahrgastes eine Zuordnung zu seiner Person ausgeschlossen ist;

- werden zu Zwecken des Reklamationsmanagements nutzungsbezogene Daten auf mobile Speichermedien (Chipkarte) geschrieben, muss es dem Fahrgast ermöglicht werden, diese Daten auf eigene Verantwortung zu löschen.

5. Getrennte Verarbeitung
Es müssen die jeweils erforderlichen technischen und organisatorischen Maßnahmen getroffen werden, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Nr. 8 der Anlage zu § 9 BDSG).

6. Zweckbindung der Ticketdaten
Darüber hinaus dürfen keine kunden- oder kartenbezogenen Auswertungen zu fremden Zwecken erfolgen. Zu Abrechnungszwecken im Verkehrsverbund dürfen allenfalls (pseudonyme) kartenbezogene Daten übermittelt werden.

7. Vorabkontrolle
Von dem oder der betrieblichen Datenschutzbeauftragten ist vor Inbetriebnahme des EFM eine Vorabkontrolle durchzuführen (§ 4 d Abs. 5 und 6 BDSG) und zu dokumentieren.

8. Zugriffsberechtigung
Der Lesezugriff für Kontrollpersonal muss auf die zur Kontrolle notwendigen Daten beschränkt sein, insbesondere auf dem Speichermedium des Fahrgastes.

9. Datenschutzgerechte Gestaltung der Systemkomponenten
Die Systemkomponenten, die von Fahrgästen bedient werden, sind datenschutzgerecht so zu gestalten, dass

- keine Möglichkeit für Unbefugte besteht, an Terminals für bargeldlose Zahlung die Eingabedaten, insbesondere Authentifikationsdaten zur Kenntnis zu nehmen,

- Fehlermeldungen der Zugangs-Erfassungssysteme die Betroffenen nicht öffentlich diskriminieren,

- die Fahrgäste in angemessenem Umfang die Möglichkeit haben, den Inhalt der Chipkarte jederzeit auslesen zu können.

10. Schutz gegen Missbrauch
Es müssen Vorkehrungen (beispielsweise Sperrung, Verschlüsselung) getroffen werden, die den Fahrgast in angemessener Weise gegen missbräuchliche Verwendung der Daten durch Dritte bei Verlust des Speichermediums schützen.

11. Löschung
Die Dauer der für die bestimmte Geschäftsprozesse erfolgenden Speicherung personenbezogener Daten muss so kurz wie möglich sein. Für die jeweiligen Geschäftsprozesse sind Regelfristen für die Löschung der Daten festzulegen (§ 4e Satz 1 Nr. 7 BDSG). In den Terminals gespeicherte Daten sind nach erfolgreicher Datenübertragung an den Rechner des Kundenvertragspartners zu löschen.

8. Anlage: Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 24./25. Oktober 2002 in Trier

Speicherung und Veröffentlichung der Standortverzeichnisse von Mobilfunkantennen

Die Speicherung und die Veröffentlichung der Standortdaten von Mobilfunkantennen durch die Kommunen oder andere öffentliche Stellen stehen zurzeit in verstärktem Maße in der öffentlichen Diskussion. Mehrere kommunale Spitzenverbände haben sich diesbezüglich bereits an die jeweiligen Landesdatenschutzbeauftragten gewandt.

Unbeschadet bereits bestehender Landesregelungen und der Möglichkeit, Daten ohne Grundstücksbezug zu veröffentlichen, fordert die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder aufgrund der bundesweiten Bedeutung der Frage den Bundesgesetzgeber auf, im Rahmen einer immissionsschutzrechtlichen Regelung über die Erstellung von Mobilfunkkatastern zu entscheiden. Dabei ist zu bestimmen, wie derartige Kataster erstellt werden sollen. Die gegenwärtige Regelung des Bundesimmissionsschutzgesetzes sieht keine ausdrückliche Ermächtigung zur Schaffung von Mobilfunkkatastern vor, so dass deren Erstellung und Veröffentlichung ohne Einwilligung der Grundstückseigentümer und -eigentümerinnen und der Antennenbetreiber keine ausdrückliche gesetzliche Grundlage hat. Bei der Novellierung ist insbesondere zu regeln, ob und unter welchen Bedingungen eine Veröffentlichung derartiger Kataster im Internet oder in vergleichbaren Medien zulässig ist. Individuelle Auskunftsansprüche nach dem Umweltinformationsgesetz oder den Informationsfreiheitsgesetzen bleiben davon unberührt.

9. Anlage: Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 24./25. Oktober 2002 in Trier

Entschließung zur datenschutzgerechten Vergütung für digitale Privatkopien im neuen Urheberrecht

Zur Umsetzung der EU-Urheberrechtsrichtlinie wird gegenwärtig über den Entwurf der Bundesregierung für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft beraten. Hierzu hat der Bundesrat die Forderung erhoben, das bisherige System der Pauschalabgaben auf Geräte und Kopiermedien, die von den Verwertungsgesellschaften auf die Urheberinnen und Urheber zur Abgeltung ihrer Vergütungsansprüche verteilt werden, durch eine vorrangige individuelle Lizenzierung zu ersetzen. Zugleich hat der Bundesrat die Gewährleistung eines ausreichenden Schutzes der Nutzerinnen und Nutzer vor Ausspähung personenbezogener Daten über die individuelle Nutzung von Werken und die Erstellung von Nutzungsprofilen gefordert.

Die Datenschutzbeauftragten des Bundes und der Länder weisen in diesem Zusammenhang auf Folgendes hin: Das gegenwärtig praktizierte Verfahren der Pauschalvergütung beruht darauf, dass der Bundesgerichtshof eine individuelle Überprüfung des Einsatzes von analogen Kopiertechniken durch Privatpersonen zur Durchsetzung von urheberrechtlichen Vergütungsansprüchen als unvereinbar mit dem verfassungsrechtlichen Schutz der persönlichen Freiheitsrechte der Nutzerinnen und Nutzer bezeichnet hat. Diese Feststellung behält auch unter den Bedingungen der Digitaltechnik und des Internet ihre Berechtigung. Die Datenschutzkonferenz bestärkt den Gesetzgeber, an diesem bewährten, datenschutzfreundlichen Verfahren festzuhalten. Sollte der Gesetzgeber – wie es der Bundesrat fordert – jetzt für digitale Privatkopien vom Grundsatz der Pauschalvergütung (Geräteabgabe) tatsächlich abgehen wollen, so kann er den verfassungsrechtlichen Vorgaben nur entsprechen, wenn er sicherstellt, dass die urheberrechtliche Vergütung aufgrund von statistischen oder anonymisierten Angaben über die Nutzung einzelner Werke erhoben wird. Auch technische Systeme zur digitalen Verwaltung digitaler Rechte (Digital Rights Management) müssen datenschutzfreundlich gestaltet werden.

10. Anlage: Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 in Dresden

Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Bundesgesetzgeber und Bundesregierung

Immer umfassendere Datenverarbeitungsbefugnisse, zunehmender Datenhunger sowie immer weitergehende technische Möglichkeiten zur Beobachtung und Durchleuchtung der Bürgerinnen und Bürger zeichnen den Weg zu immer mehr Registrierung und Überwachung vor. Das Grundgesetz gebietet dem Staat, dem entgegenzutreten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, das Recht auf informationelle Selbstbestimmung der Bürger und Bürgerinnen, wie in den Verfassungen zahlreicher deutscher Länder und in den Vorschlägen des Europäischen Verfassungskonvents, als eigenständiges Grundrecht im Grundgesetz zu verankern.

Die Datenschutzbeauftragten werden Bundesgesetzgeber und Bundesregierung bei der Weiterentwicklung des Datenschutzes unterstützen. Sie erwarten, dass die in der Koalitionsvereinbarung enthaltenen Absichtserklärungen zur umfassenden Reform des Datenschutzrechtes in der laufenden Legislaturperiode zügig verwirklicht werden.

Sie sehen dabei folgende essentielle Punkte:

Schwerpunkte für eine Modernisierung des Bundesdatenschutzgesetzes

- Im Vordergrund muss die Stärkung der informationellen Selbstbestimmung und des Selbstdatenschutzes stehen: Jeder Mensch muss tatsächlich selbst entscheiden können, welche Datenspuren er hinterlässt und wie diese Datenspuren verwertet werden. Ausnahmen müssen so gering wie möglich gehalten und stets in einer präzise formulierten gesetzlichen Regelung festgeschrieben werden.

- Es muss im Rahmen der gegebenen Strukturunterschiede ein weitgehend gleichmäßiges Schutzniveau für den öffentlichen und den nichtöffentlichen Bereich gelten. Die Einwilligung in die Datenverarbeitung darf nicht zur Umgehung gesetzlicher Aufgaben- und Befugnisgrenzen missbraucht werden.

- Die Freiwilligkeit der Einwilligung muss gewährleistet sein.

- Vor der Nutzung von Daten für Werbezwecke muss die informierte und freie Einwilligung der Betroffenen vorliegen („opt in“ statt „opt out“).

Technischer Datenschutz
Wesentliche Ziele des technischen Datenschutzes müssen darin bestehen, ein hohes Maß an Transparenz bei der Datenverarbeitung zu erreichen und den System- und Selbstdatenschutz zu stärken. Hersteller und Anbieter müssen verpflichtet werden, den Nutzerinnen und Nutzern die geeigneten Mittel zur Geltendmachung ihrer Rechte auch auf technischem Wege zur Verfügung zu stellen.

Realisierung von Audit und Gütesiegel als marktwirtschaftliche Elemente im Datenschutz
Bislang ist das Datenschutzrecht in Deutschland in erster Linie als Ordnungsrecht ausgestaltet. Seine Einhaltung soll durch Kontrolle, Kritik und Beanstandung durchgesetzt werden. Dagegen fehlen Anreize für Firmen und Behörden, vorbildliche Datenschutzkonzepte zu verwirklichen. Mit dem Datenschutzaudit könnte Firmen und Behörden ein gutes Datenschutzkonzept bestätigt werden, und es würde ihnen die Möglichkeit eröffnen, damit zu werben. Das Gütesiegel ist ein Anreiz, IT-Produkte von vornherein datenschutzgerecht zu gestalten und damit Marktvorteile zu erringen.

Eine datenschutzkonforme Technikgestaltung ist eine wichtige Voraussetzung für einen effizienten Datenschutz. Audit und Gütesiegel würden die Aufmerksamkeit auf das Thema Datenschutz lenken und so die stärkere Einbeziehung von Kundinnen und Kunden fördern. Deshalb müssen die noch ausstehenden gesetzlichen Regelungen zur Einführung des im Bundesdatenschutzgesetz vorgesehenen Datenschutzaudits umgehend geschaffen werden.

Förderung von datenschutzgerechter Technik
Die Verwirklichung des Grundrechtsschutzes hängt nicht allein von Gesetzen ab. Auch die Gestaltung der Informationstechnik hat großen Einfluss auf die Möglichkeit für alle Menschen, ihr Recht auf informationelle Selbstbestimmung auszuüben. Bislang spielt das Thema Datenschutz bei den öffentlichen IT-Entwicklungsprogrammen allenfalls eine untergeordnete Rolle. Neue IT-Produkte werden nur selten unter dem Blickwinkel entwickelt, ob sie datenschutzgerecht, datenschutzfördernd oder wenigstens nicht datenschutzgefährdend sind.

Notwendig ist, dass Datenschutz zu einem Kernpunkt im Anforderungsprofil für öffentliche IT-Entwicklungsprogramme wird.

Datenschutzgerechte Technik stellt sich nicht von alleine ein, sondern bedarf auch der Förderung durch Anreize. Neben der Entwicklung von Schutzprofilen und dem Angebot von Gütesiegeln kommt vor allem die staatliche Forschungs- und Entwicklungsförderung in Betracht. Die Entwicklung datenschutzgerechter Informationstechnik muss zu einem Schwerpunkt staatlicher Forschungsförderung gemacht werden.

Anonyme Internetnutzung

Das Surfen im World Wide Web mit seinen immensen Informationsmöglichkeiten und das Versenden von E-mails sind heute für viele selbstverständlich. Während aber in der realen Welt jeder Mensch zum Beispiel in einem Buchladen stöbern oder ein Einkaufszentrum durchstreifen kann, ohne dass sein Verhalten registriert wird, ist dies im Internet nicht von vornherein gewährleistet. Dort kann jeder Mausklick personenbezogene Datenspuren erzeugen, deren Summe zu einem aussagekräftigen Persönlichkeitsprofil und für vielfältige Zwecke (z. B. Marketing, Auswahl unter Stellenbewerbungen, Observation von Personen) genutzt werden kann. Das Recht auf Anonymität und der Schutz vor zwangsweiser Identifizierung sind in der realen Welt gewährleistet (in keiner Buchhandlung können Kundinnen und Kunden dazu gezwungen werden, einen Ausweis vorzulegen). Sie werden aber im Bereich des Internet durch Pläne für eine umfassende Vorratsspeicherung von Verbindungs- und Nutzungsdaten bedroht.

Das Recht jedes Menschen, das Internet grundsätzlich unbeobachtet zu nutzen, muss geschützt bleiben. Internet-Provider dürfen nicht dazu verpflichtet werden, auf Vorrat alle Verbindungs- und Nutzungsdaten über den betrieblichen Zweck hinaus für mögliche zukünftige Strafverfahren oder geheimdienstliche Observationen zu speichern.

Unabhängige Evaluierung der Eingriffsbefugnisse der Sicherheitsbehörden

Schon vor den Terroranschlägen des 11. September 2001 standen den deutschen Sicherheitsbehörden nach einer Reihe von Antiterrorgesetzen und Gesetzen gegen die Organisierte Kriminalität weitreichende Eingriffsbefugnisse zur Verfügung, die Datenschutzbeauftragten und Bürgerrechtsorganisationen Sorgen bereiteten. Dies zeigen Videoüberwachung, Lauschangriff, Rasterfahndung, langfristige Aufbewahrung der Daten bei der Nutzung des Internet und der Telekommunikation, Zugriff auf Kundendaten und Geldbewegungen bei den Banken.

Durch die jüngsten Gesetzesverschärfungen nach den Terroranschlägen des 11. September 2001 sind die Freiräume für unbeobachtete individuelle oder gesellschaftliche Aktivitäten und Kommunikation weiter eingeschränkt worden. Bürgerliche Freiheitsrechte und Datenschutz dürfen nicht immer weiter gefährdet werden.

Nach der Konkretisierung der Befugnisse der Sicherheitsbehörden und der Schaffung neuer Befugnisse im Terrorismusbekämpfungsgesetz sowie in anderen gegen Ende der 14. Legislaturperiode verabschiedeten Bundesgesetzen ist vermehrt eine offene Diskussion darüber notwendig, wie der gebotene Ausgleich zwischen kollektiver Sicherheit und individuellen Freiheitsrechten so gewährleistet werden kann, dass unser Rechtsstaat nicht zum Überwachungsstaat wird. Dazu ist eine umfassende und systematische Evaluierung der im Zusammenhang mit der Terrorismusbekämpfung eingefügten Eingriffsbefugnisse der Sicherheitsbehörden notwendig.

Die Datenschutzbeauftragten halten darüber hinaus eine Erweiterung der im Terrorismusbekämpfungsgesetz vorgesehenen Pflicht zur Evaluierung der neuen Befugnisse der Sicherheitsbehörden auf andere vergleichbar intensive Eingriffsmaßnahmen – wie Telefonüberwachung, großer Lauschangriff und Rasterfahndung – für geboten.

Die Evaluierung muss durch unabhängige Stellen und anhand objektiver Kriterien erfolgen und aufzeigen, wo zurückgeschnitten werden muss, wo Instrumente untauglich sind oder wo die negativen Folgewirkungen überwiegen. Wissenschaftliche Untersuchungsergebnisse zur Evaluation des Richtervorbehalts z. B. bei Telefonüberwachungen machen deutlich, dass der Bundesgesetzgeber Maßnahmen zur Stärkung des Richtervorbehalts – und zwar nicht nur im Bereich der Telefonüberwachung – als grundrechtssicherndes Verfahrenselement ergreifen muss.

Stärkung des Schutzes von Gesundheitsdaten

Zwar schützt die Jahrtausende alte ärztliche Schweigepflicht Kranke davor, dass Informationen über ihren Gesundheitszustand von denjenigen unbefugt weitergegeben werden, die sie medizinisch betreuen. Medizinische Daten werden aber zunehmend außerhalb des besonderen ärztlichen Vertrauensverhältnisses zu Patienten und Patientinnen verarbeitet. Telemedizin und High-Tech-Medizin führen zu umfangreichen automatischen Datenspeicherungen. Hinzu kommt ein zunehmender Druck, Gesundheitsdaten z. B. zur Einsparung von Kosten, zur Verhinderung von Arzneimittelnebenfolgen oder „zur Qualitätssicherung“ einzusetzen. Die Informatisierung der Medizin durch elektronische Aktenführung, Einsatz von Chipkarten, Nutzung des Internet zur Konsultation bis hin zur ferngesteuerten Behandlung mit Robotern erfordern es deshalb, dass auch die Instrumente zum Schutz von Gesundheitsdaten weiterentwickelt werden.

Der Schutz des Patientengeheimnisses muss auch in einer computerisierten Medizin wirksam gewährleistet sein. Die Datenschutzbeauftragten begrüßen deshalb die Absichtserklärung in der Koalitionsvereinbarung, Patientenschutz und Patientenrechte auszubauen.

Dabei ist insbesondere sicherzustellen, dass Gesundheitsdaten außerhalb der eigentlichen Behandlung soweit wie möglich und grundsätzlich nur anonymisiert oder pseudonymisiert verarbeitet werden dürfen, soweit die Verarbeitung im Einzelfall nicht durch ein informiertes Einverständnis gerechtfertigt ist. Das Prinzip des informierten und freiwilligen Einverständnisses ist insbesondere auch für eine Gesundheitskarte zu beachten und zwar auch für deren Verwendung im Einzelfall.

Der Bundesgesetzgeber wird auch aufgefordert, gesetzlich zu regeln, dass Patientendaten, die in Datenverarbeitungsanlagen außerhalb von Arztpraxen und Krankenhäusern verarbeitet werden, genauso geschützt sind wie die Daten in der ärztlichen Praxis.

Geprüft werden sollte schließlich, ob und gegebenenfalls wie der Schutz von Gesundheitsdaten durch Geheimhaltungspflicht, Zeugnisverweigerungsrecht und Beschlagnahmeverbot auch dann gewährleistet werden kann, wenn diese, z. B. in der wissenschaftlichen Forschung, mit Einwilligung oder auf gesetzlicher Grundlage von anderen Einrichtungen außerhalb des Bereichs der behandelnden Ärztinnen und Ärzte verarbeitet werden.

Datenschutz und Gentechnik

Die Entwicklung der Gentechnik ist atemberaubend. Schon ein ausgefallenes Haar, ein Speichelrest an Besteck oder Gläsern, abgeschürfte Hautpartikel oder ein Blutstropfen – dies alles eignet sich als Untersuchungsmaterial, um den genetischen Bauplan eines Menschen entschlüsseln zu können. Inzwischen werden Gentests frei verkäuflich angeboten. Je mehr Tests gemacht werden, desto größer wird das Risiko für jeden Menschen, dass seine genetischen Anlagen von anderen auch gegen seinen Willen analysiert werden. Versicherungen oder Arbeitgeber und Arbeitgeberinnen werden ebenfalls Testergebnisse erfahren wollen.

Niemand darf zur Untersuchung genetischer Anlagen gezwungen werden; die Durchführung eines gesetzlich nicht zugelassenen Tests ohne Wissen und Wollen der betroffenen Person und die Nutzung daraus gewonnener Ergebnisse muss unter Strafe gestellt werden.

In der Koalitionsvereinbarung ist der Erlass eines „Gen-Test-Gesetzes“ vorgesehen. Ein solches Gesetz ist dringend erforderlich, damit der datenschutzgerechte Umgang mit genetischen Daten gewährleistet wird. Die Datenschutzbeauftragten haben dazu auf ihrer 62. Konferenz in Münster vom 24. bis 26. Oktober 2001 Vorschläge vorgelegt.

Datenschutz im Steuerrecht
Im bisherigen Steuer- und Abgabenrecht finden sich äußerst lückenhafte datenschutzrechtliche Regelungen. Insbesondere fehlen grundlegende Rechte, wie ein Akteneinsichts- und Auskunftsrecht. Eine Pflicht zur Information der Steuerpflichtigen über Datenerhebungen bei Dritten fehlt ganz.

Die jüngsten Gesetzesnovellen und Gesetzesentwürfe, die fortschreitende Vernetzung und multinationale Vereinbarungen verschärfen den Mangel: Immer mehr Steuerdaten sollen zentral durch das Bundesamt für Finanzen erfasst werden. Mit einheitlichen Personenidentifikationsnummern sollen Zusammenführungen und umfassende Auswertungen der Verbunddaten möglich werden. Eine erhebliche Ausweitung der Kontrollmitteilungen von Finanzbehörden und Kreditinstituten, die ungeachtet der Einführung einer pauschalen Abgeltungssteuer geplant ist, würde zweckungebundene und unverhältnismäßige Datenübermittlungen gestatten. Die zunehmende Vorratserhebung und -speicherung von Steuerdaten entspricht nicht dem datenschutzrechtlichen Grundsatz der Erforderlichkeit. Die Datenschutzbeauftragten fordern deshalb, die Aufnahme datenschutzrechtlicher Grundsätze in das Steuerrecht jetzt anzugehen und den Betroffenen die datenschutzrechtlichen Informations- und Auskunftsrechte zuzuerkennen.

Arbeitnehmerdatenschutz
Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, zum Beispiel durch

- die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,

- die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutzstandard der EG-Datenschutzrichtlinie gilt,

- die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,

- die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die hierzu von den Arbeitsgerichten entwickelten Schranken wirken unmittelbar nur im jeweils entschiedenen Einzelfall und sind auch nicht allen Betroffenen hinreichend bekannt. Das seit vielen Jahren angekündigte Arbeitnehmerdatenschutzgesetz muss hier endlich klare gesetzliche Vorgaben schaffen.

Die Datenschutzbeauftragten fordern deshalb, dass für die in der Koalitionsvereinbarung enthaltene Festlegung zur Schaffung von gesetzlichen Regelungen zum Arbeitnehmerdatenschutz nunmehr rasch ein ausformulierter Gesetzentwurf vorgelegt und anschließend zügig das Gesetzgebungsverfahren eingeleitet wird.

Stärkung einer unabhängigen, effizienten Datenschutzkontrolle
Die Datenschutzbeauftragten fordern gesetzliche Vorgaben, die die völlige Unabhängigkeit der Datenschutzkontrolle sichern und effektive Einwirkungsbefugnisse gewährleisten, wie dies der Art. 28 der EG-Datenschutzrichtlinie gebietet.

Die Datenschutzkontrollstellen im privaten Bereich haben bis heute nicht die völlige Unabhängigkeit, die die Europäische Datenschutzrichtlinie vorsieht. So ist in der Mehrzahl der deutschen Länder die Kontrolle über den Datenschutz im privaten Bereich nach wie vor bei den Innenministerien und nachgeordneten Stellen angesiedelt und unterliegt damit einer Fachaufsicht. Selbst in den Ländern, in denen die Landesbeauftragten diese Aufgabe wahrnehmen, ist ihre Unabhängigkeit nicht überall richtlinienkonform ausgestaltet.

Stellung des Bundesdatenschutzbeauftragten
Die rechtliche Stellung des Bundesdatenschutzbeauftragten als unabhängiges Kontrollorgan muss im Grundgesetz abgesichert werden.

Verbesserung der Informationsrechte
Die im Bereich der Informationsfreiheit tätigen Datenschutzbeauftragten unterstützen die Absicht in der Koalitionsvereinbarung, auf Bundesebene ein Informationsfreiheitsgesetz zu schaffen. Nach ihren Erfahrungen hat sich die gemeinsame Wahrnehmung der Aufgaben zum Datenschutz und zur Informationsfreiheit bewährt, weshalb sie auch auf Bundesebene realisiert werden sollte. Zusätzlich muss ein Verbraucherinformationsgesetz alle Produkte und Dienstleistungen erfassen und einen Informationsanspruch auch gegenüber Unternehmen einführen.

11. Anlage: Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 in Dresden

TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden

Mit großer Skepsis sehen die Datenschutzbeauftragten des Bundes und der Länder die Pläne zur Entwicklung zentraler Kontrollmechanismen und -infrastrukturen auf der Basis der Spezifikationen der Industrie-Allianz „Trusted Computing Platform Alliance“ (TCPA).

Die TCPA hat sich zum Ziel gesetzt, vertrauenswürdige Personalcomputer zu entwickeln. Dazu bedarf es spezieller Hard- und Software. In den bisher bekannt gewordenen Szenarien soll die Vertrauenswürdigkeit dadurch gewährleistet werden, dass zunächst ein spezieller Kryptoprozessor nach dem Einschalten des PC überprüft, ob die installierte Hardware und das Betriebssystem mit den von der TCPA zertifizierten und auf zentralen Servern hinterlegten Konfigurationsangaben übereinstimmen. Danach übergibt der Prozessor die Steuerung an ein TCPA-konformes Betriebssystem. Beim Start einer beliebigen Anwendersoftware prüft das Betriebssystem dann deren TCPA-Konformität, beispielsweise durch Kontrolle der Lizenz oder der Seriennummer, und kontrolliert weiterhin, ob Dokumente in zulässiger Form genutzt werden. Sollte eine der Prüfungen Abweichungen zur hinterlegten, zertifizierten Konfiguration ergeben, lässt sich der PC nicht booten bzw. das entsprechende Programm wird gelöscht oder lässt sich nicht starten.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen alle Aktivitäten, die der Verbesserung des Datenschutzes dienen und insbesondere zu einer manipulations- und missbrauchssicheren sowie transparenten IT-Infrastruktur führen. Sie erkennen auch die berechtigten Forderungen der Softwarehersteller an, dass kostenpflichtige Software nur nach Bezahlung genutzt werden darf.

Wenn aber zentrale Server einer externen Kontrollinstanz genutzt werden, um mit entsprechend modifizierten Client-Betriebssystemen Prüf- und Kontrollfunktionen zu steuern, müssten sich Anwenderinnen und Anwender beim Schutz sensibler Daten uneingeschränkt auf die Vertrauenswürdigkeit der externen Instanz verlassen können. Die Datenschutzbeauftragten erachten es für unzumutbar, wenn

- Anwenderinnen und Anwender die alleinige Kontrolle über die Funktionen des eigenen Computers verlieren, falls eine externe Kontrollinstanz Hardware, Software und Daten kontrollieren und manipulieren kann,

- die Verfügbarkeit aller TCPA-konformen Personalcomputer und der darauf verarbeiteten Daten gefährdet wäre, da sowohl Fehler in der Kontrollinfrastruktur als auch Angriffe auf die zentralen TCPA-Server die Funktionsfähigkeit einzelner Rechner sofort massiv einschränken würden,

- andere Institutionen oder Personen sich vertrauliche Informationen von zentralen Servern beschaffen würden, ohne dass der Anwender dies bemerkt,

- die Nutzung von Servern oder PC davon abhängig gemacht würde, dass ein Zugang zum Internet geöffnet wird,

- der Zugang zum Internet und E-mail-Verkehr durch Softwarerestriktionen behindert würde,

- der Umgang mit Dokumenten ausschließlich gemäß den Vorgaben der externen Kontrollinstanz zulässig sein würde und somit eine sehr weitgehende Zensur ermöglicht wird,

- auf diese Weise der Zugriff auf Dokumente von Konkurrenzprodukten verhindert und somit auch die Verbreitung datenschutzfreundlicher Open-Source-Software eingeschränkt werden kann und

- Programmergänzungen (Updates) ohne vorherige Einwilligung im Einzelfall aufgespielt werden könnten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb Hersteller von Informations- und Kommunikationstechnik auf, Hard- und Software so zu entwickeln und herzustellen, dass

- Anwenderinnen und Anwender die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik haben, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Einwilligung im Einzelfall erfolgen,

- alle zur Verfügung stehenden Sicherheitsfunktionen für Anwenderinnen und Anwender transparent sind und

- die Nutzung von Hard- und Software und der Zugriff auf Dokumente auch weiterhin möglich ist, ohne dass Dritte davon Kenntnis erhalten und Nutzungsprofile angelegt werden können.

Auf diese Weise können auch künftig die in den Datenschutzgesetzen des Bundes und der Länder geforderte Vertraulichkeit und Verfügbarkeit der zu verarbeitenden personenbezogenen Daten sichergestellt und die Transparenz bei der Verarbeitung dieser Daten gewährleistet werden.

12. Anlage: Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 in Dresden

Datenschutzbeauftragte fordern vertrauenswürdige Informationstechnik

Anwenderinnen und Anwender von komplexen IT-Produkten müssen unbedingt darauf vertrauen können, dass Sicherheitsfunktionen von Hard- und Software korrekt ausgeführt werden, damit die Vertraulichkeit, die Integrität und die Zurechenbarkeit der Daten gewährleistet sind. Dieses Vertrauen kann insbesondere durch eine datenschutzgerechte Gestaltung der Informationstechnik geschaffen werden. Ausbleibende Erfolge bei eCommerce und E-Government werden mit fehlendem Vertrauen in einen angemessenen Schutz der personenbezogenen Daten und mangelnder Akzeptanz der Nutzerinnen und Nutzer erklärt. Anwenderinnen und Anwender sollten ihre Sicherheitsanforderungen präzise definieren und Anbieter ihre Sicherheitsleistungen schon vor der Produktentwicklung festlegen und für alle nachprüfbar dokumentieren. Die Datenschutzbeauftragten des Bundes und der Länder wollen Herstellerinnen und Hersteller und Anwenderinnen und Anwender von Informationstechnik unterstützen, indem sie entsprechende Werkzeuge und Hilfsmittel zur Verfügung stellen.

So bietet der Bundesbeauftragte für den Datenschutz seit dem 11. November 2002 mit zwei so genannten Schutzprofilen (Protection Profiles) Werkzeuge an, mit deren Hilfe Anwenderinnen und Anwender bereits vor der Produktentwicklung ihre datenschutzspezifischen Anforderungen für bestimmte Produkttypen, beispielsweise im Gesundheitswesen oder im E-Government, detailliert beschreiben können. Kerngedanke der in diesen Schutzprofilen definierten Sicherheitsanforderungen ist die Kontrollierbarkeit aller Informationsflüsse eines Rechners gemäß einstellbarer Informationsflussregeln. Die Schutzprofile sind international anerkannt, da sie auf der Basis der „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria)“ entwickelt wurden. Herstellerinnen und Hersteller können datenschutzfreundliche Produkte somit nach international prüffähigen Vorgaben der Anwenderinnen und Anwender entwickeln. Unabhängige Prüfinstitutionen können diese Produkte dann nach Abschluss der Entwicklung nach international gültigen Kriterien prüfen. [1]

---

1 Die Schutzprofile mit dem Titel „BISS - Benutzerbestimmbare Informationsflusskontrolle“ haben die Registrierungskennzeichen BSI-PP-0007-2002 und BSI-PTT-008-2002 und sind beim Bundesbeauftragten für den Datenschutz unter http://www.bfd.bund.de/technik/protection_profile.html abrufbar.

In Schleswig-Holstein bietet das Unabhängige Landeszentrum für Datenschutz ein Verfahren mit vergleichbarer Zielsetzung an, das ebenfalls zu überprüfbarer Sicherheit von IT-Produkten führt. Für nachweislich datenschutzgerechte IT-Produkte können Hersteller ein so genanntes Datenschutz-Gütesiegel erhalten. Das Landeszentrum hat auf der Grundlage landesspezifischer Rechtsvorschriften bereits im Jahr 2002 einen entsprechenden Anforderungskatalog veröffentlicht und zur CeBIT 2003 eine an die Common Criteria angepasste Version vorgestellt. [2]

Die Datenschutzbeauftragten des Bundes und der Länder empfehlen die Anwendung von Schutzprofilen und Auditierungsprozeduren, damit auch der Nutzer oder die Nutzerin beurteilen kann, ob IT-Systeme und -Produkte vertrauenswürdig und datenschutzfreundlich sind. Sie appellieren an die Hersteller, entsprechende Produkte zu entwickeln bzw. vorhandene Produkte anhand bereits bestehender oder gleichwertiger Schutzprofile und Anforderungskataloge zu modifizieren. Sie treten dafür ein, dass die öffentliche Verwaltung vorrangig solche Produkte einsetzt.

2 Die Ergebnisse der bisherigen Auditierungen durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein sind unter http://www.datenschutzzentrum.de/guetesiegel veröffentlicht.

13. Anlage: Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 in Dresden

Datenschutzrechtliche Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung

In der Diskussion über eine grundlegende Reform des Rechts der gesetzlichen Krankenversicherung (GKV) werden in großem Maße datenschutzrechtliche Belange berührt. Erweiterte Befugnisse zur Verarbeitung von medizinischen Leistungs- und Abrechnungsdaten sollen eine stärkere Kontrolle der Patientinnen und Patienten sowie der sonstigen beteiligten Parteien ermöglichen. Verbesserte individuelle und statistische Informationen sollen zudem die medizinische und informationelle Selbstbestimmung der Patientinnen und Patienten verbessern sowie die Transparenz für die Beteiligten und für die Öffentlichkeit erhöhen.

So sehen Vorschläge des Bundesministeriums für Gesundheit und Soziale Sicherung zur Modernisierung des Gesundheitswesens u. a. vor, dass bis zum Jahr 2006 schrittweise eine elektronische Gesundheitskarte eingeführt wird und Leistungs- und Abrechnungsdaten zusammengeführt werden sollen. Boni für gesundheitsbewusstes Verhalten und Ausnahmen oder Mali für gesundheitsgefährdendes Verhalten sollen medizinisch rationales Verhalten der Versicherten fördern, was eine Überprüfung dieses Verhaltens voraussetzt. Derzeit werden gesetzliche Regelungen ausgearbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder weisen erneut auf die datenschutzrechtlichen Chancen und Risiken einer Modernisierung des Systems der GKV hin.

Viele Vorschläge zielen darauf ab, Gesundheitskosten dadurch zu reduzieren, dass den Krankenkassen mehr Kontrollmöglichkeiten eingeräumt werden. Solche individuellen Kontrollen können indes nur ein Hilfsmittel zu angestrebten Problemlösungen, nicht aber die Problemlösung selbst sein. Sie sind auch mit dem Recht der Patientinnen und Patienten auf Selbstbestimmung und dem Schutz der Vertrauensbeziehung zwischen ärztlichem Personal und behandelten Personen nicht problemlos in Einklang zu bringen. Eingriffe müssen nach den Grundsätzen der Datenvermeidung und der Erforderlichkeit und Verhältnismäßigkeit auf ein Minimum beschränkt bleiben. Möglichkeiten der anonymisierten oder pseudonymisierten Verarbeitung von Patientendaten müssen ausgeschöpft werden. Eine umfassendere Information der Patientinnen und Patienten, die zu mehr Transparenz führt und die Verantwortlichkeiten verdeutlicht, ist ebenfalls ein geeignetes Hilfsmittel.

Sollte im Rahmen gesetzlicher Regelungen zur Qualitätssicherung und Abrechnungskontrolle für einzelne Bereiche der Zugriff auf personenbezogene Behandlungsdaten unerlässlich sein, müssen Vorgaben entwickelt werden, die

- den Zugriff auf genau festgelegte Anwendungsfälle begrenzen,

- das Prinzip der Stichprobe zugrunde legen,

- eine strikte Einhaltung der Zweckbindung gewährleisten und

- die Auswertung der Daten einer unabhängigen Stelle übertragen.

1. Die Datenschutzbeauftragten erkennen die Notwendigkeit einer verbesserten Datenbasis zur Weiterentwicklung der gesetzlichen Krankenversicherung an. Hierzu reichen wirksam pseudonymisierte Daten grundsätzlich aus. Eine Zusammenführung von Leistungs- und Versichertendaten darf nicht dazu führen, dass über eine lückenlose zentrale Sammlung personenbeziehbarer Patientendaten mit sensiblen Diagnose- und Behandlungsangaben z. B. zur Risikoselektion geeignete medizinische Profile entstehen. Dies könnte nicht nur zur Diskriminierung einzelner Versicherter führen, sondern es würde auch die sozialstaatliche Errungenschaft des solidarischen Tragens von Krankheitsrisiken aufgegeben. Zudem wären zweckwidrige Auswertungen möglich, für die es viele Interessierte gäbe, von Privatversicherungen bis hin zu Arbeitgebern. Durch sichere technische und organisatorische Verfahren, die Pseudonymisierung der Daten und ein grundsätzliches sanktionsbewehrtes Verbot der Reidentifizierung pseudonymisierter Datenbestände kann solchen Gefahren entgegengewirkt werden.

2. Die Einführung einer Gesundheitschipkarte kann die Transparenz des Behandlungsgeschehens für die Patientinnen und Patienten erhöhen, deren schonende und erfolgreiche medizinische Behandlung effektivieren und durch Vermeidung von Medienbrüchen und Mehrfachbehandlungen Kosten senken. Eine solche Karte kann aber auch dazu genutzt werden, die Selbstbestimmungsrechte der Patientinnen und Patienten zu verschlechtern. Dieser Effekt würde durch eine Pflichtkarte eintreten, auf der – von den Betroffenen nicht beeinflussbar – Diagnosen und Medikationen zur freien Einsicht durch Ärztinnen und Ärzte sowie sonstige Leistungserbringende gespeichert wären. Zentrales Patientenrecht ist es, selbst zu entscheiden, welchem Arzt oder welcher Ärztin welche Informationen anvertraut werden.

Die Datenschutzkonferenz fordert im Fall der Einführung einer Gesundheitschipkarte die Gewährleistung des Rechts der Patientinnen und Patienten, grundsätzlich selbst zu entscheiden,

- ob sie überhaupt verwendet wird,

- welche Daten darauf gespeichert werden oder über sie abgerufen werden können,

- welche Daten zu löschen sind und wann das zu geschehen hat,

- ob sie im Einzelfall vorgelegt wird und

- welche Daten im Einzelfall ausgelesen werden sollen.

Sicherzustellen ist weiterhin

- ein Beschlagnahmeverbot und Zeugnisverweigerungsrecht in Bezug auf die Daten, die auf der Karte gespeichert sind,

- die Beschränkung der Nutzung auf das Patienten-Arzt/Apotheken-Verhältnis und

- die Strafbarkeit des Datenmissbrauchs.

Die Datenschutzkonferenz hat bereits zu den datenschutzrechtlichen Anforderungen an den „Arzneimittelpass“ (Medikamentenchipkarte) ausführlich Stellung genommen (Entschließung vom 26.10.2001). Die dort formulierten Anforderungen an eine elektronische Gesundheitskarte sind weiterhin gültig. Die „Gemeinsame Erklärung des Bundesministeriums für Gesundheit und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen“ vom 3. Mai 2002, wonach „der Patient Herr seiner Daten“ sein soll, enthält gute Ansatzpunkte, auf deren Basis die Einführung einer Gesundheitskarte betrieben werden kann.

3. Die Datenschutzbeauftragten anerkennen die Förderung wirtschaftlichen und gesundheitsbewussten Verhaltens als ein wichtiges Anliegen. Dies darf aber nicht dazu führen, dass die Krankenkassen detaillierte Daten über die private Lebensführung erhalten („fährt Ski“, „raucht“, „trinkt zwei Biere pro Tag“), diese überwachen und so zur „Gesundheitspolizei“ werden. Notwendig ist deshalb die Entwicklung von Konzepten, die ohne derartige mitgliederbezogene Datensätze bei den Krankenkassen und ihre Überwachung auskommen.

4. Die Datenschutzbeauftragten begrüßen alle Pläne, die darauf hinauslaufen, das Verfahren der GKV allgemein sowie die individuelle Behandlung und Datenverarbeitung für die Betroffenen transparenter zu machen. Maßnahmen wie die Einführung der Patientenquittung, die Information über das Leistungsverfahren und über Umfang und Qualität des Leistungsangebotes sowie eine verstärkte Einbindung der Patientinnen und Patienten durch Unterrichtungen und Einwilligungserfordernisse stärken die Patientensouveränität und die Selbstbestimmung.

14. Anlage: Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 in Dresden

Kennzeichnung von Daten aus besonders eingriffsintensiven Erhebungen

Das Bundesverfassungsgericht hat in seinem Urteil zur strategischen Fernmeldeüberwachung des Bundesnachrichtendienstes festgestellt, dass sich die Zweckbindung der bei dieser Maßnahme erlangten personenbezogenen Daten nur gewährleisten lässt, wenn auch nach ihrer Erfassung erkennbar bleibt, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Eine entsprechende Kennzeichnung ist daher von Verfassungs wegen geboten. Dementsprechend wurde die Kennzeichnungspflicht in der Novellierung des G 10-Gesetzes auch allgemein für jede Datenerhebung des Bundesnachrichtendienstes und des Verfassungsschutzes im Schutzbereich des Art. 10 GG angeordnet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Pflicht zur Kennzeichnung aufgrund der Ausführungen des Bundesverfassungsgerichts nicht auf den Bereich der Fernmeldeüberwachung beschränkt ist. Sie gilt auch für vergleichbare Methoden der Datenerhebung, bei denen die Daten durch besonders eingriffsintensive Maßnahmen gewonnen werden und deswegen einer strikten Zweckbindung unterliegen müssen.

Deshalb müssen zumindest solche personenbezogenen Daten, die aus einer Telefon-, Wohnraum- oder Postüberwachung erlangt wurden, besonders gekennzeichnet werden.

15. Anlage: Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 in Dresden

Elektronische Signatur im Finanzbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass mit dem Signaturgesetz und der Anpassung von mehr als 3.000 Rechtsvorschriften in Deutschland die rechtlichen Voraussetzungen geschaffen wurden, um die „qualifizierte elektronische Signatur“ der eigenhändigen Unterschrift gleichzustellen. Die administrativen und technischen Voraussetzungen sind inzwischen weitgehend vorhanden. Mehr als zwanzig freiwillig akkreditierte Zertifizierungsdiensteanbieter nach dem Signaturgesetz sind von der Regulierungsbehörde für Telekommunikation und Post (RegTP) zugelassen. Sowohl Chipkarten, die für die qualifizierte elektronische Signatur zugelassen sind, als auch die dafür erforderlichen Lesegeräte sind verfügbar.

Für die elektronische Kommunikation zwischen der Finanzverwaltung und den Bürgerinnen und Bürgern ist die „qualifizierte elektronische Signatur“ gesetzlich vorgeschrieben. Die Finanzverwaltung will eine Übergangsbestimmung in der Steuerdatenübermittlungsverordnung vom 28.01.2003 nutzen, nach der bis Ende 2005 eine lediglich fortgeschrittene, die so genannte qualifizierte elektronische Signatur mit Einschränkungen eingesetzt werden kann. Aus folgenden Gründen lehnen die Datenschutzbeauftragten dieses Vorgehen ab:

- Die „qualifizierte elektronische Signatur mit Einschränkungen“ bietet im Gegensatz zur „qualifizierten elektronischen Signatur“ und der „qualifizierten elektronischen Signatur mit Anbieterakkreditierung“ keine umfassend nachgewiesene Sicherheit, vor allem aber keine langfristige Überprüfbarkeit. Die mit ihr unterzeichneten elektronischen Dokumente sind unerkannt manipulierbar. Die „qualifizierte elektronische Signatur mit Einschränkungen“ hat geringeren Beweiswert als die eigenhändige Unterschrift.

- Die technische Infrastruktur, die die Finanzverwaltung für die „qualifizierte elektronische Signatur mit Einschränkungen“ vorgesehen hat, kann sie verwenden, um elektronische, fortgeschritten oder qualifiziert signierte Dokumente von Bürgerinnen und Bürgern und Steuerberaterinnen und Steuerberatern zu prüfen und selbst fortgeschrittene Signaturen zu erzeugen. Damit die Finanzverwaltung selbst qualifiziert signieren kann, reicht eine Ergänzung mit einem qualifizierten Zertifikat aus.

- Für die elektronische Steuererklärung ELSTER sollen Zertifizierungsdienste im außereuropäischen Ausland zugelassen werden, für die weder eine freiwillige Akkreditierung noch eine Kontrolle durch deutsche Datenschutzbehörden möglich ist, anstatt Zertifizierungsdienste einzuschalten, die der Europäischen Datenschutzrichtlinie entsprechen. Damit sind erhebliche Gefahren verbunden, die vermeidbar sind.

- Die elektronische Signatur soll auch zur Authentisierung der Steuerpflichtigen und Steuerberater gegenüber ELSTER genutzt werden, obwohl die Trennung der Schlüsselpaare für Signatur und Authentisierung unerlässlich und bereits Stand der Technik ist.

Die Datenschutzbeauftragten des Bundes und der Länder befürchten, dass bei Schaffung weiterer Signaturverfahren mit geringerer Sicherheit die Transparenz für die Anwenderinnen und Anwender verloren geht und der sichere und verlässliche elektronische Rechts- und Geschäftsverkehr in Frage gestellt werden könnte.

Abweichend vom Vorgehen der Finanzverwaltung hat sich die Bundesregierung sowohl im Rahmen der Initiative „Bund Online 2005“ als auch im so genannten Signaturbündnis für sichere Signaturverfahren eingesetzt. Das Verfahren ELSTER sollte genutzt werden, um sogleich qualifizierten und damit sicheren Signaturen zum Durchbruch zu verhelfen.

Vor diesem Hintergrund empfiehlt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Bundesregierung,

- dass die Finanzbehörden Steuerbescheide und sonstige Dokumente ausschließlich qualifiziert signiert versenden,

- den Bürgerinnen und Bürgern eine sichere, zuverlässige, leicht einsetzbare und transparente Technologie zur Verfügung zu stellen,

- unterschiedliche Ausstattungen für abgestufte Qualitäten und Anwendungsverfahren zu vermeiden,

- die Anschaffung von Signaturerstellungseinheiten mit zugehörigen Zertifikaten und ggf. Signaturanwendungskomponenten für „qualifizierte elektronische Signaturen mit Anbieterakkreditierung“ staatlich zu fördern,

- die vorhandenen Angebote der deutschen und sonstigen europäischen Anbieter vornehmlich heranzuziehen, um die qualifizierte elektronische Signatur und den Einsatz entsprechender Produkte zu fördern,

- eGovernment- und eCommerce-Projekte zu fördern, die qualifizierte elektronische Signaturen unterhalb der Wurzelzertifizierungsinstanz der RegTP einsetzen und somit Multifunktionalität und Interoperabilität gewährleisten,

- die Entwicklung von technischen Standards für die umfassende Einbindung der qualifizierten elektronischen Signatur zu fördern,

- die Weiterentwicklung der entsprechenden Chipkartentechnik voranzutreiben.

16. Anlage: Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 in Dresden

Transparenz bei der Telefonüberwachung

Nach derzeitigem Recht haben die Betreiber von Telekommunikationsanlagen eine Jahresstatistik über die von ihnen zu Strafverfolgungszwecken durchgeführten Überwachungsmaßnahmen zu erstellen. Diese Zahlen werden von der Regulierungsbehörde für Telekommunikation und Post veröffentlicht. Auf diese Weise wird die Allgemeinheit über Ausmaß und Entwicklung der Telekommunikationsüberwachung in Deutschland informiert.

Nach aktuellen Plänen der Bundesregierung soll diese Statistik abgeschafft werden. Begründet wird dies mit einer Entlastung der Telekommunikationsunternehmen von überflüssigen Arbeiten. Zudem wird darauf verwiesen, dass das Bundesjustizministerium eine ähnliche Statistik führt, die sich auf Zahlen der Landesjustizbehörden stützt. Dabei wird verkannt, dass die beiden Statistiken unterschiedliches Zahlenmaterial berücksichtigen. So zählen die Telekommunikationsunternehmen jede Überwachungsmaßnahme getrennt nach den einzelnen Anschlüssen, während von den Landesjustizverwaltungen nur die Anzahl der Strafverfahren erfasst wird.

In den vergangenen Jahren ist die Zahl der überwachten Anschlüsse um jährlich etwa 25 Prozent gestiegen. Gab es im Jahr 1998 noch 9.802 Anordnungen, waren es im Jahr 2001 bereits 19.896. Diese stetige Zunahme von Eingriffen in das Fernmeldegeheimnis sehen die Datenschutzbeauftragten des Bundes und der Länder mit großer Sorge. Eine fundierte und objektive Diskussion in Politik und Öffentlichkeit ist nur möglich, wenn die tatsächliche Anzahl von Telefonüberwachungsmaßnahmen bekannt ist. Allein eine Aussage über die Anzahl der Strafverfahren, in denen eine Überwachungsmaßnahme stattgefunden hat, reicht nicht aus. Nur die detaillierten Zahlen, die derzeit von den Telekommunikationsunternehmen erhoben werden, sind aussagekräftig genug.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine Beibehaltung der Unternehmensstatistik nach § 88 Abs. 5 Telekommunikationsgesetz sowie ihre Erstreckung auf die Zahl der Auskünfte über Telekommunikationsverbindungen, um auf diesem Wege bessere Transparenz bei der Telefonüberwachung zu schaffen.

17. Anlage Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 28. April 2003

Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation

Im Zuge der bevorstehenden Novellierung des Telekommunikationsgesetzes plant die Bundesregierung neben der Abschaffung der Unternehmensstatistik (vgl. dazu Entschließung der 65. Konferenz vom 28.03.2003 zur Transparenz bei der Telefonüberwachung) eine Reihe weiterer Änderungen, die zu einer Absenkung des gegenwärtigen Datenschutzniveaus führen würden.

Zum einen ist vorgesehen, die Zweckentfremdung von Bestandsdaten der Telekommunikation (z. B. Art des Anschlusses, Kontoverbindung, Befreiung vom Telefonentgelt aus sozialen oder gesundheitlichen Gründen) für Werbezwecke weitergehend als bisher schon dann zuzulassen, wenn der Betroffene dem nicht widerspricht. Dies muss – wie bisher – die informierte Einwilligung des Betroffenen voraussetzen.

Außerdem plant die Bundesregierung, Daten, die den Zugriff auf Inhalte oder Informationen über die näheren Umstände der Telekommunikation schützen (wie z. B. PINs und PUKs - Personal Unblocking Keys), in Zukunft der Beschlagnahme für die Verfolgung beliebiger Straftaten zugänglich zu machen. Bisher kann der Zugriff auf solche Daten nur angeordnet werden, wenn es um die Aufklärung bestimmter schwerer Straftaten geht. Diese Absenkung oder gar Aufhebung der verfassungsmäßig gebotenen Schutzschwelle für Daten, die dem Telekommunikationsgeheimnis unterliegen, wäre nicht gerechtfertigt; dies ergibt sich auch aus dem Urteil des Bundesverfassungsgerichts vom 12.03.2003.

Aus der Sicht des Datenschutzes ist auch die Versagung eines anonymen Zugangs zum Mobilfunk problematisch. Die beabsichtigte Gesetzesänderung führt dazu, dass z. B. der Erwerb eines „vertragslosen“ Handys, das mit einer entsprechenden – im Prepaid-Verfahren mit Guthaben aufladbaren – SIM-Karte ausgestattet ist, einem Identifikationszwang unterliegt. Dies hat zur Folge, dass die Anbieter von Prepaid-Verfahren eine Reihe von Daten wegen eines möglichen Zugriffs der Sicherheitsbehörden auf Vorrat speichern müssen, die sie für ihre Betriebszwecke nicht benötigen. Die verdachtslose rountinemäßige Speicherung zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer künftiger Straftaten würde auch zur Entstehung von selbst für die Sicherheitsbehörden sinn- und nutzlosen Datenhalden führen. So sind erfahrungsgemäß z. B. die Erwerber häufig nicht mit den tatsächlichen Nutzern der Prepaid-Angebote identisch.

Insgesamt fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, das gegenwärtige Datenschutzniveau bei der Telekommunikation zu verbessern, statt es weiter abzusenken. Hierzu sollte jetzt ein eigenes Telekommunikations-Datenschutzgesetz verabschiedet werden, das den Anforderungen einer freiheitlichen Informationsgesellschaft genügt und später im Zuge der noch ausstehenden zweiten Stufe der Modernisierung des Bundesdatenschutzgesetzes mit diesem zusammengeführt werden könnte.

18. Anlage: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 30. April 2003

Entschließung zur Neuordnung der Rundfunkfinanzierung

Die Länder bereiten gegenwärtig eine Neuordnung der Rundfunkfinanzierung vor, die im neuen Rundfunkgebührenstaatsvertrag geregelt werden soll. Die dazu bekannt gewordenen Vorschläge der Rundfunkanstalten lassen befürchten, dass bei ihrer Umsetzung die bestehenden datenschutzrechtlichen Defizite nicht nur beibehalten werden, sondern dass mit zum Teil gravierenden Verschlechterungen des Datenschutzes gerechnet werden muss:

- Insbesondere ist geplant, alle Meldebehörden zu verpflichten, der GEZ zum In-Kraft-Treten des neuen Staatsvertrages die Daten aller Personen in Deutschland zu übermitteln, die älter als 16 Jahre sind. Dadurch entstünde bei der GEZ faktisch ein bundesweites zentrales Register aller über 16-jährigen Personen mit Informationen über ihre sozialen Verhältnisse (wie Partnerschaften, gesetzliche Vertretungen, Haushaltszugehörigkeit und Empfang von Sozialleistungen), obwohl ein großer Teil dieser Daten zu keinem Zeitpunkt für den Einzug der Rundfunkgebühren erforderlich ist.

- Auch wenn in Zukunft nur noch für ein Rundfunkgerät pro Wohnung Gebühren gezahlt werden, sollen alle dort gemeldeten erwachsenen Bewohner von vornherein zur Auskunft verpflichtet sein, selbst wenn keine Anhaltspunkte für eine Gebührenpflicht bestehen. Für die Auskunftspflicht reicht es demgegenüber aus, dass zunächst – wie bei den amtlichen Statistiken erfolgreich praktiziert – nur die Meldedaten für eine Person übermittelt werden, die dazu befragt wird.

- Zudem soll die regelmäßige Übermittlung aller Zu- und Wegzüge aus den Meldedaten nun um Übermittlungen aus weiteren staatlichen bzw. sonstigen öffentlichen Dateien wie den Registern von berufsständischen Kammern, den Schuldnerverzeichnissen und dem Gewerbezentralregister erweitert werden. Auf alle diese Daten will die GEZ künftig auch online zugreifen.

- Gleichzeitig soll die von den zuständigen Landesdatenschutzbeauftragten als unzulässig bezeichnete Praxis der GEZ, ohne Wissen der Bürgerinnen und Bürger deren personenbezogene Daten bei Dritten – wie beispielsweise in der Nachbarschaft oder bei privaten Adresshändlern – zu erheben, ausdrücklich erlaubt werden.

- Schließlich sollen die bisher bestehenden Möglichkeiten der Aufsicht durch die Landesbeauftragten für den Datenschutz ausgeschlossen werden, so dass für die Rundfunkanstalten und die GEZ insoweit nur noch eine interne Datenschutzkontrolle beim Rundfunkgebühreneinzug bestünde.

Diese Vorstellungen der Rundfunkanstalten widersprechen dem Verhältnismäßigkeitsprinzip und sind daher nicht akzeptabel.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre Forderung nach einer grundlegenden Neuorientierung der Rundfunkfinanzierung, bei der datenschutzfreundliche Modelle zu bevorzugen sind. Sie haben hierzu bereits praktikable Vorschläge vorgelegt.

19. Anlage: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 18. Juli 2003

Bei der Erweiterung der DNA-Analyse Augenmaß bewahren

Derzeit gibt es mehrere politische Absichtserklärungen und Gesetzesinitiativen mit dem Ziel, die rechtlichen Schranken in § 81 g StPO für die Entnahme und Untersuchung von Körperzellen und für die Speicherung der dabei gewonnenen DNA-Identifizierungsmuster (sog. genetischer Fingerabdruck) in der zentralen DNA-Analyse-Datei des BKA abzusenken.

Die Vorschläge gehen dahin,

- zum einen als Anlasstat zur Anordnung einer DNA-Analyse künftig nicht mehr – wie vom geltenden Recht gefordert – in jedem Fall eine Straftat von erheblicher Bedeutung oder – wie jüngst vom Bundestag beschlossen – eine Straftat gegen die sexuelle Selbstbestimmung zu verlangen, sondern auch jede andere Straftat mit sexuellem Hintergrund oder sogar jedwede Straftat ausreichen zu lassen,

- zum anderen die auf einer eigenständigen, auf den jeweiligen Einzelfall bezogenen Gefahrenprognose beruhende Anordnung durch Richterinnen und Richter entfallen zu lassen und alle Entscheidungen der Polizei zu übertragen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass die Anordnung der Entnahme und Untersuchung von Körperzellen zur Erstellung und Speicherung eines genetischen Fingerabdrucks einen tiefgreifenden und nachhaltigen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen darstellt; dies hat auch das Bundesverfassungsgericht in seinen Beschlüssen vom Dezember 2000 und März 2001 bestätigt.

Selbst wenn bei der DNA-Analyse nach der derzeitigen Rechtslage nur die nicht codierenden Teile untersucht werden: Schon daraus können Zusatzinformationen gewonnen werden (Geschlecht, Altersabschätzung, Zuordnung zu bestimmten Ethnien, möglicherweise einzelne Krankheiten wie Diabetes, Klinefelter-Syndrom). Auch deshalb lässt sich ein genetischer Fingerabdruck mit einem herkömmlichen Fingerabdruck nicht vergleichen. Zudem ist immerhin technisch auch eine Untersuchung des codierenden Materials denkbar, so dass zumindest die abstrakte Eignung für viel tiefer gehende Erkenntnisse ge-

geben ist. Dies bedingt unabhängig von den gesetzlichen Einschränkungen ein höheres abstraktes Gefährdungspotential.

Ferner ist zu bedenken, dass das Ausstreuen von Referenzmaterial (z. B. kleinste Hautpartikel oder Haare), das mit dem gespeicherten Identifizierungsmuster abgeglichen werden kann, letztlich nicht zu steuern ist, so dass in höherem Maß als bei Fingerabdrücken die Gefahr besteht, dass genetisches Material einer Nichttäterin oder eines Nichttäters an Tatorten auch zufällig, durch nicht wahrnehmbare Kontamination mit Zwischenträgern oder durch bewusste Manipulation platziert wird. Dies kann für Betroffene im Ergebnis zu einer Art Umkehr der Beweislast führen.

Angesichts dieser Wirkungen und Gefahrenpotentiale sehen die Datenschutzbeauftragten Erweiterungen des Einsatzes der DNA-Analyse kritisch und appellieren an die Regierungen und Gesetzgeber des Bundes und der Länder, die Diskussion dazu mit Augenmaß und unter Beachtung der wertsetzenden Bedeutung des Rechts auf informationelle Selbstbestimmung zu führen. Die DNA-Analyse darf nicht zum Routinewerkzeug jeder erkennungsdienstlichen Behandlung und damit zum alltäglichen polizeilichen Eingriffsinstrument im Rahmen der Aufklärung und Verhütung von Straftaten jeder Art werden. Auf das Erfordernis der Prognose erheblicher Straftaten als Voraussetzung einer DNA-Analyse darf nicht verzichtet werden.

Im Hinblick auf die Eingriffsschwere ist auch der Richtervorbehalt für die Anordnung der DNA-Analyse unverzichtbar. Es ist deshalb auch zu begrüßen, dass zur Stärkung dieser grundrechtssichernden Verfahrensvorgabe für die Anordnungsentscheidung die Anforderungen an die Begründung des Gerichts gesetzlich präzisiert wurden. Zudem sollte die weit verbreitete Praxis, DNA-Analysen ohne richterliche Entscheidung auf der Grundlage der Einwilligung der Betroffenen durchzuführen, gesetzlich ausgeschlossen werden.

20. Anlage: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 7. August 2003

Zum automatischen Software-Update

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die zunehmenden Bestrebungen von Softwareherstellern, über das Internet unbemerkt auf die Personalcomputer der Nutzerinnen und Nutzer zuzugreifen.

Zur Gewährleistung der Sicherheit und der Aktualität von System- und Anwendungssoftware ist es notwendig, regelmäßig Updates vorzunehmen. Weltweit agierende Softwarehersteller bieten in zunehmendem Maße an, im Rahmen so genannter Online-Updates komplette Softwarepakete oder einzelne Updates über das Internet auf die Rechner ihrer Kunden zu laden und automatisch zu installieren. Diese Verfahren bergen erhebliche Datenschutzrisiken in sich:

- Immer öfter werden dabei – oftmals vom Nutzer unbemerkt oder zumindest nicht transparent – Konfigurationsinformationen mit personenbeziehbaren Daten aus dem Zielrechner ausgelesen und an die Softwarehersteller übermittelt, ohne das dies im derzeit praktizierten Umfang aus technischen Gründen erforderlich ist.

- Darüber hinaus bewirken Online-Updates vielfach Änderungen an der Software der Zielrechner, die dann in der Regel ohne die erforderlichen Tests und Freigabeverfahren genutzt werden.

- Ferner ist nicht immer sichergestellt, dass andere Anwendungen problemlos weiter funktionieren. Das – unbemerkte – Update wird dann nicht als Fehlerursache erkannt.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Änderungen an automatisierten Verfahren zur Verarbeitung personenbezogener Daten oder an den zugrunde liegenden Betriebssystemen Wartungstätigkeiten im datenschutzrechtlichen Sinn sind und daher nur den dazu ausdrücklich ermächtigten Personen möglich sein dürfen. Sollen im Zusammenhang mit derartigen Wartungstätigkeiten personenbezogene Daten von Nutzerinnen und Nutzern übermittelt und verarbeitet werden, ist die ausdrückliche Zustimmung der für die Daten verantwortlichen Stelle erforderlich.

Die meisten der derzeit angebotenen Verfahren zum automatischen Software-Update werden diesen aus dem deutschen Datenschutzrecht folgenden Anforderungen nicht gerecht. Insbesondere fehlt vielfach die Möglichkeit, dem Update-Vorgang ausdrücklich zuzustimmen. Die Daten verarbeitenden Stellen dürfen daher derartige Online-Updates nicht nutzen, um Softwarekomponenten ohne separate Tests und formelle Freigabe auf Produktionssysteme einzuspielen.

Auch für private Nutzerinnen und Nutzer sind die automatischen Update-Funktionen mit erheblichen Risiken für den Schutz der Privatsphäre verbunden. Den Erfordernissen des Datenschutzes kann nicht ausreichend Rechnung getragen werden, wenn unbemerkt Daten an Softwarehersteller übermittelt werden und somit die Anonymität der Nutzerinnen und Nutzer gefährdet wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher die Softwarehersteller auf, überprüfbare, benutzerinitiierte Update-Verfahren bereitzustellen, die nicht zwingend einen Online-Datenaustausch mit dem Zielrechner erfordern. Auch weiterhin sollten datenträgerbasierte Update-Verfahren angeboten werden, bei denen lediglich die für den Datenträgerversand erforderlichen Daten übertragen werden. Automatisierte Online-Update-Verfahren sollten nur wahlweise angeboten werden. Sie sind so zu modifizieren, dass sowohl der Update- als auch der Installationsprozess transparent und revisionssicher sind. Software-Updates dürfen in keinem Fall davon abhängig gemacht werden, dass den Anbietern ein praktisch nicht kontrollierbarer Zugriff auf den eigenen Rechner gewährt werden muss. Personenbezogene Daten dürfen nur dann übermittelt werden, wenn der Verwendungszweck vollständig bekannt ist und in die Verarbeitung ausdrücklich eingewilligt wurde. Dabei ist in jedem Fall das gesetzlich normierte Prinzip der Datensparsamkeit einzuhalten.

21. Anlage: Entschließung der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. September 2003 in Leipzig

Entschließung zum Gesundheitsmodernisierungsgesetz

Die Datenschutzkonferenz begrüßt, dass mit den gesetzlichen Regelungen zur Gesundheitskarte und zu dem bei den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung gebildeten zentralen Datenpool datenschutzfreundliche Lösungen erreicht werden konnten. Die Gesundheitskarte unterliegt auch künftig der Verfügungsgewalt der Patientinnen und Patienten. Für den quartals- und sektorenübergreifenden Datenpool dürfen nur pseudonymisierte Daten gespeichert werden.

Die Datenschutzkonferenz wendet sich nicht grundsätzlich gegen zusätzliche Kontrollmechanismen der Krankenkassen.

Die Datenschutzbeauftragten kritisieren, dass sie zu wesentlichen, erst in letzter Minute eingeführten und im Schnellverfahren realisierten Änderungen nicht rechtzeitig und ausreichend beteiligt wurden. Diese Änderungen bedingen erhebliche Risiken für die Versicherten:

- Für das neue Vergütungssystem werden künftig auch die Abrechnungen der ambulanten Behandlungen mit versichertenbezogener Diagnose an die Krankenkassen übermittelt. Mit der vorgesehenen Neuregelung könnten die Krankenkassen rein tatsächlich umfassende und intime Kenntnisse über 60 Millionen Versicherte erhalten. Die Gefahr gläserner Patientinnen und Patienten rückt damit näher. Diese datenschutzrechtlichen Risiken hätten durch die Verwendung moderner und datenschutzfreundlicher Technologien einschließlich der Pseudonymisierung vermieden werden können. Leider sind diese Möglichkeiten überhaupt nicht berücksichtigt worden.

- Ohne strenge Zweckbindungsregelungen könnten die Krankenkassen diese Daten nach den verschiedensten Gesichtspunkten auswerten (z. B. mit data-warehouse-systemen).

Die Datenschutzkonferenz nimmt anerkennend zur Kenntnis, dass vor diesem Hintergrund durch Beschlussfassung des Ausschusses für Gesundheit und Soziale Sicherheit eine Klarstellung dahingehend erfolgt ist, dass durch technische und organisatorische Maßnahmen sicherzustellen ist, dass zur Verhinderung von Versichertenprofilen bei den Krankenkassen

- eine sektorenübergreifende Zusammenführung der Abrechnungs- und Leistungsdaten unzulässig ist und dass

- die Krankenkassen die Daten nur für Abrechnungs- und Prüfzwecke nutzen dürfen.

Darüber hinaus trägt eine Entschließung des Deutschen Bundestages der Forderung der Datenschutzkonferenz Rechnung, durch eine Evaluierung der Neuregelung in Bezug auf den Grundsatz der Datenvermeidung und Datensparsamkeit unter Einbeziehung der Möglichkeit von Pseudonymisierungsverfahren sicherzustellen, dass Fehlentwicklungen vermieden werden.

Die Datenschutzkonferenz hält eine frühestmögliche Pseudonymisierung der Abrechnungsdaten für notwendig, auch damit verhindert wird, dass eine Vielzahl von Bediensteten personenbezogene Gesundheitsdaten zur Kenntnis nehmen kann.

22. Anlage: Entschließung der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. September 2003 in Leipzig

Konsequenzen aus der Untersuchung des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Mai dieses Jahres sein im Auftrag des Bundesministeriums der Justiz erstelltes Gutachten „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen“ vorgelegt. Darin hat es festgestellt, dass

- die Zahl der Ermittlungsverfahren, in denen TKÜ-Anordnungen erfolgten, sich im Zeitraum von 1996 bis 2001 um 80 % erhöht (1996: 2.149; 2001; 3.868) hat,

- die Gesamtzahl der TKÜ-Anordnungen pro Jahr im Zeitraum von 1990 bis 2000 von 2.494 um das Sechsfache auf 15.741 gestiegen ist,

- sich die Zahl der jährlich davon Betroffenen im Zeitraum von 1994 bis 2001 von 3.730 auf 9.122 fast verdreifacht hat,

- in 21 % der Anordnungen zwischen 1.000 und 5.000 Gespräche, in 8 % der Anordnungen mehr als 5.000 Gespräche abgehört worden sind,

- der Anteil der staatsanwaltschaftlichen Eilanordnungen im Zeitraum von 1992 bis 1999 von ca. 2 % auf ca. 14 % angestiegen ist,

- die Beschlüsse in ca. 3/4 aller Fälle das gesetzliche Maximum von 3 Monaten umfassen, 3/4 aller Maßnahmen tatsächlich aber nur bis zu 2 Monaten andauern,

- lediglich 24 % der Beschlüsse substantiell begründet werden,

- es nur in 17 % der Fälle Ermittlungserfolge gegeben hat, die sich direkt auf den die Telefonüberwachung begründenden Verdacht bezogen,

- 73 % der betroffenen Anschlussinhaberinnen und -inhaber nicht über die Maßnahme unterrichtet wurden.

Die Telefonüberwachung stellt wegen ihrer Heimlichkeit und wegen der Bedeutung des Rechts auf unbeobachtete Kommunikation einen gravierenden Eingriff in das Persönlichkeitsrecht der Betroffenen dar, zu denen auch unbeteiligte Dritte gehören. Dieser Eingriff kann nur durch ein legitimes höherwertiges Interesse gerechtfertigt werden. Nur die Verfolgung schwerwiegender Straftaten kann ein solches Interesse begründen. Vor diesem Hintergrund ist der Anstieg der Zahl der Verfahren, in denen Telefonüberwachungen angeordnet werden, kritisch zu bewerten. Dieser kann – entgegen häufig gegebener Deutung – nämlich nicht allein mit dem Zuwachs der Anschlüsse erklärt werden. Telefonüberwachungen müssen ultima ratio bleiben. Außerdem sind die im Gutachten des Max-Planck-Instituts zum Ausdruck kommenden strukturellen Mängel zu beseitigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber und die zuständigen Behörden auf, aus den Ergebnissen der Untersuchung daher folgende Konsequenzen zu ziehen:

- Der gesetzliche Richtervorbehalt darf nicht aufgelockert werden. Die Verwertung der angefertigten Aufzeichnungen sollte in Fällen staatsanwaltschaftlicher Eilanordnungen davon abhängig gemacht werden, dass ein Gericht rückwirkend deren Rechtmäßigkeit feststellt.

- Um die Qualität der Entscheidungen zu verbessern, sollte die Regelung des § 100b StPO dahin gehend ergänzt werden, dass die gesetzlichen Voraussetzungen der Anordnung einzelfallbezogen darzulegen sind. Die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen sollten gesetzlich geregelt werden (z. B. Beweisverwertungsverbote).

- Um die spezifische Sachkunde zu fördern, sollten die Aufgaben der Ermittlungsrichterinnen und -richter auf möglichst wenige Personen konzentriert werden. Die Verlagerung auf ein Kollegialgericht ist zu erwägen.

- Der Umfang des – seit Einführung der Vorschrift regelmäßig erweiterten – Straftatenkataloges des § 100a StPO muss reduziert werden.

- Um eine umfassende Kontrolle der Entwicklung von TKÜ-Maßnahmen zu ermöglichen, muss in der StPO eine Pflicht zur zeitnahen Erstellung aussagekräftiger Berichte geschaffen werden. Jedenfalls bis dahin muss auch die in § 88 Abs. 5 TKG festgelegte Berichtspflicht der Betreiber von Telekommunikationsanlagen und der Regulierungsbehörde beibehalten werden.

- Der Umfang der Benachrichtigungspflichten, insbesondere der Begriff der Beteiligten, ist im Gesetz näher zu definieren, um die Rechte – zumindest aller bekannten – Gesprächsteilnehmerinnen und -teilnehmer zu sichern. Für eine längerfristige Zurückstellung der Benachrichtigung ist zumindest eine richterliche Zustimmung entsprechend § 101 Abs. 1 Satz 2 StPO vorzusehen. Darüber hinaus müssen die Strafverfolgungsbehörden beispielsweise durch Berichtspflichten angehalten werden, diesen gesetzlich festgeschriebenen Pflichten nachzukommen.

- Zum Schutz persönlicher Vertrauensverhältnisse ist eine Regelung zu schaffen, nach der Gespräche zwischen den Beschuldigten und zeugnisverweigerungsberechtigten Personen grundsätzlich nicht verwertet werden dürfen.

- Zur Sicherung der Zweckbindung nach § 100b Abs. 5 StPO und § 477 Abs. 2 Satz 2 StPO muss eine gesetzliche Verpflichtung zur Kennzeichnung der aus TKÜ-Maßnahmen erlangten Daten geschaffen werden.

- Die Höchstdauer der Maßnahmen sollte von drei auf zwei Monate reduziert werden.

- Auch aufgrund der Weiterentwicklung der Technik zur Telekommunikationsüberwachung (z. B. IMSI-Catcher, stille SMS, Überwachung des Internetverkehrs) ist eine Fortführung der wissenschaftlichen Evaluation dieser Maßnahmen unabdingbar. Die gesetzlichen Regelungen sind erforderlichenfalls deren Ergebnissen anzupassen.

23. Anlage: Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 21. November 2003

Gravierende Verschlechterungen des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes

Die Bundesregierung hat am 15. Oktober 2003 den Entwurf für ein neues Telekommunikationsgesetz beschlossen. Dieser Entwurf sieht jetzt zwar – entsprechend der Forderung der Datenschutzbeauftragten – die vorläufige Beibehaltung der Unternehmensstatistik zu Überwachungsmaßnahmen vor; im Übrigen enthält er aber gravierende Verschlechterungen des Datenschutzniveaus.

Insbesondere berechtigt der Gesetzentwurf die Diensteanbieter, grundsätzlich alle entstehenden Verkehrsdaten (also auch alle Zielrufnummern) unverkürzt bis zu sechs Monaten nach Versendung der Rechnung zu speichern. Damit wird ohne Not und ohne überzeugende Begründung eine Regelung aufgegeben, die bisher die Speicherung von verkürzten Zielrufnummern vorsieht, wenn die Kundinnen und Kunden sich nicht für die vollständige Speicherung oder vollständige Löschung entscheiden. Die bisherige Regelung berücksichtigt in ausgewogener Weise sowohl die Datenschutz- als auch die Verbraucherschutzinteressen der beteiligten Personen und hat sich in der Praxis bewährt. Vollends inakzeptabel ist die inzwischen vom Rechtsausschuss des Bundesrates vorgeschlagene Pflicht zur Vorratsdatenspeicherung für sechs Monate. Gegen eine solche Regelung bestehen erhebliche verfassungsrechtliche Bedenken.

Schon die von der Bundesregierung vorgeschlagene Regelung würde dazu führen, dass Millionen von Verkehrsdatensätzen selbst dann noch unverkürzt gespeichert bleiben und dem Zugriff anderer Stellen ausgesetzt sind, wenn die Diensteanbieter sie für ihre Abrechnungszwecke nicht mehr benötigen. Das im Entwurf weiterhin vorgesehene Recht der Kundinnen und Kunden, die Speicherung gekürzter Zielrufnummern oder ihre vollständige Löschung nach Rechnungsversand zu verlangen, wird daran wenig ändern, weil nur eine Minderheit es wahrnehmen wird. Die Beibehaltung des bisherigen angemessenen Datenschutzstandards sollte nicht von der Initiative der Betroffenen abhängig gemacht werden, sondern allen zugute kommen, die nicht ausdrücklich einer weitergehenden Speicherung zustimmen. Zudem sind die Rechte der angerufenen Teilnehmerinnen und Teilnehmer zu berücksichtigen, in die durch eine Speicherung der unverkürzten Verkehrsdaten zusätzlich eingegriffen wird.

Die Datenschutzbeauftragten haben zudem stets die Zwangsidentifizierung beim Erwerb von vertragslosen (prepaid) Handys als gesetzwidrig kritisiert und sehen sich jetzt in dieser Auffassung durch das Urteil des Bundesverwaltungsgerichts vom 22. Oktober 2003 (Az.: 6 C 23.02) bestätigt. Zugleich wenden sie sich gegen die mit der TKG-Novelle geplante Einführung einer derartigen Identifikationspflicht, die zu einer verdachtslosen Datenspeicherung auf Vorrat führen würde. Wer ein solches Handy kauft, gibt es häufig ab oder verschenkt es und ist deshalb nicht identisch mit der Person, die das Handy nutzt. Deshalb bringen diese Daten keinen nennenswerten Informationsgewinn für die Sicherheitsbehörden.

Schließlich soll den Strafverfolgungsbehörden, der Polizei und den Nachrichtendiensten ohne Bindung an einen Straftatenkatalog oder einen Richtervorbehalt der Zugriff auf Passwörter, PINs, PUKs usw. eröffnet werden, mit denen die Inhalte oder nähere Umstände einer Telekommunikation geschützt werden. Dies würde die Möglichkeit eröffnen, von dieser Befugnis unkontrolliert Gebrauch zu machen. Die Befugnis dürfte zudem häufig ins Leere laufen, da die Anbieter diese Daten aus Gründen der Datensicherheit für sie selbst unlesbar verschlüsselt speichern.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, den Entwurf bei den bevorstehenden Beratungen in diesen sensiblen Punkten zu korrigieren und den gebotenen Schutz des Telekommunikationsgeheimnisses sicherzustellen.

7. ABKÜRZUNGEN

AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
AO	Abgabenordnung
AWO	Arbeiterwohlfahrt
BAföG	Bundesausbildungsförderungsgesetz
BAT-Ost	Bundesangestelltentarif
BDSG	Bundesdatenschutzgesetz
BDH	Bundesverband für Rehabilitation und Interessenvertretung Behinderter
BfF	Bundesamt für Finanzen
BGBl.	Bundesgesetzblatt
BKA	Bundeskriminalamt
BMGS	Bundesministerium für Gesundheit und Soziale Sicherung
BNotO	Bundesnotarordnung
BOÄ	Berufsordnung für die Ärztinnen und Ärzte Mecklenburg-Vorpommern
BOS	Funkkommunikation von Behörden und Organisationen mit Sicherheitsaufgaben
BR-Drs.	Bundesrats-Drucksache
BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik

BSG	Bundessozialgericht
BT-Drs.	Bundestags-Drucksache
BVerfGE	Entscheidung des Bundesverfassungsgerichts (Band ..., Seite ...)
CD-ROM	Compakt Disk - Read Only Memory
CN	Corporate Network
DFKI	Deutsches Forschungszentrum für Künstliche Intelligenz
DHCP	Dynamic Host Configuration Protocol
DMP	Disease-Management-Programm
DNA-Analyse	Deoxyribonucleic Acid
DNS	Domain Name System
DRM	Digital Rights Management
DSG M-V	Landesdatenschutzgesetz
DVD	Digital Versatile Disk
EFS	Encrypting File System
EstG	Einkommensteuergesetz
EVA	Elektronischer Vorgangsassistent
EU	Europäische Union
FAQ	Frequently Asked Questions
FAR	False Acception Rate

FER	False Enrollment Rate
FRR	False Rejection Rate
GdP	Gewerkschaft der Polizei
GEZ	Gebühreneinzugszentrale
GewO	Gewerbeordnung
GG	Grundgesetz
GI	Gesellschaft für Informatik e. V.
GSM	Global System for Mobile Communication
HP	Hewlett-Packard
Host-Namen	Rechnernamen
http	Hypertext Transport Protocol
ID	Identifier
IDS	Intrusion Detection System
IGD	Fraunhofer Institut für graphische Datenverarbeitung Darmstadt
IMA-IT	Interministerieller Ausschuss für Informations- und Kommunikationstechnik
IMEI	International Mobile Equipment Identity
IMK	Konferenz der Innenminister der Länder
IMSI	International Mobile Subscriber Identity
INPOL	Informationssystem der Polizei

IP	Internet Protocol
IT	Informationstechnik
KitaG	Kindertagesstättengesetz
KiföG	Gesetz zur Förderung von Kindern in Tageseinrichtungen und in Tagespflege
LAN	Lokal Area Network (lokales Netz)
LBG M-V	Landesbeamtengesetz Mecklenburg-Vorpommern
LDL-Apherese	Low Density Lipoproteins – Apherese (Eliminationstherapie)
LKA M-V	Landeskriminalamt Mecklenburg-Vorpommern
LKatSG M-V	Landeskatastrophenschutzgesetz Mecklenburg-Vorpommern
LKHG M-V	Landeskrankenhausgesetz Mecklenburg-Vorpommern
LKSt	Landeskoordinierungstelle für Informations- und Telekommunikationstechnik
LMG	Landesmeldegesetz
LT-Drs.	Landtagsdrucksache
LverfG	Landesverfassungsgericht
LVerfSchG M-V	Landesverfassungsschutzgesetz Mecklenburg-Vorpommern
LVersA M-V	Landesversorgungsamt Mecklenburg-Vorpommern
MAC	Media Accsess Code
MDK	Medizinischer Dienst der Krankenversicherung

MoZArT	Modellvorhaben zur Zusammenarbeit zwischen Arbeits- und Sozialämtern
NDR	Norddeutscher Rundfunk
NGSCB	Next-Generation Secure Computing Base
ÖGDG M-V	Gesetz über den Öffentlichen Gesundheitsdienst im Land Mecklenburg-Vorpommern
OWiG	Gesetz über Ordnungswidrigkeiten
PC	Personalcomputer
PED	Polizeiliche Erkenntnisdatei
PIN	Persönliche Identifikations-Nummer
RegTP	Regulierungsbehörde für Telekommunikation und Post
SchulG M-V	Schulgesetz Mecklenburg-Vorpommern
SGB I	Sozialgesetzbuch Erstes Buch
SGB IV	Sozialgesetzbuch Viertes Buch
SGB V	Sozialgesetzbuch Fünftes Buch
SGB VI	Sozialgesetzbuch Sechstes Buch
SGB VII	Sozialgesetzbuch Siebtes Buch
SGB VIII	Sozialgesetzbuch Achtes Buch
SGB X	Sozialgesetzbuch Zehntes Buch
SigG	Signaturgesetz

SigV	Signaturverordung
SMS	Short Message Service
SIM-Karte	Subscriber Identification Module
SOG M-V	Gesetz über die öffentliche Sicherheit und Ordnung Mecklenburg-Vorpommern
SSID	Service Set Identifier
StDÜV	Steuerdaten-Übermittlungsverordnung
StGB	Strafgesetzbuch
StVG	Straßenverkehrsgesetz
TAB	Büro für Technikfolgenabschätzung beim Deutschen Bundestag
TCP	Transmission Control Protocol
TCPA	Trusted Computing Platform Alliance
TPM	Trusted Platform Modul
TSS	Trusted Platform Support Service
TÜViT	Technischer Überwachungsverein Informationstechnik
UMTS	Universal Mobile Telecommunication System
USB	Universal Serial Bus
Verf M-V	Verfassung des Landes Mecklenburg-Vorpommern
VermKatG	Vermessungs- und Katastergesetz
VwVfG	Verwaltungsverfahrensgesetz

VNC	Virtual Network Computing
WEP	wired equivalent privacy
WLAN	Wireless-Local Area Network
ZED	Zentralstelle für die Vorbereitung der Einführung eines bundesweit einheitlichen digitalen Sprech- und Datenfunksystems

8. STICHWORTVERZEICHNIS

9. PUBLIKATIONEN

Beim Landesbeauftragten für den Datenschutz sind derzeit folgende Publikationen kostenlos erhältlich bzw. stehen im Internetangebot unter [www.lfd.m-v.de] zum Abruf bereit:

Broschüren

- 1. Tätigkeitsbericht für den Zeitraum 1992/93
- 2. Tätigkeitsbericht für den Zeitraum 1994/95
- 3. Tätigkeitsbericht für den Zeitraum 1996/97
- 4. Tätigkeitsbericht für den Zeitraum 1998/99
- 5. Tätigkeitsbericht für den Zeitraum 2000/01
- 6. Tätigkeitsbericht für den Zeitraum 2002/03

- Landesdatenschutzgesetz 2002 mit Erläuterungen
- Gesetze und Verordnungen zum Datenschutz (Loseblattsammlung)

- Datenschutzgerechtes E-Government (Handlungsempfehlungen und datenschutzfreundliche Lösungen für die Verwaltung)
- Vom Bürgerbüro zum Internet - Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung
- Datenschutz im Krankenhaus
- Datenschutzfreundliche Technologien
- Technik und Datenschutz (Arbeitsergebnisse und Tagungsunterlagen des Arbeitskreises Technik)

- Bundesdatenschutzgesetz (Text und Erläuterungen)
- Schutz der Sozialdaten
- Datenschutz in der Telekommunikation

Infoblätter

- Datenschutz – was ist das?
- Ihre Datenschutzrechte im Meldewesen
- Datenschutz und Telefax
- Datenschutz und Statistik
- Handys – Komfort nicht ohne Risiko

Orientierungshilfen

- Empfehlungen zur Passwortgestaltung und zum Sicherheitsmanagement
- Transparente Software - eine Voraussetzung für datenschutzfreundliche Technologien
- Forderung an Wartung und Fernwartung von DV-Anlagen
- Data Warehouse und Data Mining im öffentlichen Bereich (Datenschutzrechtliche und -technische Aspekte)
- Datenschutz bei Windows XP Professional
- TCPA, Palladium und DRM

- Datensicherheit bei USB-Geräten
- Datenschutzfragen zum Anschluss von Netzen der öffentlichen Verwaltung an das Internet
- Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten
- Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz
- Datenschutzfragen zur Präsentation von öffentlichen Stellen im Internet
- Datenschutz und Internet in der Schule

- Datenschutzgerechte Vernichtung von Schriftgut mit personenbezogenen Daten
- Anforderungen zur informationstechnischen Sicherheit bei Chipkarten
- Datenschutzrechtliche Aspekte beim Einsatz optischer Datenspeicherung
- Datenschutz und Telefax
- Datenschutz in kommunalen Vertretungsorganen
- Datenschutz und Telemedizin - Anforderungen an Medizinnetze -
- Datenschutz bei Telearbeit

Muster

- Mustervertrag zur Verarbeitung personenbezogener Daten im Auftrag
- Mustervertrag zur datenschutzgerechten Vernichtung von Schriftgut mit personenbezogenen Daten
- Musterdienstvereinbarung über die Nutzung der Telekommunikationsanlage
- Musterdienstvereinbarung zur Nutzung von Internetdiensten
- Muster einer Verpflichtungserklärung zum Datengeheimnis gemäß § 6 DSG M-V
- Muster einer Bestellung zur oder zum behördlichen Datenschutzbeauftragten

Formulare

- Verfahrensbeschreibung nach § 18 DSG M-V; Hinweise zur Führung der Verfahrensbeschreibung
- Widerspruch gegen die Weitergabe der Meldedaten gemäß §§ 32, 35 Landesmeldegesetz

Weitere Informationen unter:

www.bfd.bund.de
www.lfd.m-v.de
www.datenschutz.de (Virtuelles Datenschutzbüro)