LANDTAG DES SAARLANDES
11. Wahlperiode

Drucksache 11/1926
26.02.99

SIEBZEHNTER BERICHT

über die

Tätigkeit des Landesbeauftragten für Datenschutz gemäß § 27 des Saarländischen Gesetzes zum Schutz personenbezogener Daten
(Berichtszeitraum: 1997/1998)

Ausgegeben: 12.03.99

17. Tätigkeitsbericht

des

Landesbeauftragten für Datenschutz

für die Jahre 1997 und 1998

dem Landtag und der Landesregierung

vorgelegt am 26. Februar 1999

(Landtagsdrucksache 11 / 1926)

Der Landesbeauftragte
für Datenschutz Saarland
Bernd Dannemann

Fritz-Dobisch-Str. 12, 66111 Saarbrücken
Postfach 102631, 66026 Saarbrücken
Tel.: 0681/94781-0, Fax: 0681/94781-29
E-Mail-Adresse: lfd-saar@t-online.de
Internet-Angebot unter www.lfd.saarland.de

Saarbrücken 1999

Inhaltsverzeichnis

1 Vorbemerkung

Die Jahre 1997 und 1998, auf die sich dieser Bericht bezieht, zeichnen kein einheitliches Bild von der Entwicklung des Datenschutzes. Es gibt ermutigende Zeichen bei Bürgern und datenverarbeitenden Stellen, die von einem gewachsenen Bewußtsein dieses Grundrechts zeugen. Gleichfalls feststellbar ist andererseits erhebliche Nachlässigkeit - auch im übrigen der Betroffenen selbst - im täglichen Umgang mit personenbezogenen Daten, und nicht immer hat man den Eindruck, daß Gesetzgeber und Verwaltung vorrangig bestrebt sind, den Freiheitsraum zu erweitern. Dies gilt überregional ebenso wie für den öffentlichen Bereich im Saarland, auf den sich meine Beratungs- und Kontrolltätigkeit konzentriert.

Der Rang, den Bürgerinnen und Bürgern ihrem Grundrecht auf informationelle Selbstbestimmung einräumen, ist hoch; viele sehen sich derzeit bei privater und öffentlicher Datenverarbeitung in ihrer Privatsphäre beeinträchtigt und wünschen sich einen verstärkten Schutz. Dies kommt in einer bundesweiten Meinungsumfrage zum Ausdruck, die im vergangenen Herbst veröffentlicht wurde.

In einer repräsentativen Befragung durch das Hamburger BAT-Freizeitforschungsinstitut hatte ein großer Teil Mißtrauen gegenüber Institutionen und Unternehmen hinsichtlich eines sorgsamen Umgangs mit ihren Daten bekundet. Sehr viele hielten ihre Daten selbst bei denjenigen Stellen nicht für absolut geschützt, die sie als besonders vertrauensvoll einschätzten. Und leider sahen sie für sich oft keine effektive Möglichkeit einer Gegenwehr.

Die beste Möglichkeit ist, schon bei Auswahl der Geräte, Techniken und Verfahren (oder der Kontaktpartner, die diese verwenden) darauf zu setzen, daß Daten gar nicht erfaßt oder gespeichert oder daß solche allenfalls in möglichst geringem Umfang weiter verarbeitet werden. Diese Chance einer selbstbestimmten Entscheidung setzt natürlich eine entsprechende Auswahlmöglichkeit voraus, die der einzelne nur bedingt hat oder erkennt. Gut wäre, wenn das Prinzip der Datensparsamkeit von vornherein bereits "eingebaut" würde; mit Anreizen und normativen Vorgaben könnte hierauf hingewirkt werden. Die Erforderlichkeit datenschutzfreundlicher Technologien haben die Datenschutzbeauftragten in einer Entschließung vom 23./24. Oktober 1997 (Anlage 19.9) betont.

Nicht immer wird dies gelingen. Um so wichtiger ist, daß der Gesetzgeber selbst, wenn er mit wichtigen Gemeinschaftsinteressen abwägt, gebührend auf den Schutz der Privatheit achtet, und daß er die Verwaltungen zu entsprechendem Handeln anhält (und ihnen hierzu ausreichende Möglichkeiten gibt).

Während der Landtag sich im Berichtszeitraum nur mit verhältnismäßig wenigen Vorhaben befaßte, die herausragende Bedeutung für das Recht auf

informationelle Selbstbestimmung hatten, war die Normsetzung auf Bundesebene zum Ende der Legislaturperiode des Bundestages in dieser Beziehung um so intensiver. Allerdings gilt gerade hier, daß die beschlossenen Gesetze keineswegs immer die Freiheitssphäre des Einzelnen erweitert haben. Bei unserer Beteiligung im Vorfeld hatten wir Datenschutzbeauftragten in vielen Fällen auf Verbesserungen gedrungen, nur teilweise jedoch mit Erfolg.

Zu den positiven Beispielen gehört die Multimedia-Gesetzgebung im Bund (und parallel bei den Ländern) (TZ 17.1). Bei der Masse der Gesetzesarbeit fällt das Urteil eher indifferent aus wie bei dem jetzt endlich erlassenen Justizmitteilungsgesetz (TZ 5.3). Besonders kritisch mußten wir zu Vorschriften Stellung nehmen, mit denen im Interesse der Strafverfolgung oder Gefahrenabwehr sowie zu Kontrollzwecken bei Gewährung staatlicher Leistungen tief in die Privatsphäre von Bürgerinnen und Bürgern eingegriffen wurde, wie etwa dem "Großen Lauschangriff" (TZ 5.1), der DNA-Identitätsfeststellung (TZ 5.2), Zugriffsmöglichkeiten für Sicherheitsorgane in der Telekommunikation (TZ 17.1) und dem Mißbrauchsabgleich bei Sozialleistungen (TZ 10.1) oder gar der Aufenthaltsmitteilung bei Empfang solcher Leistungen (TZ 10.3). Die Einwände betrafen grundsätzlich nicht das Anliegen als solches, sondern das Zurücksetzen individueller Freiheit. Zu vermissen ist vielfach auch, daß eine "Erfolgskontrolle" hinsichtlich der geschaffenen Eingriffsmöglichkeiten und ihrer Grundrechtsverträglichkeit unterbleibt; für den Sicherheitsbereich haben meine Kollegen und ich dies mit Entschließung vom 5./6. Oktober 1998 (Anlage 19.17) betont und von Regierung und Gesetzgeber eingefordert.

Wenn in der genannten Untersuchung ein Großteil der Befragten mangelnde Aufsicht als Ursache für unzureichenden Datenschutz nennt, stützt dies die Forderung der Datenschutzbeauftragten, daß die Verwaltungsleitungen selbst sich hierum kümmern und für genügende Hilfen und ausreichende Unterrichtung der Mitarbeiter sorgen. Es belegt auch den Wunsch nach effektiveren Möglichkeiten der externen Datenschutzkontrolle.

Ich habe bei den öffentlichen Stellen, mit denen ich zu tun hatte, zwar großenteils wachsendes Verständnis und vielfach auch Bemühen um angemessenen Schutz feststellen können, und ich gebe auch gern Hilfe, diesen Schutz noch zu verbessern. Zufrieden kann ich aber keineswegs sein. Noch immer fehlt es bei vielen Stellen an elementarsten Vorkehrungen, wie sich bei Querschnittsprüfungen ergeben hat (TZ 3.6, 6.8). Vielleicht war der Eindruck, den ich vor meinem letzten Bericht gewonnen hatte, doch zu positiv.

Meine Kontroll- und (zunehmend) Beratungstätigkeit kann bei der Vielzahl der Stellen und Sachbereiche immer nur punktuell wirken. Erst recht gibt die Darstellung der Tätigkeit in diesem Bericht stets lediglich einen Ausschnitt wieder und versucht auch gar nicht, nach Arbeitsintensität oder vermuteter Vielzahl von Betroffenen zu gewichten. Die Hinweise und ihre Veröffentli-

chung haben exemplarischen Charakter. Ihre Mitteilung an Regierung und Parlament soll natürlich auch dazu dienen, über Aufsicht und parlamentarische Kontrolle das im konkreten Fall umzusetzen, was nicht bereits im unmittelbaren Kontakt mit den Verwaltungen selbst gelungen ist. Vor allem aber geht es darum, die Problematik deutlich zu machen und festgestellte Mängel bei vergleichbaren anderen Stellen zu vermeiden oder auszuräumen.

Der Ausschuß für Datenschutz des Saarländischen Landtags hat in mehreren Sitzungen meinen vergangenen (16.) Tätigkeitsbericht erörtert, ohne allerdings ein abschließendes Ergebnis festgestellt zu haben. Er hat sich darüber hinaus - auch in meiner Dienststelle - mit Einzelfragen beschäftigt, etwa zu der Nutzung des Internet. Das Landtagsplenum hat sich mit diesen Fragen im Berichtszeitraum nicht eingehender befaßt. Eine solche Behandlung, wie sie in anderen Bundesländern bestimmt oder üblich ist, könnte durchaus im Parlament selbst die wünschenswerte Offenheit für Datenschutzfragen steigern.

Die Veröffentlichung des Berichts soll auch bei den Betroffenen das Bewußtsein schärfen, daß Grundrechtsschutz nicht in vollkommener Weise selbstverständlich ist, sondern schrittweise errungen werden muß. Jeder hat die Möglichkeit, selbst hierzu beizutragen: durch Aufmerksamkeit, Auswahl sparsamer Verfahren und bewußte Entscheidung, wenn er in bestimmte Verarbeitungen einwilligt, mit eigenen Rechten gegenüber den verantwortlichen Stellen, und selbstverständlich kann er sich unmittelbar an mich wenden, wenn er sich in der Verarbeitung seiner Daten durch eine öffentliche Stelle im Land verletzt glaubt.

2 Allgemeines Datenschutzrecht

2.1 Europäischer Datenschutz

Zwar gelang es bisher nicht, den grundrechtlichen Charakter des Datenschutzes im Primärrecht der europäischen Union selbst zu verankern. Mit der weiteren Fortschreibung des Gemeinschaftsrechts im Vertrag von Amsterdam wurden aber immerhin die Pflichten der EU-Organe und -Institutionen klargestellt. Die Konkretisierung hinsichtlich einer europäischen Kontrollinstanz steht noch aus.

Die Europäische Union bemüht sich um weitere Konkretisierung des Persönlichkeitsschutzes durch Vorgaben für die jeweiligen Mitgliedsstaaten; neben der EG-Datenschutzrichtlinie ist besonders auf die bereits erlassene Telekommunikationsrichtlinie hinzuweisen, die allerdings bis Oktober 1998 in nationales Recht hätte umgesetzt werden müssen. Die Beteiligung der Datenschutzbeauftragten des Bundes und der Länder bereits in der Vorbereitung trägt der zunehmenden Bedeutung europaweiten Rechts Rechnung.

Wesentlich erscheint die Verpflichtung zum Schutz der Privatsphäre auch in den Bereichen außerhalb der "ersten Säule" des Vertragsrechts. Speziell für die Verarbeitung höchst sensibler Daten bei EUROPOL bestand Anlaß, gelegentlich der Verhandlungen zur Fortentwicklung mit einer Entschließung auf den auch vom Europäischen Parlament betonten Schutzbedarf aufmerksam zu machen (Anlage 19.4). Aus rechtspolitischer Sicht zweifelhaft ist, daß zwischenzeitlich den EUROPOL-Bediensteten bei ihrer Tätigkeit Immunität eingeräumt wurde, denn dies erschwert die Kontrollmöglichkeit.

2.2 Umsetzung der EG-Datenschutzrichtlinie

Bereits im letzten Bericht (TZ 6.1) habe ich auf die von Rat und Parlament der Europäischen Union am 24. Oktober 1995 verabschiedete Richtlinie hingewiesen, die den Datenschutz in den Mitgliedsstaaten auf einem hohen Niveau harmonisieren soll. Dies soll zugleich innerhalb der EU einen grenzüberschreitenden Datenverkehr ohne Beschränkungen möglich machen und vermeiden, daß Datenverarbeitungen aus Wettbewerbsgründen in Länder mit unangemessen niedrigem Standard verlagert werden. Die hierfür gesetzte dreijährige Umsetzungsfrist ist mittlerweile abgelaufen, ohne daß in Deutschland die notwendigen legislatorischen Konsequenzen gezogen worden wären; bis Ende 1998 haben lediglich Hessen und Brandenburg ihre Landes-Datenschutzgesetze novelliert, in manchen anderen Ländern wurden jedenfalls Entwürfe vorgelegt.

Daß - trotz wiederholter Erinnerungen von verschiedenster Seite - gerade das zentrale Datenschutzgesetz des Bundes nicht rechtzeitig geändert wurde, ist dabei besonders bedauerlich. Denn die Verbesserungen des Persönlichkeitsschutzes der Bürger sollen nach der Zielrichtung der Richtlinie gerade auch im privatwirtschaftlichen Bereich wirksam werden, für den die datenschutzrechtlichen Regelungen großenteils im Bundesdatenschutzgesetz getroffen werden. Bei der europäischen Harmonisierung können die meisten Vorschriften dieses Gesetzes nicht unverändert fortbestehen.

Zu wünschen wäre auch gewesen, über die Modernisierung des Bundesgesetzes Leitlinien auch für die Ländergesetzgebung zu setzen und damit die Chance zu nutzen, ebenfalls im öffentlichen Bereich ein Auseinanderlaufen von Begrifflichkeiten und Inhalten zu vermeiden. Wie in anderen Ländern auch war das Zuwarten auf die modellhafte Umsetzung auf Bundesebene für die saarländische Landesregierung Grund dafür, von eigenen Initiativen für die Anpassung des Landesrechts abzusehen, und zwar auch dort, wo der Sachzusammenhang sie bereits nahegelegt hätte (vgl. TZ 17.2).

Für die Anpassung des BDSG mag es kein Nachteil sein, daß der Entwurf des Bundesinnenministeriums gar nicht mehr in das Gesetzgebungsverfahren eingebracht worden ist, denn obwohl er gesetzestechnisch außerordentlich umfänglich war, zielte er inhaltlich bewußt auf eine Minimal-Änderung

ohne gleichzeitige Modernisierung. Insoweit ist noch Spielraum für eine offene Diskussion, die die Vorschläge der Datenschutzbeauftragten des Bundes und der Länder berücksichtigt.

Ein Jahr vor Ablauf der Umsetzungsfrist haben meine Kollegen und ich mit einer Entschließung (Anlage 19.7) noch die wesentlichen Aspekte zusammengefaßt, die Gegenstand einer Novelle des Bundesdatenschutzgesetzes werden sollten. Sie sind nach wie vor aktuell.

Nach Beginn der neuen Legislaturperiode muß nunmehr zügig mit der Novellierung begonnen werden; die Koalitionsvereinbarung der jetzigen Mehrheitsfraktionen im Deutschen Bundestag enthält eine entsprechende Absichtserklärung, ohne allerdings bereits inhaltliche Vorgaben zu setzen. Immerhin hatte bereits die Fraktion Bündnis 90 / Die Grünen im letzten Deutschen Bundestag einen Gesetzentwurf vorgestellt, der über die bloße Anpassung hinausreicht.

Auf Landesebene wird man mit der Umsetzung ebenfalls nicht länger warten können.

Die Bundesrepublik und auch die einzelnen Bundesländer riskieren ein Vertragsverletzungsverfahren wegen nicht rechtzeitiger Umsetzung, dessen Einleitung durch die EU-Kommission bereits angesprochen wurde. Aber auch ohne daß - mit oder ohne diesen Druck - die Bundes- und Landesgesetze förmlich geändert sind, hat die EG-Datenschutzrichtlinie bereits rechtliche Auswirkungen. Als an die Mitgliedsstaaten gerichtete Pflicht bindet sie ohne gesetzliche Anpassung zwar nicht die Bürger, wohl aber die rechtsanwendenden Verwaltungsstellen und Gerichte, soweit sie inhaltlich unbedingt und hinreichend bestimmbar ist und dem einzelnen Bürger subjektive Rechte gegenüber dem Mitgliedsstaat verleiht. Sie ist natürlich auch bereits bei Auslegung der vorhanden Regelungen zu beachten. Auf die entsprechende ständige Rechtsprechung des Europäischen Gerichtshofs habe ich die Ressorts hingewiesen, denen ja aufgetragen ist, für ihren Geschäftsbereich die Ausführung der Rechtsvorschriften über den Datenschutz sicherzustellen.

Bereits jetzt zu beachten sind insbesondere

- das grundsätzliche Verbot, besondere Kategorien von Daten wie etwa Gesundheitsdaten außerhalb solcher Bereiche zu verarbeiten, für die fachspezifisch angemessene Garantien festgelegt sind,
- die Verpflichtung, begründete Einwände Betroffener auch gegen rechtmäßige Datenverarbeitung zu prüfen und zu berücksichtigen,
- erweiterte Rechte der Betroffenen auf Information über die Verarbeitung sowie engere Ausnahmen, die Auskunft an sie zu verweigern.

2.3 Datenschutzmodernisierung

Obwohl das Datenschutzrecht noch vergleichsweise jung ist, besteht in der Fachöffentlichkeit kein Zweifel daran, daß es bereits grundlegender Modernisierung bedarf. Zu sehr ist es noch geprägt von technischen Konzepten, die vielen als überholt gelten, und trotz einer Fülle von Normen, die selbst der Fachmann nicht mehr überschauen kann, lassen sich wichtige Aspekte gar nicht in das geltende Recht einpassen. Globale elektronische Kommunikation im Internet, Chipkarten, Videoüberwachung sind alltägliche Realität, aber Rechtssicherheit - vor allem gesicherten Schutz von Freiheitsrechten - gibt es längst noch nicht überall.

Die Überlegungen zur Modernisierung des Datenschutzrechts zielen zunehmend auch darauf, es in den größeren Zusammenhang einer allgemeinen Informationsordnung einzubinden. Nicht erstmals, aber besonders vernehmlich wurde dies in Deutschland im vergangenen Jahr in verschiedenen Veröffentlichungen zum 62. Deutschen Juristentags gefordert und klingt auch in dessen Beschlüssen an. Dabei wird u.a. dem Gesetzgeber empfohlen, konzentriert und umfassend den Datenumgang und -zugang auch formal in einem einzigen Informationsgesetzbuch zusammenzufassen. Dies ermöglicht sicher eine übersichtlichere und widerspruchsfreiere Regelung informationsbezogener Inhalte. Ob es für den Bürger allerdings transparenter ist, die notwendigermaßen differenzierenden Vorschriften außerhalb der Fachgesetze suchen zu müssen, ist fraglich. Die von vielen beklagte Unübersichtlichkeit würde möglicherweise nur verlagert.

In einer Entschließung vom 5./6. Oktober 1998 (Anlage 19.14) haben die Datenschutzbeauftragten von Bund und Ländern die Überlegungen dieses Gremiums grundsätzlich begrüßt.

2.4 Allgemeines Informationszugangsrecht

Ein spezieller Gesichtspunkt hierbei ist, dem eher als abwehrrechtlich und persönlichkeitsbezogen entwickelten Datenschutzrecht (jedenfalls gleichberechtigt) die Möglichkeit zur Seite zu stellen, Bürgern auch ohne persönliche Betroffenheit Zugang zu Informationen zu eröffnen, die bei öffentlichen Stellen in Akten und anderen Unterlagen vorhanden sind. Dies dient dem Ziel, den bestehenden Informationsvorsprung des Staates zugunsten eines Informationsgleichgewichts abzubauen. Hierfür gibt es vor allem unter dem allgemeinpolitischen Aspekt, in einer demokratisch verfaßten Informationsgesellschaft kommunikative Freiheit und Mitwirkung der Bürgerinnen und Bürger zu erweitern, gute Gründe. Eine derartige Ergänzung hat Beispiele in verschiedenen europäischen und außereuropäischen Rechtsordnungen, zum Teil auch im Aufgabenspektrum der jeweiligen Datenschutzkontrollinstanz. Forderungen zu entsprechender Normierung gibt es auch bei uns seit langem.

Unter anderem geprägt durch Erfahrungen der jüngeren Vergangenheit, verbürgt die Verfassung des Landes Brandenburg ebenfalls den Anspruch auf Einsicht in amtliche Unterlagen; im Vorfeld der gesetzlichen Umsetzung dieses Rechts wurde das Thema in der Konferenz der Datenschutzbeauftragten angesprochen. Eine Arbeitsgruppe, an der sich mehrere Kollegen beteiligt haben, hat hierzu ein eingehendes Papier erarbeitetet, das mit Vorstellungen zur Ausgestaltung u. a. auf die ausdrückliche Forderung der Datenschutzbeauftragten nach einem solchen Zugangsrecht zielte. Diesem Anliegen habe ich allerdings in amtlicher Tätigkeit nicht zustimmen können, und zwar im wesentlichen deswegen, weil es nach meinem Verständnis außerhalb des mir derzeit im SDSG gesetzlich übertragenen (begrenzten) Auftrags liegt; diesem entspricht vielmehr, einen Ausgleich mit der teilweise gegenläufigen Zielrichtung zu suchen.

Eine förmliche Entschließung wurde hierzu nicht gefaßt. In Brandenburg ist zwischenzeitlich das Datenschutzgesetz um die Regelung über ein Recht auf Akteneinsicht ergänzt und meinem Kollegen die Aufgabe zugewiesen worden, auch hierüber zu wachen. Außerhalb dieses Bundeslandes ist die Angelegenheit gleichwohl nicht abschließend erledigt, weil ja eine Abwägung zwischen dem Persönlichkeitsschutz Betroffener und dem demokratisch zu begründenden Teilhaberecht aller Bürger auf informationelle Grundversorgung stattfinden muß, soweit sich entsprechende gesetzgeberische Initiativen hierauf richten; damit ist zu rechnen.

3 Technisch-organisatorischer Datenschutz

3.1 Teilverlagerung von Aufgaben der ZDV-Saar zur debis-Systemhaus-Saar GmbH

Einen erheblichen Anteil unserer Arbeitskapazität hat die Mitwirkung an einem Privatisierungsprojektin Anspruch genommen, das für die Datenverarbeitung im Bereich der Landesverwaltung von beträchtlicher Bedeutung hätte werden können, letztlich jedoch nicht verwirklicht wurde. Auch über die Grenzen des Landes hinaus entfällt damit vorerst die Möglichkeit, mit einem größeren Vorhaben zum "Outsourcing" von Leistungen öffentlicher Verwaltung in der Praxis Erfahrungen zu sammeln, das nicht nur für den beteiligten privaten Partner modellhaften Charakter für Projekte mit weiteren öffentlichen Stellen gewonnen hätte. Die in der privaten Wirtschaft vielfach geübte Praxis kann nämlich nicht unbesehen auf den öffentlichen Sektor übertragen werden, weil hier teilweise abweichende Vorschriften beachtet werden müssen.

Dies rührt nicht etwa daher, daß der Schutzstandard in privaten Datenverarbeitungseinrichtungen generell als geringer einzuschätzen wäre. Vielmehr obliegt den öffentlichen Stellen aufgrund ihrer gesetzlich bestimmten Aufgaben eine besondere und auch besonders geregelte Verantwortung im Um-

gang mit Daten, die Bürgerinnen und Bürger ihnen ja großenteils nicht aus eigener Entscheidung und mit der Möglichkeit anvertrauen, Leistungen eines Wettbewerbers zu nutzen. Daß teilweise unterschiedliche Vorschriften anwendbar sind, erklärt sich - jedenfalls überwiegend - nicht aus der unterschiedlichen Entwicklung der Rechtsgebiete; der Gesetzgeber hat mit gutem Grund den öffentlichen Stellen oftmals zusätzliche Bindungen auferlegt. Ein Teil hiervon dient zugleich auch dem Schutz von Persönlichkeitsrechten, deren Beachtung ich zu kontrollieren habe.

Im Juli 1996 erhielt ich im interministeriellen Ausschuß für Informationstechnologie Kenntnis davon, daß im Saarland die Gründung eines Gemeinschaftsunternehmens von Land und der debis-Systemhaus GmbH geplant sei, das die Datenverarbeitungsaufgaben der bisherigen ZDV-Saar übernehmen sollte. Vom federführenden Ministerium für Wirtschaft und Finanzen (MWF) erbat ich nähere Informationen, aus denen die Modalitäten dieser Auftragsdatenverarbeitung und insbesondere eine datenschutzrechtliche Bewertung hervorgehen sollten. Nachdem das MWF im Oktober 1996 eine Betriebsaufnahme schon zum 1.1.97 angekündigt hatte, mußte ich auf noch ungeklärte Fragen verweisen, die sich bei der Verarbeitung von Steuer- und Sozialdaten aus den spezialgesetzlichen Anforderungen ergeben. In einem Rundschreiben an alle Ressorts wies ich diese auf ihre datenschutzrechtliche Verantwortung hin und bat um Prüfung der Anforderungen bei einer Auftragsdatenverarbeitung, insbesondere unter Berücksichtigung des § 5 SDSG bzw. spezialgesetzlicher Regelungen.

- Auch nachdem das MWF die Absicht aufgegeben hatte, die Steuerdatenverarbeitung als Auftragsdatenverarbeitung durchzuführen (unter den Finanzministerien von Bund und Ländern war zwischenzeitlich geklärt worden, daß bei Verlagerung der steuerlichen Datenverarbeitung aus finanzverfassungsrechtlichen Gründen in jedem Fall die volle Sachherrschaft der Steuerverwaltung fortbestehen müsse), verblieben nach Durchsicht der Vertragsentwürfe und einer juristischen Bewertung des MWF noch Unklarheiten und grundsätzliche Zweifel an Zulässigkeit und Modalitäten einer Übertragung.

  Ich habe deshalb noch vor Unterzeichnung der Gründungsverträge gefordert, diese Fragen zu klären sowie eine Risikoanalyse und ein Sicherheitskonzept zu erstellen, die durch einen neutralen Gutachter bewertet werden sollten. Bei Vertragsschluß zur Gründung von "debis Systemhaus Saar GmbH" (dSS) im September 1997 lag - auch mir - zwar ein Sicherheitskonzept des privaten Mehrheitsgesellschafters debis vor, das vom TÜV Süddeutschland geprüft und aus technischer Sicht als ausreichend sicher angesehen wurde; jedoch waren noch nicht alle datenschutzrechtlichen Fragen abgeklärt. Nicht geklärt war auch die Forderung nach einer Verschlüsselung im Landesdatennetz, wenn dessen Betrieb durch das private Gemeinschaftsunternehmen betrieben wird.

Eine sichere Basis bestand auch noch nicht, als im Januar 1998 mit Original-Steuerdaten Integrationstests durchgeführt wurden, für die diese Echtdaten in die neue Umgebung verlagert worden waren. Weil dabei auch festgestellt werden mußte, daß die im Sicherheitskonzept vorgesehenen Maßnahmen noch nicht vollständig umgesetzt waren, wurden auf meine Intervention hin die Integrationstests gestoppt und alle Daten gelöscht. Im Ergebnis erwiesen sich so Sorgen, die in großer Zahl auch öffentlich geäußert worden waren, als unbegründet.

In der Folgezeit wurde dann die Problematik auch seitens der verantwortlichen Ressorts mit angemessener Intensität behandelt; es gelang, die rechtlichen Grundsatzfragen befriedigend zu lösen. Aus diesen Erkenntnissen heraus mußten das Sicherheitskonzept fortgeschrieben und weitere technische und organisatorische Maßnahmen, insbesondere auch systemtechnischer und baulicher Art getroffen werden. Dies erforderte sowohl bei ZDV und übriger Landesverwaltung als auch bei dem privaten Unternehmen erhebliche Anstrengungen; die sehr konstruktive Mitwirkung vor allem meines Technik-Referatsleiters möchte ich ebenfalls hervorheben. Bis Ende des Jahres 1998 wurden mit großem Personaleinsatz und Engagement und in enger Abstimmung mit meiner Dienststelle allgemeine und verfahrensspezifische Konzepte erstellt und die Möglichkeit ihrer Umsetzung unter Beteiligung einzelner Ressorts überprüft.

Ergebnis war letztendlich, daß bei allen kritischen Datenverarbeitungsverfahren (Steuer, Soziales, Statistik, Bezüge, Beihilfe, Kataster) das private Gemeinschaftsunternehmen keines dieser Daten hätte zur Kenntnis nehmen können. Generell wurde festgelegt, daß kritische Aktivitäten wie z. B. die Systemverwaltung nur im Vier-Augen-Prinzip zwischen dSS und Land hätten wahrgenommen werden können, während die Programmierung, das Operating, die Druckausgabe, die Nachbereitung und die Netzadministration weiter in Landeszuständigkeit verblieben wäre. Es war vorgesehen, vor Aufnahme des - solchen Einschränkungen unterworfenen - Produktionsbetriebs die Maßnahmen, die in den Sicherheitskonzepten vorgesehen waren, mit Hilfe einer IT-Checkliste im Rahmen eines IT-Controlling unter Beteiligung von Landesstellen und von dSS abzunehmen und ihre Wirksamkeit mit Hilfe von Integrationstests zu überprüfen.

Ende 1998 - nach Feststellung einer langwierig und kostenträchtig zu beseitigenden Asbestverseuchung im geplanten Rechenzentrum - sind die Partner des Joint Venture übereingekommen, das Projekt nicht mehr weiterzuführen, weil ein weiteres Verschieben des Produktionsbeginns nicht zu vertreten sei. Zudem, so die Ministerin für Wirtschaft und Finanzen, müsse die Steuerverwaltung zur Vorbereitung einer bundesweit einheitlichen Steuerfestsetzung alle Kräfte auf die parallel dazu laufende Umstellung auf das bayerische Verfahren und damit auch zur Lösung der Jahr-2000-Problematik sowie zur Einführung des Euro einsetzen; danach allerdings stelle sich das Thema Privatisierung erneut.

Ich kann davon ausgehen, daß die bisherige intensive Begleitung des Projekts "Verlagerung von Teilaufgaben der bisherigen ZDV-Saar zur debis-Systemhaus-Saar GmbH" durch meine Dienststelle zu einer aus datenschutzrechtlicher Sicht befriedigenden Absicherung des Einsatzes personenbezogener Daten geführt hätte. Deshalb halte ich die von allen Seiten hierin investierte umfangreiche Arbeit auch nicht für verloren. Vielmehr hoffe ich, daß die erstellten Konzepte und die mit diesem Projekt erreichten Erkenntnisse wieder herangezogen werden können, wenn im Jahre 2000 erneut eine Privatisierung - dann der sechste Versuch einer Verlagerung von Datenverarbeitungsaktivitäten der ZDV-Saar - in Angriff genommen werden sollte.

Nicht nur unsere eigene Beschäftigung mit diesem Vorhaben hat indes den Arbeitsaufwand erkennen lassen, der bei der "präventiven" Datenschutzkontrolle für den knappen Personalbestand der einzelnen Datenschutzbeauftragten im jeweiligen Land anfällt, wenn Verwaltungs- bzw. Datenverarbeitungsaufgaben ausgegliedert oder ganz aus dem öffentlichen Bereich herausgelöst werden sollen. Um Kenntnisse und Erfahrungen in derartigen Fällen auszutauschen und Lösungsansätze - auch für ein notwendig erscheinendes Fortentwickeln von Rechtsvorschriften - zu suchen, wurden innerhalb der Konferenz der Datenschutzbeauftragten gemeinsame Erörterungen zum "Outsourcing" aufgenommen, die noch nicht abgeschlossen sind.

3.2 Prüfung der Sparkasseninformations- und Kommunikationsservice GmbH (SIK)

In verschiedenen Bereichen nutzen auch derzeit öffentliche Stellen die fachliche und technische Kapazität privater Stellen für Datenverarbeitungsaufgaben.

So stieß ich im Rahmen der datenschutzrechtlichen Prüfung bei einer Gemeinde darauf, daß diese die Verarbeitung der Bezügedaten ihrer Bediensteten einem privatrechtlich organisierten Betrieb übertragen hatte. Dabei handelt es sich um ein Tochterunternehmen der Sparkassen, das Datenverarbeitungsaufgaben nicht nur für diese, sondern auch für andere Stellen zentral wahrnimmt.

Nach Klärung meiner Prüfkompetenz (vgl. TZ 9.1) habe ich zunächst kontrolliert, ob die datenschutzrechtlichen Anforderungen gem. § 5 SDSG eingehalten sind. Bemängeln mußte ich, daß das Unternehmen sich das Recht einer beliebigen Unterauftragsvergabe vorbehalten hatte, die sogar so weit gehen konnte, daß an Dritte die komplette Berechnung und Zahlbarmachung von Vergütung, Löhnen und Besoldung ohne Zustimmung des Auftraggebers hätte vergeben werden können. Nach einigen Diskussionen, in denen auch die Anwendbarkeit des SDSG gänzlich in Frage gestellt worden war, konnte

ich Auftraggeber und Unternehmen von der bestehenden Rechtslage überzeugen, die derart unbegrenzte Unterauftragsverhältnisse ausschließt.

Meine Prüfung, ob für den Auftrag im Unternehmen ausreichende technische und organisatorische Maßnahmen gem. § 11 SDSG getroffen wurden, ergab nur geringfügige Beanstandungen und im wesentlichen nur Verbesserungsvorschläge für einen datenschutzgerechten Ablauf. Insbesondere habe ich darum gebeten, eine Risikoanalyse und ein darauf aufbauendes Sicherheitskonzept zu erstellen und die getroffenen Maßnahmen damit abzugleichen. Bei der innerbetrieblichen Organisation habe ich vorgeschlagen, den internen Datenschutzbeauftragten stärker, auch formal, in die Abläufe einzubinden. Bei der Freigabe von Verfahren sollten die Auftraggeber direkter in die Verantwortung einbezogen werden, da sie letztlich für den Datenschutz verantwortlich bleiben; dies gilt auch für etwaige Unterauftragsverhältnisse. In ihrer Stellungnahme hat das Unternehmen die Umsetzung meiner Vorschläge zugesagt.

3.3 Modellhafte Beteiligung an Verfahren der Landkreise am Beispiel des Kfz-Zulassungsverfahrens ZW2000

Im Zuge der Kommunalisierung zur Jahreswende 1996/97 wurde den Landkreisen und dem Stadtverband die Zuständigkeit für die Kfz-Zulassung übertragen. Damit ging die Verantwortlichkeit zur Einführung eines EDV- Verfahrens, das landesweit eingesetzt werden sollte, an sie über. Zur Abwicklung der Freigabe des Verfahrens schaltete sich koordinierend der Landkreistag ein; der Landkreis Saarlouis erklärte sich bereit, die dazu notwendigen Arbeiten modellhaft zu übernehmen und sie den anderen Landkreisen zur Verfügung zu stellen. Dazu erstellte der Landkreis eine vorbildliche Risikoanalyse und ein Sicherheitskonzept, eine Muster-IT-Dienstanweisung für den Einsatz vor Ort und eine Muster-Meldung zum Dateienregister. Die technischen und organisatorischen Maßnahmen wurden in enger Abstimmung mit meiner Dienststelle konzipiert und umgesetzt, so daß die anderen Kreise diese Vorgehensweise nur analog nachzuvollziehen brauchten. Leider ist die Umsetzung bisher noch nicht von allen Landkreisen abgeschlossen worden.

Aufgrund der positiven Erfahrungen aus diesem Projekt besteht bei den Verantwortlichen der Landkreise und des Stadtverbandes großes Interesse, in gleicher Weise anstehende Probleme auch weiterhin gemeinsam zu lösen und die erforderliche Abstimmung mit dem LfD in datenschutzrechtliche Fragen ebenfalls gebündelt vorzunehmen. So ist beabsichtigt, zukünftige Verfahrenseinführungen nach dem gleichen Schema mit Hilfe einer Modellösung zu vereinfachen und damit eine inhaltlich aufwendige Mehrfachbeteiligung zu vermeiden. Der Geschäftsführer des Landkreistages hat eine entsprechende Unterstützung zugesagt. Derzeit ist ein neues Projekt zur Vereinfachung der Kfz-Zulassung über das Internet in der Abstimmung.

Ich halte dieses Vorgehen für sinnvoll und ökonomisch. Zu betonen ist aber, daß die modellhafte Entwicklung und Bündelung in der Abstimmung die datenschutzrechtliche Verantwortlichkeit des einzelnen Kommunalverbandes unberührt läßt, der deshalb auch für sich die Anwendung freigeben muß; auch die nach dem SDSG bestimmten Pflichten zur Beteiligung und Registermeldung bleiben als solche bestehen, können indes faktisch einfacher wahrgenommen werden.

3.4 Internet-Angebote der Kommunen und öffentlichen Stellen

Bei Kommunen, aber auch bei anderen öffentlichen Stellen wächst das Interesse, das Internet für die Selbstdarstellung und das Angebot von Leistungen zu nutzen. Mit zunehmender - auch privater - Verbreitung dieser Zugriffsmöglichkeiten wird dies manchmal auch erwartet, oder es werden gar entsprechende Forderungen gestellt. Großenteils enthalten die bisher vorliegenden Angebote Informationen ohne jeden Personenbezug und sind deswegen - was den Inhalt, nicht den Kommunikationsvorgang als solchen betrifft - datenschutzrechtlich nicht problematisch.

In Angeboten wie der Selbstdarstellung der Behörde, Verzeichnissen von Dienststellen mit jeweiligen Ansprechpartnern, Verweisen auf öffentliche Einrichtungen, Vereine und Verbände sind jedoch teilweise auch Daten enthalten, die sich auf individuelle Personen beziehen lassen, diese mitunter auch herausstellen. Es finden sich sogar Links zu privaten Homepages einzelner Bediensteter. Ferner eröffnen viele Stellen die Möglichkeit einer direkten elektronischen Kontaktaufnahme.

Bei allen faszinierenden Chancen der neuen Technologie dürfen doch die Gefahren nicht vergessen werden, die nicht geschützte Kommunikation im Internet für Persönlichkeitsrechte birgt. Persönliche Daten können kaum kontrollierbar kopiert und verfälscht oder unproblematisch mit anderen Zusammenhängen verknüpft werden, und dies weltweit und ohne jede verläßliche Möglichkeit einer Korrektur; gerichtlich durchsetzbare Ansprüche gegen die oft ausländischen Betreiber gibt es meist nicht. Einmal herausgegebene Daten sind - über die faktische Beschränkung einer beispielsweise regionalen oder fachinternen Mitteilung hinaus - "allgemein zugängliche Quellen". Deswegen muß man sorgfältig prüfen und bewerten, wo und mit welchem Inhalt dieses Medium genutzt werden soll. Dabei sind natürlich die Sonderheiten der jeweiligen Verwaltungssparte zu beachten; in der wissenschaftlichen Forschung besteht anderer Kommunikationsbedarf als beim Verkehr mit einer Kommunalverwaltung.

Generell habe ich, soweit ich bei Prüfungen oder aus sonstigem Anlaß darauf gestoßen bin, empfohlen, Personenbezüge möglichst ganz zu vermeiden. Soweit Mitarbeiterdaten betroffen sind, verweise ich auf TZ 14.5.

Der Umfang personenbezogener Informationen sollte nach kritischer Prüfung auf das Notwendigste, d. h. solche Daten beschränkt werden, die in Beziehung zur - i.d.R. - beruflichen Tätigkeit des Betroffenen stehen (Prinzip der Datensparsamkeit). Sind Betroffene mit Speicherung und Übermittlung im Internet einverstanden, so muß die - vorherige - Einwilligung im echten Sinn freiwillig sein; eine Verweigerung muß das Löschen der Daten zur Folge haben und darf nicht zu nachteiligen Folgen führen. Selbstverständlich bestehen weiter die üblichen datenschutzrechtlichen Auskunfts-, Berichtigungs- und Löschungsrechte.

Darüber hinaus müssen, weil solche Angebote an die Öffentlichkeit sich kommunikationsrechtlich je nach Inhalt als Medien- oder Teledienste oder auch als Telekommunikationsleistung darstellen, die entsprechenden Schutzbestimmungen eingehalten werden.

Auf allgemeine Risiken bei der Internet-Nutzung und entsprechende datenschutzrechtliche Empfehlungen (z. B. Abschottung, Firewall, Verschlüsselung) habe ich schon in meinem letzten Tätigkeitsbericht (TZ 4.7) aufmerksam gemacht; auf diese Darstellung der Problematik sei verwiesen. Eine aktualisierte Orientierungshilfe "Internet" ist in meinem Internet-Angebot unter www.lfd.saarland.de enthalten. Ein Muster für eine "Betriebsvereinbarung e-Mail und Internet" findet sich in der Zeitschrift Datenschutz und Datensicherheit Nr. 12/1997, Seite 703.

3.5 Modernisierung der Verfahren in den Kommunen

Bereits im letzten Bericht (TZ 4.14) habe ich darauf hingewiesen, daß mich die 1996 in größerem Umfang erkennbaren Pläne und Maßnahmen von Kommunen, Ersatz für die bisher betriebene Hard- und Software zu beschaffen, zu "präventivem" Handeln veranlaßt haben. Um bei dieser Ablösung auch rechtzeitig auf die datenschutzrechtlichen Anforderungen aufmerksam zu machen, hatte ich allen Kreisen, Städten und Gemeinden eine Übersicht über die geltenden datenschutzrechtlichen Bestimmungen zugesandt und um Berücksichtigung gebeten. Auch wenn ich damals gefordert hatte, die nach § 8 SDSG notwendige Freigabe der Verfahren ordnungsgemäß abzuwickeln und den LfD vorher zu beteiligen, ließ die Resonanz zu wünschen übrig. Erst im Zusammenhang mit konkreten Prüfungen vor Ort konnte die Bedeutung der datenschutzrechtlichen Bestimmungen vermittelt und eine korrekte Bearbeitung erreicht werden. Diese Prüfungen werde ich kontinuierlich fortsetzen.

Durch Rückfragen zu einzelnen Verfahren ergab sich, daß nur die wenigsten Kommunen erkannt hatten, daß die Freigabe eines Verfahrens durch jede Kommune selbst erfolgen mußte; einige glaubten, die erstmalige Freigabe durch eine andere Gemeinde oder die modellhafte Freigabe z.B. durch die beschaffende Kreisverwaltung reiche dazu völlig aus. Daß dies sich auch bei

einer "gebündelten" Beteiligung des LfD nicht erübrigt, hatte ich im Zusammenhang mit der KfZ-Zulassung in den Kreisen bereits betont (TZ 3.3)

Zusätzlich habe ich versucht, mit Anbietern der neuen Softwaresysteme Muster-Prüfungen vorzunehmen und Muster-Meldungen zum Dateienregister zu erarbeiten, um zu helfen, den Aufwand beim späteren Einsatz in einer Kommune für die damit verbundene Freigabe und Meldung im Einzelfalle zu verringern. Dies ist nur mit einem Teil der Anbieter gelungen, die ja zu einem Kontakt mit mir auch nicht verpflichtet sind. Teilweise war kein Ergebnis zu erzielen, weil die Mehrheitsverhältnisse sich laufend änderten oder die Organisation des Anbieters gerade im Umbau war. Teilweise war auch keine Reaktion zu verzeichnen, weil die Anbieter den Aufwand dazu scheuten und hofften, die Anwender würden sich über die gesetzlichen Anforderungen hinwegsetzen. Teilweise haben die Anbieter auf diesbezügliche Forderungen von Kommunen wohl auch deswegen nicht reagiert, weil die geringe Zahl betroffener Anwender im Saarland keine ausreichende Marktmacht darstellt. In allen diesen Fällen, in denen von unserem Service kein Gebrauch gemacht wird, bleibt den Kommunen nichts anderes übrig, als den Aufwand im Einzelfall jedesmal für sich zu betreiben oder eventuell mit anderen Anwendern zu kooperieren und deren Lösungen mit Anpassungen zu übernehmen.

3.6 Datenschutz im kommunalen Bereich - Ergebnisse stichprobenartiger Kontrollen

Im Jahre 1998 habe ich (kleinere) Gemeinden aus jedem Landkreis und dem Stadtverband aus datenschutzrechtlicher Sicht überprüft, ohne mich dabei von vornherein auf einen eng spezifizierten Bereich zu konzentrieren. Hierdurch rückten natürlich die technisch-organisatorischen Aspekte stärker in den Vordergrund.

Das Ergebnis der Prüfungen hat in allen Gemeinden im wesentlichen das gleiche Bild ergeben, daß nämlich in der Umsetzung der datenschutzrechtlichen Verpflichtungen erheblicher Nachholbedarf vorhanden ist. Manchmal fehlte es sogar an elementarsten Vorkehrungen zum Schutz des Informationellen Selbstbestimmungsrechts, aber auch an hinreichenden Sicherungen für die Anwendungen selbst.

Dies ist um so unverständlicher, als ich die Kreise und Gemeinden in mehreren Rundschreiben auf die gesetzlichen Anforderungen aufmerksam gemacht und ihnen in Form von Beratung bzw. Muster-Texten Hilfestellung angeboten habe. Eine Diskette mit Materialien und eine CD mit dem IT-Grundschutzhandbuch des BSI wurde den Kommunen kostenlos zur Verfügung gestellt.

Bei den Prüfungen mußten folgende grundsätzliche Mängel festgestellt werden
(davon bei manchen Gemeinden eine Vielzahl gleichzeitig):

- Ein Sicherheitskonzept mit vorgeschalteter Risikoanalyse war nicht vorhanden. Die technischen und organisatorischen Maßnahmen wurden eher intuitiv festgelegt und waren in der Regel unzureichend.
- Die informationstechnischen Verfahren wurden nicht gemäß § 8 Abs. 2 SDSG freigegeben. Die vorgeschriebene Beteiligung des LfD vor der Freigabe war ignoriert worden. Es war übersehen worden, daß auch am Arbeitsplatz entwickelte Verfahren (z. B. Excel- oder Access-Anwendungen) nur nach Beauftragung entwickelt werden durften und auch diese Verfahren der Freigabe bedürfen und dem LfD zu melden sind.
- In der Regel fehlten die nach § 23 SDSG vorzulegenden Meldungen zum Dateienregister, waren nicht vollständig oder nicht aktuell.
- Das nach § 9 SDSG erforderliche Geräteverzeichnis war nicht vorhanden.
- Die nach § 11 Abs. 2 SDSG zu treffenden technischen und organisatorischen Maßnahmen waren nicht ausreichend. Insbesondere fehlte eine nach Ziffer 10 notwendige IT-Dienstanweisung als wichtigstes Element der Organisationskontrolle.
- Die Funktionstrennung bei der Wahrnehmung kritischer Aufgaben wie Systemverwaltung, Programmierung, Verfahrensanwendung und Kontrolle war nicht gewährleistet. So lagen diese Aufgaben oft alleine in der Hand des Systemverwalters. Dieser war damit zwangsläufig auch dem Risiko ausgesetzt, für unzulässige Datenmanipulationen verantwortlich gemacht zu werden, ohne sich gegen einen solchen Vorwurf wehren zu können.
- Die nach § 7 SDSG erforderliche Unterrichtung zum Datenschutz wurde noch immer in Form einer nach dem alten SDSG (bis 1993) vorgeschriebenen Verpflichtung gehandhabt.
- Die Absicherung einzelstehender PC war oft unzureichend. So war die Boot-Reihenfolge noch so eingestellt, daß zuerst die Diskette nach einem Betriebssystem abgesucht wurde, die Virenkontrolle des BIOS war nicht aktiviert und oft lediglich das BIOS-Paßwort als Zugriffsschutz genutzt, obwohl inzwischen bekannt ist, wie dieser Schutz relativ einfach zu umgehen ist.
- Auch der Zugriffsschutz auf Netzwerke und Menüsysteme war verbesserungsbedürftig. Paßworte waren nach der erstmaligen Vergabe noch nicht geändert worden. Die Paßwortlänge war zu kurz oder es wurden Gruppenpaßwörter benutzt, die amts- oder gar gemeindeweit bekannt waren. Auch die Nutzung von leicht zu erratenden Trivialpaßworten war festzu-

stellen. Zugriffe auf Datenbestände waren z. T. über das zulässige und erforderliche Maß hinaus freigegeben. Ein paßwortgesicherter Bildschirmschoner wurde nicht genutzt, obwohl die Software vorhanden war.

- Der Netzwerkserver stand teilweise im Büro unter dem Schreibtisch oder war gemeinsam mit anderen Einrichtungen oder Arbeitsplätzen in ungesicherten Räumen untergebracht.
- Die Daten- und Systemsicherung war direkt beim Server in einer offenen Box gelagert oder wurde gar vom Systemverwalter - gut gemeint, aber unzulässigerweise - zu Hause aufbewahrt.
- Eine Kontrolle der getroffenen Maßnahmen und eine Überprüfung der datenschutzrechtlichen Zulässigkeit der Verarbeitung wurde nicht vorgenommen.
- Die Vernichtung von Datenträgern wurde nicht im Sinne der Richtlinie des MdI zur Vernichtung von Schriftgut und sonstigen Datenträgern (GMBl 1989 S. 2) gehandhabt. Insbesondere entsprachen die Aktenvernichter nicht der vorgeschriebenen Sicherheitsstufe S4 der DIN 32757. Die Löschungsfristen von Daten waren nicht genau bekannt oder waren - teilweise auch mit Verweis auf fehlende personelle Kapazitäten zur Vernichtung - weit überschritten.
- Der Datenträgeraustausch erfolgte ohne Begleitscheine; eine Verschlüsselung der Daten wurde nicht genutzt. Eine Virenkontrolle der eingehenden Datenträger war nicht selbstverständlich.
- Das Risiko von Zugängen zu Online-Diensten und zum Internet, insbesondere über PC mit Netzwerkanschluß, war nicht erkannt worden. Firewalls als Absicherung waren nicht vorhanden.
- Für die Dienstleistung von Firmen im Rahmen von Installation, Wartung und Reparatur fehlte es an Vorkehrungen, wie sie für die Auftragsdatenverarbeitung nach § 5 SDSG geregelt sind. Wenn die Dienstleistung vertraglich geregelt war, wurden in der Regel firmenspezifische Verträge unterzeichnet, die vorrangig nach den Interessen der Firmen gestaltet waren und den datenschutzrechtlichen Anforderungen nicht genügten. Der Regelungsumfang der sogenannten besonderen Vertragsbedingungen (BVB) die im GMBl des Saarlandes veröffentlicht sind, war nicht bekannt. Zielsetzung dieser BVB ist es, die Interessen von öffentlichem Auftraggeber und privatem Auftragnehmer ausgewogen zur berücksichtigen.

Die betroffenen Gemeinden haben eine Beseitigung der festgestellten Mängel, soweit sie nicht gleich behoben werden konnten, zugesagt. Mit den zuständigen Bearbeitern wurde in vielen Fällen ein fruchtbarer Dialog begon-

nen, bei dem Unklarheiten beseitigt und das datenschutzgerechte Vorgehen abgestimmt werden konnten.

Die Berichte über diese Prüfungen habe ich auch den Landkreisen und dem Stadtverband zugesandt. Ich erwarte, daß auch sie im Rahmen der Kommunalaufsicht die Gemeinden anhalten werden, den gesetzlichen Anforderungen Rechnung zu tragen und den Datenschutz im kommunalen Bereich zu verbessern. Bisher konnte ich von dort noch keine Reaktion verzeichnen.

3.7 IT-Dienstanweisungen im öffentlichen Bereich

Aufgrund ihres umfassenden Regelungsinhalts ist eine Dienstanweisung für den Einsatz der Informationstechnik die wichtigste nach § 11 SDSG geforderte Maßnahme zur Organisationskontrolle, bei der auch weitgehend die anderen geforderten technischen und organisatorischen Maßnahmen geregelt werden. Zusätzlich ist die Dienstanweisung für die betroffenen Mitarbeiter eine Informationsquelle und gibt Hilfe bei auftretenden Fragen. Selbstverständlich reicht der Erlaß einer Dienstanweisung allein nicht aus, sondern er muß durch eingehende Unterrichtung begleitet und ergänzt werden. Die Dienstanweisung dient auch keinesfalls, wie fälschlich manchmal behauptet wird, dem Abwälzen von Verantwortlichkeiten, sondern stellt diese, auch mit Blick auf die besondere Verantwortung der Behördenleitung, klar heraus.

Im Berichtszeitraum habe ich versucht, die in meinem letzten Bericht (TZ 4.11) erwähnten Muster-Dienstanweisungen im öffentlichen Bereich des Saarlandes zur Umsetzung zu bringen. Leider ist dies nur teilweise gelungen. Soweit die fehlende Umsetzung mit der laufenden Ablösung der veralteten Informationstechnik begründet wurde, da dann die neue Technik gleich richtig integriert werden könne, habe ich mich dieser Argumentation angeschlossen. Teilweise wurde aber auch eine Umsetzung mit Verweis auf personelle Engpässe zurückgestellt (z. B. Unikliniken, bei denen ein fertiger Entwurf seit längerem vorliegt). In Einzelfällen wurden ohne meine Beteiligung und ohne Berücksichtigung der übergebenen ausführlichen Muster unzulängliche Dienstanweisungen in Kraft gesetzt (z. B. Ministerium für Bildung, Kultur und Wissenschaft).

Daß die Umsetzung der Anforderungen aus einer IT-Dienstanweisung gerade auch in kleinen Dienststellen, insbesondere kleineren Kommunalverwaltungen, nicht stets ohne Schwierigkeiten gelingt, war abzusehen. Insbesondere ist die Forderung nach Funktionstrennung zwischen Systembetreuung und Verfahrensanwendung sowie nach Einrichtung einer internen Revision und Datenschutzkontrolle mit personellen Konsequenzen verbunden, deren Notwendigkeit nicht sofort eingesehen wurde.

Der Städte- und Gemeindetag hat aufgrund der Anfragen verschiedener Gemeinden in einer Stellungnahme auf diese Probleme verwiesen und dabei

dankenswerterweise den hohen Stellenwert des Datenschutzes im kommunalen Bereich herausgestellt; eine Dienstanweisung wird für grundsätzlich erforderlich gehalten. Um den Anforderungen unter Berücksichtigung der personellen und finanziellen Engpässe bei den Kommunen gleichwohl zu entsprechen, käme nach meiner Auffassung als Lösungsmöglichkeit in Betracht, ähnlich wie beim Gemeindeprüfungsamt, die genannten Funktionen gemeindeübergreifend und gegebenenfalls auch vom zuständigen Landkreis oder Stadtverband koordinierend wahrzunehmen.

Da mit dem Erlaß von Dienstanweisungen auch die datenschutzrechtlichen Verantwortlichkeiten und insbesondere die Anforderungen für die Behördenleitungen geklärt werden, werde ich meine Anstrengungen weiter fortsetzen, auf den Erlaß einer solchen Dienstvorschrift hinzuwirken, und bei Kontrollen auf ausreichende organisatorische Maßnahmen dringen. Dauerhaft unzureichende Vorkehrungen bei entsprechendem Schutzbedarf der Anwendungen werde ich künftig auch bei kleineren Dienststellen bzw. Gemeinden nicht unbeanstandet hinnehmen können.

3.8 Datenübertragung (eMail/X400) und Verschlüsselung

Die Landesverwaltung hat verstärkte Anstrengungen unternommen, den Informationsaustausch untereinander auf elektronische Vorgangsbearbeitung über den Mail-Dienst X400 umzustellen. In Abstimmung mit mir wurden die Anforderungen für elektronische Verzeichnisse festgelegt, Empfehlungen zur Regelung des Einsatzes erarbeitet und Muster-Layouts für Briefbogen und Vermerke entworfen.

In einer Testphase soll der Einsatz dieser Technik erprobt werden. Dabei sollen Dokumente ausgetauscht werden, deren Schutzbedarf nicht höher als der eines erlaubten Fax-Versandes sein darf.

Für höheren Schutzbedarf habe ich die Forderung nach einer Verschlüsselung der Dokumente bzw. ihrer Anlagen erhoben. Um dieser Forderung entsprechen zu können, hat die Landesverwaltung eine eigene Arbeitsgruppe eingerichtet, die entsprechende Produkte prüfen und Einsatzvorschläge erarbeiten soll. Als Übergangslösung habe ich einfache Verschlüsselungsprodukte und alternativ das leistungsfähige und im Internet-Verkehr übliche Verschlüsselungsprogramm PGP zur Anwendung empfohlen und in meinem Internet-Angebot meinen öffentlichen PGP-Schlüssel integriert.

Meinen Vorschlag zur Verschlüsselung hat jetzt schon das Ministerium der Justiz aufgegriffen, das den Austausch der Schuldnerverzeichnisse mit Hilfe einer Verschlüsselung der Daten sicher gestalten will. Im Projekt "Teilverlagerung von Aufgaben der ZDV-Saar zur debis-Systemhaus-Saar GmbH", bei dem auch mit meiner Dienststelle umfangreiche Abstimmungen stattfanden, wurde der Austausch von Dokumenten, auch unter Nutzung von

Verschlüsselungsverfahren, intensiv genutzt und damit die Projektarbeit beschleunigt.

3.9 Übernahme der bayerischen Steuer-Verfahren und Beteiligung des LfD

Das Ministerium für Wirtschaft und Finanzen hat sich entschlossen, durch Einführung der bayerischen Steuer-Verfahren die Umstellung auf das Jahr 2000-Problem und die spätere Umstellung auf das geplante bundeseinheitliche Verfahren FISCUS zu erleichtern.

Trotz mehrfacher Nachfragen wurde ich bei den Vorbereitungsarbeiten nicht ausreichend beteiligt; erste Unterlagen erhielt ich erst Anfang 1999. Auch habe ich von der geplanten Realisierung der elektronischen Steuererklärung erst aus der Presse erfahren müssen. Ob bei der Einführung die datenschutzrechtlichen Anforderungen erfüllt sind, kann ich derzeit mangels prüfbarer Unterlagen nicht beurteilen.

3.10 Televerwaltung beim Ministerium für Bildung, Kultur und Wissenschaft

Ende 1996 wurde ich vom Ministerium für Bildung, Kultur und Wissenschaft (MBKW) darüber informiert, daß ein Projekt "Televerwaltung Saar - Kommunikation und Workflow über verteilte Standorte" geplant sei, ich wurde um datenschutzrechtliche Mitwirkung gebeten.

Vorausgegangen war ein Forschungsprojekt "IVM-Innovatives Verwaltungsmanagement - Referenzmodelle für das Lehrermanagement". Aufbauend auf dessen Ergebnissen sollten zum Handlungsfeld "Workflow und Bildungsinformationssystem" Lösungen entworfen werden, die die Kommunikation zwischen Lehrern, Schulen, Schulämtern und dem MBKW unterstützen und die Verwaltungsabläufe vereinfachen sollten. Die Lehrereinsatzplanung, das Erstellen von Statistiken und sogar eine Vorgangsverwaltung sollten realisiert werden, bei der die Vorgänge - z. B. Bewerbungen, Beurlaubungen, Versetzungen, Krankmeldungen, Dienstunfallmeldungen - elektronisch, statt auf Papier, versandt werden.

Im Rahmen der Telekommunikationsinitiative des MWF wurde das Projekt unterstützt von der Deutschen Telekom AG und der IDS Prof. Scheer GmbH und wissenschaftlich begleitet durch das Institut für Wirtschaftsinformatik der Universität des Saarlandes. Als erster Schritt sollte ein Datenaustausch für das Lehrermanagement über das Internet abgewickelt und sicher gestaltet werden.

Neben der Nutzung des Internetfür die landesweite Datenübertragung sollte der Internet-Server der Landesregierung, das Novell-Netz des MBKW und

das dort vorhandene Bildungs- und Informationssystem BIS auf Basis einer ORACLE-Datenbank zum Einsatz kommen. Die erforderliche Software sollte mit Hilfe des von Prof. Scheer entwickelten "ARIS-Workflow-Tool-Sets" entwickelt werden.

Bezüglich der datenschutzrechtlichen Anforderungen konnte ich auf meine Stellungnahmen zu gleichgelagerten früheren Projekten wie "LID", "Lehrerdatei", "RULEP" und "LEDA" verweisen. Mit Blick auf die besondere Risikosituation der beabsichtigten Datenübertragung über das Internet forderte ich eine Risikoanalyse und ein Sicherheitskonzept unter Berücksichtigung der IT-Sicherheitsrichtlinie des Saarlandes und des IT-Grundschutzhandbuchs des BSI. Als Probleme stellten sich sofort dar:

- Absicherung der Zugriffe von außen
- Sicherung der Datenübertragung
- Sicherung der Integrität der elektronischen Dokumente gegen Verfälschung
- Sicherung der Identität des Absenders
- Abschottung des verwaltungsinternen Intranet gegenüber dem Internet und der sonstigen Nutzung des Servers im MBKW.

Zu dem ersten Entwurf des Sicherheitskonzepts für die Internet-Komponente habe ich mich fachlich geäußert und dabei eine Reihe von Anregungen gegeben, aber auch auf noch offene Punkte hingewiesen. Zu einer abschließenden Beteiligung ist es nicht gekommen, weil das MBKW im September 1998 mitgeteilt hat, daß der inzwischen entwickelte Prototyp nicht im produktiven Einsatz verwendet werden soll und aus diesem Grunde das Sicherheitskonzept nicht weiterentwickelt wird.

Ich gehe davon aus, daß dieses Projekt oder ähnliche Projekte in Zukunft fortgeführt bzw. neu aufgesetzt werden dürften und bitte darum, dabei die bisher genannten Anforderungen zu berücksichtigen.

3.11 Datenschutz in Schulen

Bei Überprüfung der Installation einer Schulverwaltungssoftware habe ich in einer Schule festgestellt, daß der Betrieb von Rechnern in den Schulen unter den gleichen mängelbehafteten Bedingungen erfolgt, wie ich sie oben (TZ 3.6) bei der Prüfung kleinerer Gemeinden festgestellt hatte.

Hinzu kommt, daß nach der "Verordnung über die Erhebung, Verarbeitung und sonstige Nutzung personenbezogener Daten in den Schulen" vom 3. 11. 1986 (Amtsbl. S. 990) Verwaltungsarbeiten nur mit einem ausschließlich dafür bestimmten, nicht auch im Rahmen des Unterrichts verwendeten Rechner

ausgeführt werden dürfen. Diese Datenverarbeitungsanlagen dürfen auch nicht mit anderen vernetzt sein.

Kritisch ist letzteres insbesondere bei bus-förmiger Ethernet-Vernetzung (auch stern-förmiger mit Hilfe von Hubs), da dann jede Station im Netz prinzipiell den gesamten Datenstrom - z. B. auch einschließlich der im Klartext übertragenen Benutzerkennung und des Paßwortes des Systemverwalters - mitlesen kann. Bei Anschluß der Netze an das Internet kann dann, auch bei Vorschaltung eines sogenannten Firewall-Rechners, die Sicherheit der Schuldaten und -programme gefährdet sein. Auf meine Orientierungshilfe "Internet" sei noch einmal verwiesen.

Die Schulen werden gebeten, die kritischen Aussagen zur Prüfung kleinerer Gemeinden zu bewerten und in ihrem Bereich dafür zu sorgen, daß die genannten Mängel abgestellt und die Anforderungen der Verordnung erfüllt werden.

3.12 Checklisten für Unix, Novell, Windows-NT; Orientierungshilfe Internet

Der Landesbeauftragte für Datenschutz, Niedersachsen, hat mir freundlicherweise seine Checklisten zur Verfügung gestellt, die ich unter Berücksichtigung des Schutzstufenkonzepts der IT-Sicherheitsrichtlinie des Saarlandes ergänzt habe.

Ebenso wurde die Orientierungshilfe "Internet" von einem Arbeitskreis der Datenschutzbeauftragten des Bundes und der Länder an den aktuellen Stand angepaßt.

Beide Texte habe ich in mein Internet-Angebot aufgenommen, das für die öffentlichen Stellen im Land, aber auch allgemein unter www.lfd.saarland.de zugänglich ist. Auf die weiteren Materialien und Gesetzestexte in diesem Angebot möchte ich an dieser Stelle ebenfalls hinweisen.

Ich bitte die Behörden, das Angebot zu nutzen und die entsprechenden Hilfen konkret vor Ort einzusetzen.

3.13 IT-Sicherheitsrichtlinie des Saarlandes und Datenschutzkapitel im IT-Grundschutzhandbuch des BSI

Die in meinem letzten Tätigkeitsbericht angekündigte IT-Sicherheitsrichtlinie wurde nach Veröffentlichung im GMBl 1997 (S. 74) in Kraft gesetzt.

Diese IT-Sicherheitsrichtlinie gilt für die Planung und Realisierung der Sicherheit der Informationstechnik im Rahmen informationstechnischer und kommunikationstechnischer Verfahren in der Landesverwaltung. Sie ist er-

gänzend zu den ADV-Projektrichtlinien vom 30.10.1987, GMBl 1987, S. 346, anzuwenden.

Ziel der IT-Sicherheitsrichtlinie ist es, mit Hilfe eines umfassenden IT-Sicherheitsmanagements die Datensicherheit und den Datenschutz zu gewährleisten und dabei die Erstellung von Risikoanalysen und Sicherheitskonzepten zu unterstützen. Dabei ist das IT-Grundschutzhandbuch des Bundesamtes für die Sicherheit in der Informationstechnik (IT-GSHB) in der jeweils aktuellen Form als Maßnahmenempfehlung für den mittleren Schutzbedarf und als Mindeststandard für Verfahren der Informationstechnik und Kommunikation zugrunde zu legen.

Als Hilfe für die saarländischen Behörden habe ich in meinem Internet-Angebot ein Muster-Sicherheitskonzept bereitgestellt, das auch eine Risikoanalyse und eine Schutzbedarfsbewertung enthält und verschiedentlich schon als Grundlage für die Erarbeitung eines eigenen Konzeptes diente.

Das IT-GSHB war bisher im wesentlichen auf technische Sachverhalte und Aspekte der Datensicherung ausgerichtet. Obwohl diese Aspekte auch weitgehend dem Datenschutz Rechnung tragen, erscheint doch eine Ergänzung des Handbuchs aus datenschutzrechtlicher Sicht erforderlich. Dazu erarbeitete eine gemeinsame Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder mit dem BSI ein eigenes Datenschutzkapitel, das in der Version 1999 des Handbuchs veröffentlicht werden soll.

3.14 Virtuelles Prüfungsamt der Universität

Das wirtschaftswissenschaftliche Prüfungsamt hat unter dem Arbeitstitel VIPA ein "virtuelles" Prüfungsamt eingerichtet. Damit sollen die bisher üblichen Warteschlangen vor dem realen Prüfungsamt abgebaut und der für die Studenten zu erbringende Service im Rahmen von Prüfungsanmeldungen (pro Semester ca. 4500 Anmeldungen und ca. 1000 Abmeldungen) und Ergebnisbereitstellung (bisher Listen mit Matrikelnummern am schwarzen Brett) verbessert werden.

Auf Anfrage übersandte die Universität eine Beschreibung des Verfahrens und ein Sicherheitskonzept. Verschiedene Aspekte, die sich aus den Unterlagen nicht klar ergaben und ergänzende Fragen wurden bei einem Besuch vor Ort diskutiert. Für Testzwecke wurde dem LfD auch eine Testkennung bereitgestellt. Danach stellt sich das System wie folgt dar:

Gegen Vorlage seines Personalausweises erhält ein Student ein individuelles Paßwort und kann mit Hilfe seiner Matrikelnummer über das Internet auf einen VIPA-Server zugreifen, der folgende Dienstleistungen bietet:

- Auswahl von Wahlpflichtfächern
- An- und Abmeldungen zu Prüfungen

- Rücktritt von Teilprüfungen
- Seminaranmeldungen
- Ändern der eMail-Adresse
- Anforderung von Transaktionsnummern
- Ändern des Paßwortes
- Ziehung von Diplomarbeiten
- Abfragen von Informationen (Noten, Anmeldestatus, eMail-Adresse, Prüfungstermine)
- schwarzes Brett.

Kritische Aktivitäten, wie z. B. die Änderung des Paßwortes oder die Anmeldung zu einer Prüfung müssen zusätzlich mit Hilfe von sogenannten Transaktionsnummern bestätigt werden, die dem Studenten ausgehändigt werden und ihn eindeutig identifizieren, so wie es im Bankenbereich schon seit längerem üblich ist.

Das von der Universität Bamberg für ein virtuelles Prüfungsamt entwickelte System FLEXNOW wurde übernommen und an die spezifische Situation und die Bedürfnisse in Saarbrücken angepaßt (Win-NT-Server, ADABAS-Datenbank). Das VIPA-System besteht aus zwei (logischen) Servern: einem Datenbank-Server zur Verwaltung der Daten und einem Internet-Server zur Kommunikation über das Internet. Ein Durchgriff von einem Server aus auf den anderen ist prinzipiell nicht möglich. Auf den Datenbankserver können nur das Prüfungsamt (Prüfungsordnung, Studenten- und Prüfungsverwaltung, Raum- und Zeitplanung, Mail-Versand), der Prüfungsausschußvorsitzende (lesend auf die Lehrstuhlinfos, Statistiken) und die Lehrstühle (eingeschränkt auf lehrstuhlspezifische Prüfungen und Ergebnisse, Diplomarbeiten) zugreifen. Der Datenübergang zwischen Internet- und Datenbankserver erfolgt mit Hilfe von eMails.

Das Verfahren fand sich zum Zeitpunkt der Prüfung schon im Echteinsatz, ohne daß die gesetzlich vorgeschriebene Beteiligung des LfD oder die Freigabe des Verfahrens erfolgt war. Eine Meldung zum Dateienregister lag nicht vor. Der Datenschutzbeauftragte der Universität war nicht beteiligt worden.

Aus datenschutzrechtlicher Sicht problematisch an dieser Lösung waren insbesondere:

- Datenbank- und Internet-Server liefen als Softwarelösung auf dem gleichen physikalischen Rechner
- ein Firewall zur Absicherung des Internet-Übergangs war nicht vorhanden

- der eMail-Verkehr wurde über einen Server der Universität in Bamberg abgewickelt, so daß alle Paßworte im Klartext über ungeschützte Internet-Leitungen liefen.

Um den Datenschutz zu gewährleisten, habe ich gefordert:

- den Datenbank- und Internet-Server auf getrennte Rechner zu verlagern
- den Internet-Übergang durch eine Firewall abzusichern
- den eMail-Verkehr über den Bamberger Rechner aufzugeben und statt dessen über einen sicheren Rechner der Universität abzuwickeln
- die TAN-Listen-Verschlüsselung vom Rechner der Universität Bamberg zum VIPA-Rechner der Universität Saarbrücken zu verlagern
- den Serverbetrieb und damit die Datenübertragung über das Internet zum Studenten über eine SSL-Verbindung zu verschlüsseln und damit zu sichern
- eindeutige Benutzerkennungen für Mitarbeiter der Lehrstühle zu vergeben und die Aktivitäten auf den Servern ausreichend zu protokollieren.

Das wirtschaftswissenschaftliche Prüfungsamt hat zugesagt, meinen Forderungen kurzfristig zu entsprechen. Ein Vollzug der ersten, wichtigsten Schritte wurde schon mitgeteilt. Eine schriftliche Stellungnahme zu meinem Prüfbericht steht noch aus.

3.15 Fax in Personalangelegenheiten

Verhaltensregeln, die so selbstverständlich sind, daß jeder sie kennt und beachtet, müssen nicht eingehend in Vorschriften fixiert sein. Leider gibt es auch in der öffentlichen Verwaltung immer wieder Fälle, in denen selbst elementare Schutzvorkehrungen beim Umgang mit personenbezogenen Daten nicht beachtet werden, und dann schätzt man die Hilfe von Verwaltungsvorschriften, die den korrekten Weg weisen.

So erhielt ich beispielsweise Hinweise, daß eine oberste Landesbehörde eilbedürftige Benachrichtigungen in Personalangelegenheiten mit sehr sensitiven Daten dem Betroffenen per Fax übermittelt hatte.

Der Betroffene sah sich zu Recht dadurch in seinem Recht auf informationelle Selbstbestimmung verletzt, daß auf diesem Weg leicht für andere die Möglichkeit eröffnet würde, von dem Inhalt der an ihn gerichteten Benachrichtigung Kenntnis zu nehmen. Im konkreten Fall hätte etwa wegen der Sensitivität der Daten mit dem Adressaten eine Vereinbarung darüber ge-

troffen werden müssen, daß dieser am Telefax-Gerät steht, wenn die vertrauliche Telefaxsendung ausgedruckt wird.

Ich möchte deshalb nochmals darauf hinweisen, daß jede öffentliche Stelle für die Nutzung von Telefax-Geräten eine solche Dienstanweisung erlassen sollte. Dies ist vielfach, trotz der wohl flächendeckenden Ausstattung der öffentlichen Stellen mit Telefax-Geräten, noch nicht geschehen. Durch den Erlaß einer Dienstanweisung werden den Bediensteten häufig erst die Gefahren für eine Verletzung des Rechts auf informationelle Selbstbestimmung durch die Nutzung von Telefax-Geräten bewußt.

Insbesondere die obersten Landesbehörden sollten hier vorbildlich im eigenen Ressort handeln und im nachgeordneten Bereich für den Erlaß der Dienstanweisung Sorge tragen. Eine positive Rückmeldung für den gesamten Landesbereich in der Stellungnahme der Landesregierung würde ich daher sehr begrüßen.

Ein Muster einer "Dienstanweisung für die Übermittlung von Daten mit Hilfe von Telefax-Geräten" habe ich als Anlage 10 zu meinem 14. TB vorgestellt und auf die Problematik auch in meinem letzten Bericht hingewiesen (Anlage 3 zum 16. TB).

4 Polizei

4.1 Automatisiertes Informationssystem der Polizei "DIPOL"

Weil polizeiliche Arbeit zu einem erheblichen Teil Umgang mit Informationen ist, kommt dem Vorhaben, diese Tätigkeit mit einem automationsgestützten Verfahren zu erleichtern und effizienter zu machen, besondere Bedeutung zu. Wie bereits in meinem 16. Tätigkeitsbericht (vgl. TZ 5.8) dargestellt, wurde für das Projekt DIPOL, mit dem die Polizei im Saarland bereits seit längerem befaßt ist, ein neues technisches Konzept erstellt. An der Umsetzung werde ich beteiligt. Inzwischen wurden die Polizeidienststellen mit der entsprechenden Hardware ausgestattet. Auch wurden als Zugangssicherung Chipkarten ausgegeben, ohne die eine Anmeldung an dem polizeilichen Rechner im Rahmen der DIPOL-Anwendung nicht möglich ist.

Als erste Entwicklungsstufe war neben der Textverarbeitung zunächst eine formularorientierte Arbeitsplatzlösung eingeführt worden. Mit deren Hilfe wird das Ausfüllen und der Ausdruck der gebräuchlichsten Formulare erleichtert. Die dazu benötigten personenbezogenen Daten werden nach kurzer Zeit gelöscht. Ich konnte bei der Gestaltung der Formulare meine datenschutzrechtlichen Forderungen einbringen, die größtenteils auch berücksichtigt wurden.

Inzwischen wurde innerhalb der datenbankorientierten Individualsoftware DIPOL ein Prototyp entwickelt, der mir vorgeführt wurde. Mit ihm können in

verschiedenen der angestrebten Verfahrensschritte und -arten personenbezogene Daten verarbeitet werden. Eine dauerhafte Speicherung von Daten ist allerdings auch hiermit noch nicht verbunden, da bei Fortschreibung der Software die bisher gespeicherten Daten gelöscht werden.

Auch das Sicherheitskonzept, das ich gefordert hatte, wurde inzwischen vorgelegt. Es berücksichtigt meine datenschutzrechtlichen Anregungen zum größten Teil. Für die verschiedenen Einsatzbereiche (Polizeiwache, -Inspektion, -Direktion) wurden spezielle Checklisten zum Datenschutz - Prüfung Netzwerk Windows NT - vorgelegt, die die Zielkonzeption beschreiben und noch umzusetzen sind. Offen ist nach wie vor auch die datenschutzrechtliche Beurteilung der Benutzerrechtematrix, der Aufbewahrungsfristen sowie der zu speichernden Protokollierungen im DIPOL-Verfahren.

Die Fortentwicklung dieses wichtigen Projekts werde ich weiterhin kritisch, aber konstruktiv begleiten.

4.2 Einsatz privater PC im Polizeibereich

Trotz der Ausstattung mit Geräten im Hinblick auf den DIPOL-Einsatz scheint indes jedenfalls bei manchen Dienststellen Bedarf zu bestehen, noch weitere EDV-Unterstützung zu erhalten. So wurde ich seitens des Ministeriums des Innern mit dem Wunsch einer Polizeiinspektion befaßt, verschiedene - selbst entwickelte - Verfahren auf einem privaten PC erledigen zu wollen, mit dem insbesondere Personaldaten der in der Dienststelle tätigen Polizisten verarbeitet werden sollten. Die für den Polizeibereich verbindliche Polizeidienstvorschrift sieht die Genehmigung für den Einsatz eines privaten PC nur vor, wenn keine personenbezogenen Daten, mit Ausnahme von Daten im Rahmen der Textverarbeitung, gespeichert werden.

Zu der Problematik bei Einsatz privater Hard- und Software hatte ich beim Erlaß der "Dienstanweisung für den Einsatz von Personalcomputern bei den Behörden und Einrichtungen der Vollzugspolizei des Saarlandes" Stellung genommen. Bereits damals hatte ich Bedenken gegen den Einsatz sowohl im dienstlichen wie auch privaten Bereich geäußert. Obwohl das Ministerium des Innern diese Bedenken teilte, sah es sich seinerzeit aufgrund faktischer Zwänge veranlaßt, den Einsatz privater Hard- und Software unter bestimmten in der Dienstanweisung festgelegten Voraussetzungen zuzulassen. Allerdings - so die Aussage des Ministeriums - sollte es sich lediglich um eine Übergangsregelung handeln, da mit fortschreitender Bereitstellung dienstlicher IT-Komponenten der Bedarf für den Einsatz privater Hard- und Software entfalle. Mitte 1996 waren jedenfalls noch ca. 142 private IT-Komponenten im Einsatz. Wie der oben dargestellte Antrag einer Polizeiinspektion zeigt, ist offensichtlich auch im Jahre 1998 der Bedarf nach dienstlich zur Verfügung gestellten IT-Komponenten noch nicht ausreichend gedeckt.

Die Restriktion der genannten Vorschrift ist in Anbetracht der erhöhten Risiken für die Persönlichkeitsrechte der Betroffenen sachgerecht, da insbesondere im Bereich der Datenschutzkontrolle bei privaten Komponenten Defizite auftreten können. Dies gilt auch dann, wenn es wie im konkreten Fall - im wesentlichen - um personenbezogene Daten von Bediensten und weniger um den korrekten Umgang mit Informationen über unbeteiligte Bürger geht. Ich habe deshalb dem Ministerium empfohlen, die erforderliche Genehmigung zu versagen.

Meines Erachtens spricht viel dafür, gerade im Polizeibereich ein generelles Verbot des Einsatzes privater Hard- und Software durchzusetzen, wie es in den anderen Verwaltungsbereichen bereits praktiziert wird.

4.3 Datenschutzvorgaben für Polizeiinspektionen

Bei einer Polizeiinspektion mittlerer Größenordnung habe ich in einzelnen Bereichen die Datenverarbeitung kontrolliert. Der Umfang dabei festgestellter Mängel, über die ich auch das Innenministerium unterrichtet habe, blieb erfreulicherweise gering. Auch wenn schon aufgrund des Stichpobencharakters der Prüfung meine Feststellungen keinen Anspruch auf Vollständigkeit erheben können, soll hier exemplarisch für alle Polizeidienststellen dieser Größenordnung im folgenden dargestellt werden, in welchen Bereichen ich auf Fehler gestoßen bin. Ich gehe dabei davon aus, daß die entsprechenden Dienststellen der Polizei von sich aus zumindest diese Mängel, sofern sie auch in ihrem Bereich bestehen sollten, bereinigen werden.

4.3.1 IT-Einsatz

Solange das für den landesweiten Einsatz konzipierte DIPOL-Projekt noch nicht verwirklicht ist, muß die Polizeidienstvorschrift 880 (SL) beachtet werden, die die ordnungsgemäße Handhabung eingesetzter Disketten regelt.

Das Ministerium des Innern hat mir mitgeteilt, daß gleichzeitig mit der Beschaffung dienstlicher Datenträger die Nutzung privater Datenträger untersagt wurde.

4.3.2 Einsicht in das Melderegister

Stellt die Polizei Auskunftsersuchen an das Meldeamt nach § 31 Abs. 3 Meldegesetz (MG) zu Daten, die über den Datenumfang des § 31 Abs. 1 MG einschließlich der Paßdaten hinausgehen oder sich auf Hinweise zu jedweden Meldedaten beziehen, so muß sie dies aufzeichnen. Zwar kommen diese Auskunftsersuchen seltener vor als solche nach § 31 Abs. 1 MG, die bereits einen Umfang von 13 Einzeldaten beinhalten; für die Gewährleistung der

Aufzeichnungspflicht bei diesen sogenannten "erweiterten Übermittlungsersuchen" sollten die Dienststellen jedoch durch entsprechende Formulare Vorsorge treffen. Diese Aufzeichnungen sind gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Erstellung der Aufzeichnung folgt, zu vernichten.

Inhaltlich gleichlautende Bestimmungen gelten des weiteren, unabhängig vom Umfang der Daten, bei der Einsichtnahme der Polizei außerhalb der Dienstzeiten der Meldebehörden in Listen oder Mikrofilme (§ 5 Abs. 5 Meldedatenübermittlungsverordnung).

4.3.3 Auskunft von der örtlichen Kfz-Zulassungsstelle

Für die Übermittlung von Daten aus dem örtlichen Fahrzeugregister außerhalb der üblichen Dienstzeiten sieht § 36 Abs. 8 Straßenverkehrsgesetz ebenfalls eine gesonderte Aufzeichnungs- und Aufbewahrungspflicht für die Polizei vor, die nicht deswegen vernachlässigt werden darf, weil die Fälle selten vorkommen. An die insofern bestehende Verfügung des Landeskriminalamtes aus dem Jahre 1993 wäre nochmals zu erinnern.

4.3.4 Amtshilfeersuchen an die Polizei von Stellen außerhalb des Saarlandes in Verwarnungsgeldverfahren

Durch Erlasse hat das Ministerium des Innern bestimmt, in welchen Fällen Bildvergleiche an Hand des Personal-/Paßausweisregisters durchgeführt werden dürfen. Es wurde festgelegt, daß Bildvergleiche im Bereich der Verwarnungsgeldverfahren unter Verhältnismäßigkeitsgesichtspunkten nicht gerechtfertigt seien. Diesem Verfassungsgrundsatz muß jegliches staatliches Handeln Rechnung tragen.

Klargestellt wurde in diesem Zusammenhang, daß es insofern keinen Unterschied gibt zwischen Amtshilfeersuchen im Verwarnungsgeldbereich von saarländischen oder außersaarländischen Dienststellen, da dem Verfassungsgrundsatz der Verhältnismäßigkeit stets Geltung zu verschaffen ist. Allerdings soll, wie mir bekannt wurde, ein entsprechender Erlaß des Ministeriums des Innern noch ausstehen, so daß in manchen Dienststellen zwischen saarländischen und außersaarländischen Ersuchen immer noch zu Unrecht differenziert wird.

4.3.5 Aufbewahrung von Unterlagen, die zu keiner polizeilichen Maßnahme führten, und sonstigen Loseblattsammlungen

Am Grundsatz der Erforderlichkeit muß sich die Aufbewahrung von Unterlagen ausrichten, mit der polizeiliches Handeln dokumentiert wird. Die generelle Aufbewahrungsdauer von 5 Jahren erscheint entschieden zu lang, wenn darin auch beispielsweise Fälle wie erfolglose Suizidversuche einbezogen werden.

Falsch ist, der Lösung dieser Problematik mit Hinweis auf vorgesehene Löschungsfristen in einem künftigen automationsgestützten Verfahren ausweichen zu wollen. Im Zusammenhang mit der geplanten Speicherung im EDV-System des DIPOL-Projektes sind die Aufbewahrungszeiten noch nicht abschließend erörtert. Ich bin der Auffassung, daß indes für die Aktenaufbewahrung schon heute verkürzte Fristen zur Wahrung des Rechts auf informationelle Selbstbestimmung festgelegt werden können. Auch durch Speicherungen in den Akten halten Eingriffe in die Persönlichkeitsrechte unverhältnismäßig lange an, so daß vor allem nicht der unbestimmte Zeitpunkt abgewartet werden darf, zu dem DIPOL endgültig verwirklicht ist.

4.4 Vorlage von Lichtbildern bei Verfolgung von Ordnungswidrigkeiten

Im Berichtszeitraum wurde Beschwerde darüber geführt, daß im Rahmen der Fahrerermittlung zu Verkehrsordnungswidrigkeiten bei Dritten Beweisfotos vorgelegt wurden, auf denen außer dem Fahrer weitere Begleitpersonen erkennbar abgebildet waren.

Die Vorlage des Beweisfotos bei Dritten (Nachbarn, Arbeitgebern, Familienangehörigen) stellt eine sehr belastende Maßnahme dar, die erst dann ergriffen werden darf, wenn alle anderen Ermittlungen wie Vorladung des Betroffenen, Aufsuchen des Betroffenen in der Wohnung, Vergleich mit dem Bild im Personalausweisregister nicht zum Erfolg geführt haben (vgl. dazu meinen 15. TB, TZ 2.3). Für die Fahrerermittlung reicht regelmäßig ein Foto aus, das eventuelle Begleitpersonen nicht erkennen läßt. Sind solche Personen mit abgebildet, sind sie vor Vorlage zu schwärzen oder abzudecken; es sei denn, die Ermittlungen erfordern die Feststellung der Identität der Begleitperson, beispielsweise um sie als Zeuge zu vernehmen.

Das Ministerium des Innern teilt meine Rechtsauffassung und hat zwischenzeitlich durch Erlaß die beschriebene Verfahrensweise verbindlich geregelt.

4.5 Verkehrsunfallaufnahme durch die Polizei

Mit Wirkung zum 1. Januar 1998 hat der Minister des Innern die Polizeidienstvorschrift "Aufgaben der Polizei bei Verkehrsunfällen" in Kraft gesetzt.

Eine rechtzeitige Beteiligung im Sinn des § 8 Abs. 1 SDSG erfolgte nicht. Ich habe deshalb nachträglich aus datenschutzrechtlicher Sicht folgende Verbesserungen gefordert:

- Die Aufbewahrung der Unterlagen bei der Spurensuche ist in Abhängigkeit vom Ausgang des Verfahrens zu regeln.
- Anstelle des in der Vorschrift abgedruckten Formulars bei Anhörung des Betroffenen an der Unfallstelle ist ein bereits früher mit dem Ministerium des Innern abgestimmtes datenschutzgerechtes Formular zu verwenden.
- Spontane Äußerungen und Angaben bei der ersten informatorischen Befragung dürfen nicht in die Anzeige aufgenommen werden, weil dies einer vorweggenommenen Vernehmung gleichkommt, ohne daß der Betroffene über das ihm zustehende Zeugnisverweigerungsrecht belehrt wurde.
- Die Vorlage der Unfallakten von außerdienstlichen Unfällen von Polizeibeamten, bei denen ein Straftatbestand verwirklicht wurde, an den Dienstvorgesetzten ist nicht gerechtfertigt; die Unterrichtung im Rahmen des Justizmitteilungsgesetzes ist ausreichend.

Inwieweit meinen datenschutzrechtlichen Forderungen entsprochen wurde, entzieht sich meiner Kenntnis.

4.6 Videoabstandsmeßanlage bei der Polizei

Bei der Überprüfung der Anlage wurde festgestellt, daß bis März 1997 die Abstandsmessung in der Weise erfolgte daß mit einer Videokamera von Autobahnbrücken in einer "Totaleinstellung" das gesamte Verkehrsverhalten auf der Autobahn über eine Wegstrecke von etwa 300 m aufgezeichnet wurde. Diese Videoaufnahme ließ im Regelfall eine Identifizierung der im Fahrzeug befindlichen Insassen sowie des Kfz-Kennzeichens nicht zu. Bei Verdacht eines ahndungswürdigen Abstands- und in Ausnahmefällen eines Geschwindigkeitsverstoßes lösten die Beamten eine auf dem Mittelstreifen installierte Frontfotoanlage manuell aus. Über die permanent eingespielte Zeit bei beiden Geräten erfolgte die Zuordnung des Frontfotos zu der Videosequenz.

Gegen die geschilderte Verfahrensweise bestehen aus datenschutzrechtlicher Sicht keine Bedenken, da identifizierende Aufnahmen nur von Störern bei Vorliegen eines konkreten Anfangsverdachtes vorgenommen werden. Identifizierbare Aufnahmen Unverdächtiger sind bei diesem Verfahren im Regelfall ausgeschlossen.

Von März 1997 bis Dezember 1997 wurde neben der Videokamera für den Gesamtverkehr eine zweite Kamera installiert, die parallel über die gesamte Meßzeit - in der Regel über die Länge des Videobandes - die Fahrzeugin-

sassen sowie die Kfz-Kennzeichen identifizierbar aufgenommen hat. Je nach Fahrzeugdichte und Verkehrsverhalten der Verkehrsteilnehmer konnte es vorkommen, daß nur wenige Verkehrsverstöße, dagegen eine Vielzahl sich korrekt verhaltender Verkehrsteilnehmer aufgenommen wurden. Da eine Rechtsgrundlage für die Anfertigung der Aufnahmen nicht ersichtlich ist, habe ich die Löschung der unzulässig erfolgten Aufnahmen gefordert. § 100c StPO verlangt einen Anfangsverdacht, der bei dieser Aufnahmepraxis jedoch im Regelfall nicht vorlag. Nach Auskunft der Polizei ist eine Bereinigung der Aufnahmen zwischenzeitlich erfolgt.

Seit Anfang 1998 stellt sich das Aufnahmeverfahren der Polizei ähnlich dem bei den Kommunen praktizierten Verfahren dar (vgl. TZ 6.3) Es werden nur noch Videoaufnahmen gefertigt, wenn der Verdacht eines ahndungswürdigen Verkehrsverstoßes vorliegt. Da im Gegensatz zu den Anlagen der Kommunen bei der Auswertung kein spezielles Verfahren zur Verfügung steht, das die Kenntnisnahme Unverdächtiger weitgehend ausschließt, ist auf jeden Fall eine hohe Wahrscheinlichkeit für das Vorliegen eines Verkehrsverstoßes zu fordern und die Sequenzen sind auf das erforderliche Mindestmaß zu reduzieren. Die technisch-organisatorischen Datensicherungsmaßnahmen mußten ebenfalls verbessert werden. So wurde die Aufbewahrungsdauer auf 2 Jahre reduziert und zur Löschung der Bänder ein besonders Entmagnetisierungsgerät eingesetzt.

4.7 Auskunft über Daten aus dem Polizeibereich durch den LfD

Wenn Betroffene sich an mich wenden, weil sie den Umgang mit ihren Daten durch die Polizei nicht für korrekt halten, machen sie von ihrem Anrufungsrecht nach § 25 SDSG Gebrauch und haben Anspruch auf Mitteilung der Ergebnisse meiner Überprüfung. Manchmal haben sie zuvor oder gleichzeitig von der Polizei selbst Auskunft erbeten darüber, ob und welche Daten über sie gespeichert sind. Gelegentlich erwarten sie diese Mitteilung aber auch von mir. Hierzu detaillierte Auskünfte zu geben, ist sicher nicht meine Aufgabe, aber in vielen Fällen - zumal dann, wenn eben keine Speicherung vorliegt - ist sinnvoll, in meiner Antwort hierzu nicht völlig zu schweigen.

Zwar steht es in der ausschließlichen Entscheidungskompetenz des LfD, ob und in welchem Rahmen er inhaltliche Auskunft an den Petenten erteilt. Der Umfang der Auskunft kann jedoch durch § 18 Abs. 5 SDSG eingeschränkt sein, wenn die Zustimmung zur Auskunftserteilung eingeschränkt oder versagt wird, was das Polizeigesetz zuläßt. Durch diese Vorschrift soll eine unzulässige Umgehung der Auskunftsverweigerung durch die Polizei verhindert werden. Allerdings sind im Regelfall die für die Auskunftsverweigerung geltenden Gründe zu nennen.

Über einige Zeit lang hat es sich das Landeskriminalamt aber zu leicht gemacht, wenn es Auskünfte an Betroffene durch den LfD als nicht sinnvoll an-

gesehen und meiner Bitte um Zustimmung zur (inhaltlichen) Auskunft schlicht entgegengehalten hatte, der Betroffene könne ja eine Auskunft durch die Polizei unmittelbar erhalten. Es bedurfte einiger Mühen klarzumachen, daß dies die Betroffenenrechte verkürzt und nicht im Einklang mit der Rechtslage steht.

Das Ministerium des Innern teilt meine Auffassung.

4.8 Datenweitergabe durch die Polizei an den Vermieter

Ein Petent hat sich an mich gewandt, weil das Verhalten eines Polizeibeamten für ihn einschneidende Veränderungen in seinen Wohnverhältnissen mit sich brachte.

Der Polizeibeamte hatte sich, nachdem die Beschlagnahme von Gegenständen, die dem Petenten gehörten, aufgehoben worden war, darum bemüht, den Betroffenen hiervon zu benachrichtigen. Da er jedoch nur dessen Vermieter angetroffen hatte, bat er diesen, er möge dem Mieter ausrichten, daß er ehemals beschlagnahmte Gegenstände bei der Polizei abholen könne.

Der Vermieter erhielt dadurch Kenntnis von Umständen, die ihn nichts angingen und aus denen er möglicherweise völlig unberechtigte Schlüsse ziehen konnte. Wie mir berichtet wurde, hat er tatsächlich den Kontakt des Petenten zur Polizei zum Anlaß genommen, das Mietverhältnis mit ihm zu kündigen.

- Im Rahmen der disziplinarrechtlichen Bewertung wurde der Polizeibeamte eingehend darüber belehrt, daß hier ein Datenschutzverstoß vorlag, der für den Petenten in der Realität gravierende Auswirkungen hatte.

  Sehr befremdlich erschien bei dieser doch recht eindeutig unzulässigen Datenübermittlung von einer öffentlichen an eine private Stelle die Wertung des Sachverhaltes durch das Oberlandesgericht des Saarlandes. In einem Beschluß des Gerichtes heißt es, die Bitte der Polizei an den Vermieter, er möge seinen Mieter informieren, daß ein zuvor beschlagnahmter Gegenstand in Empfang genommen werden könne, enthalte in keiner Weise eine Diskriminierung.

5 Justiz

5.1 Großer Lauschangriff

Herausragend in der rechtspolitischen Diskussion war im Berichtszeitraum, daß der Bundesgesetzgeber die Rechtsgrundlage für das heimliche Abhören von Personen in Privatwohnungen zum Zweck der Strafverfolgung geschaffen hat. Er ist damit dem Drängen vor allem von Sicherheitsorganen und -politikern gefolgt, die diesen Eingriff in zuvor besonders geschützte Bereiche

auch zu Strafverfolgungszwecken als unabdingbar ansehen, die Bevölkerung effektiv vor schwerer Kriminalität zu schützen.

Mit gutem Grund hatte die bisherige Verfassung der Bundesrepublik dies ausgeschlossen; denn jedenfalls solange es nicht um die Abwehr unmittelbar drohender Gefahr für Leib und Leben geht, sollte der engste Bereich persönlicher Lebensgestaltung staatlicher Ausforschung verwehrt bleiben. Nun erlaubt das geänderte Grundgesetz das amtliche Belauschen aus Wohnungen - und zwar nicht nur von "Gangstern" - auch zu einem anderen Zweck.

Auf Bedenken habe ich in TZ 12.9 meines letzten Tätigkeitsberichts hingewiesen, ebenso auf Forderungen, denen mindestens bei einem derartigen Schritt entsprochen werden müßte; sie waren einmütig von den Kollegen im Bund und allen Ländern erhoben worden. Tatsächlich haben einige dieser Punkte nach intensiver Diskussion Eingang in die konkrete Regelung der Strafprozeßordnung gefunden, jedoch nicht alle.

Zwar hat nun der Gesetzgeber mit ausreichender Mehrheit eine Entscheidung getroffen, doch Rechtsfrieden besteht nicht, weder selbstverständlich bei denjenigen, die die Befugnis schon grundsätzlich für unvereinbar mit einer liberalen Verfassung halten, noch bei solchen, die das konkrete Verfahren und seine Voraussetzungen so nicht akzeptieren wollen.

Tatsächliche Grenzen eines Eingriffs in den Intimbereich, der jeden Bürger treffen kann, werden das zu Recht nicht einfache Verfahren, vor allem aber technische Kapazität, Zeit und Kosten setzen. Der Betroffene kann sich damit nicht trösten.

Und noch weitergehend wird gefordert, auch die im Gesetzgebungsverfahren abgelehnte heimliche optische Überwachung in Privatwohnungen möglich zu machen, also den "Spähangriff". Ist es dann nur ein Versehen, wenn auf eine Frage zum Großen Lauschangriff Vertreter der Polizei sich mir gegenüber zur Beschaffung von Video-Überwachungsgeräten äußerten?

5.2 DNA-Identitätsfeststellungsgesetz

Die gentechnische Analyse von Körperzellen und ihr Vergleich mit vorgefundenem Spurenmaterial ist ein recht zuverlässiges und deswegen immer mehr verwendetes Mittel zur Aufklärung von Straftaten. Voraussetzungen und Verfahren für den Einsatz in konkreten Fällen hat der Bundesgesetzgeber im März 1997 in der Strafprozeßordnung geregelt ("Genetischer Fingerabdruck"). Mit der Bindung daran, daß der Eingriff richterlich angeordnet werden und die DNA-Analyse anonymisiert erfolgen muß sowie daß die Erkenntnisse prinzipiell nur zweckgebunden verwendet werden dürfen, kommt das Gesetz wesentlichen datenschutzrechtlichen Forderungen nach.

Schon früher wurde die Forderung erhoben, diese Methode auch vorbeugend - also außerhalb konkreter Straf- bzw. Ermittlungsverfahren - nutzbar

zu machen: Selbst wenn keinerlei sonstige Verdachtsmomente vorliegen, kann so der Abgleich aufgefundenen Materials mit bereits vorliegenden Proben beispielsweise eines bereits früher einschlägig vorbestraften Menschen schnell dessen Täterschaft aufzeigen oder sie umgekehrt weitestgehend ausschließen. Besonders unter dem Eindruck von Fällen schwerster Sexualkriminalität, die auch die Bevölkerung erschüttert hatten, wollte man schnelle Ergebnisse, und so ordnete der Bundesinnenminister den Aufbau einer Datei beim Bundeskriminalamt an, noch bevor in einem speziellen Gesetz hierfür die Rechtsgrundlage geschaffen war. Auf dessen Notwendigkeit und die hierbei zu beachtenden Punkte hatten die Datenschutzbeauftragten mit Entschließung vom 17./18. April 1997 (Anlage 19.2) eindringlich hingewiesen.

Inzwischen hat der Bundestag im "DNA-Identitätsfeststellungsgesetz" vom 7. 9. 1998 Voraussetzungen und Verfahren einer Speicherung festgelegt: Es geht jetzt darum, die Errichtungsanordnung für die höchst sensible Zentraldatei beim Bundeskriminalamt den Bedingungen dieses Gesetzes anzupassen und das Verfahren zu regeln, mit dem der Verkehr mit den Polizeibehörden der Länder bestimmt wird. Hieran sind die Datenschutzbeauftragten beteiligt.

Aus der Diskussion herausgreifen möchte ich die Frage, ob die Speicherung in der Datei auch auf die Einwilligung des Betroffenen gestützt werden darf; das Gesetz bestimmt ja, daß der Richter die molekulargenetische Untersuchung und die Speicherung in der DNA-Datei anordnet.

- Daß zur Entnahme von Körperzellen, die gewöhnlich aus einem Mundhöhlenabstrich besteht, die Einwilligung als Rechtfertigung herangezogen wird, ist - problematische - Praxis. (Rechtlich zweifelhaft kann hier sein, ob es nicht aufgrund faktischer Zwänge oft weitgehend der erforderlichen echten Freiwilligkeit entbehrt; erinnert sei nur an den Massentest in Norddeutschland, der allerdings letztlich zum Ergreifen des Täters geführt hat.)

  In Übereinstimmung mit der saarländischen Justizverwaltung vertrete ich die Auffassung, daß aber allenfalls die Entnahme von Körperzellen von der Einwilligung des Betroffenen gedeckt sein kann. Diese Rechtfertigung kommt aber nicht in Betracht für die Durchführung der molekulargenetischen Untersuchung und erst recht die Speicherung in einer staatlicherseits errichteten Datei, die Strafverfolgungszwecken dienen soll. Diese weitergehenden Schritte dürfen m.E. keinesfalls auf die Einwilligung von "braven" Bürgern gestützt werden, die sich hierdurch gewissermaßen vorbeugend von jeglichem Verdacht fernhalten wollen. Das entspräche auch nicht dem gesetzlich festgelegten Zweck der Datei, die Überprüfung mit vermutlichen Wiederholungstätern bei schwersten Straftaten möglich zu machen; die Datei würde zudem aufgebläht, so daß auch die Datenpflege im Übermaß anwachsen würde.

In der Errichtungsanordnung zu der Datei sollte klargestellt werden, daß lediglich DNA-Ergebnisse, denen eine richterliche Anordnung zugrunde liegt, dauerhaft gespeichert werden dürfen.

5.3 Neufassung der Anordnung über Mitteilungen in Strafsachen (MiStra)

Nachdem im Berichtszeitraum das Justizmitteilungsgesetz nach einer langwierigen Gesetzgebungsphase in Kraft getreten ist, waren auch die bereits bestehenden untergesetzlichen, konkretisierenden Verwaltungsvorschriften über Mitteilungen in Strafsachen zu novellieren. Diese sind nunmehr ab 1.6.1998 in Kraft.

Vor ihrem Erlaß waren die Datenschutzbeauftragten des Bundes und der Länder an der Novellierung beteiligt. Die Vorschläge und Anregungen wurden dabei zum Teil berücksichtigt.

Einen Vorschlag, der meines Erachtens mit unzutreffender Begründung unberücksichtigt geblieben ist, möchte ich jedoch nochmals aufgreifen.

Die Datenschutzbeauftragten haben gefordert, daß dann, wenn Mitteilungen in Ausnahmefällen erfolgen oder von der Unterrichtung Betroffener gänzlich abgesehen werden soll, die für die Anordnung maßgeblichen Gründe - etwa in Form eines Aktenvermerks - dokumentiert werden.

Der Vorschlag wurde abgelehnt, weil eine "vorsorgliche Begründung" hinsichtlich evtl. später auf Initiative der Betroffenen zu treffender Entscheidungen auch sonst im Rahmen staatlichen Handelns nicht vorgesehen sei. Außerdem sei der zusätzliche und gesetzlich nicht vorgeschriebene Aufwand der Praxis - angesichts der vorhandenen Belastung - nicht zumutbar.

Bei den Mitteilungen handelt es sich in aller Regel um zweckändernde Verarbeitung von personenbezogenen Daten. Einer der Grundgedanken des Datenschutzrechts ist, daß der Betroffene, wenn er nicht selbst bewußt hierüber entschieden hat, von der dann auf gesetzlicher Grundlage stattfindenden Verarbeitung Kenntnis haben, jedenfalls aber die Möglichkeit hierzu erhalten muß.

Wird, obwohl grundsätzlich angeordnet, der Betroffene gar nicht informiert, hat er in der Regel keinerlei Chance, selbst um Rechtsschutz nachzusuchen; er muß auf die Hilfe der (internen oder externen) Datenschutzkontrolle vertrauen. Selbst der allgemeine Grundsatz, daß alles staatliche Handeln nachvollziehbar sein muß, verlangt in diesen Fällen eine ausreichende Dokumentation. Handelt es sich um einen besonderen Fall einer Mitteilung, für die keine das Justizmitteilungsgesetz konkretisierende ausdrückliche gesetzliche Grundlage vorhanden ist, sondern die unter Ausfüllung unbestimmter Rechtsbegriffe wie "Abwehr erheblicher Nachteile für das Gemeinwohl" auf

allgemeine Rechtsgrundlagen gestützt werden soll, bedarf es erst recht einer eingehenden Rechtfertigung, die zu dokumentieren ist.

Ich habe die Hoffnung, daß solche Vermerke aus datenschutzrechtlichen Gründen gefertigt werden, auch wenn untergesetzliche Verwaltungsvorschriften diese nicht ausdrücklich anordnen.

5.4 Fehlende bereichsspezifische Regelungen bei der Justiz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich zu Beginn einer neuen Legislaturperiode der Gesetzgebungsorgane des Bundes erneut veranlaßt gesehen, auf immer noch fehlende bereichsspezifische Regelungen in der Justiz hinzuweisen (Anlage 19.2).

Vor allem die fehlenden gesetzlichen Aufbewahrungsbestimmungen in Strafverfahren haben auch verschiedentlich in der Rechtsprechung dazu geführt, die Zulässigkeit von Datenspeicherungen zu verneinen. Zu Recht ist angesichts der seither vergangenen 15 Jahre in den Entscheidungen abgelehnt worden, man könne Speicherungen immer noch auf den sogenannten Übergangsbonus zum Volkszählungsurteil aus dem Jahre 1983 stützen.

Welche noch offenstehenden Fragen in der Strafprozeßordnung einer Lösung zugeführt werden müssen, war - auf der Grundlage eines früheren Gesetzentwurfs - Gegenstand einer weiteren Entschließung der Datenschutzbeauftragten (Anlage 19.1). Entwürfe zu einem (neuen) Strafverfahrensänderungsgesetz (1999) sollen den Justizverwaltungen durch die Bundesregierung bereits übersandt worden sein.

Dagegen hat der Bundesgesetzgeber gegen Ende der vergangenen Legislaturperiode mit dem Gesetz zum Schutz von Zeugen bei Vernehmungen im Strafverfahren und zur Verbesserung des Opferschutzes noch Vorschriften erlassen, die auch den Persönlichkeitsschutz verbessern sollen. Leider hat er hierbei nur einen Teil der Vorstellungen aufgegriffen, die die Datenschutzbeauftragten im Vorfeld dieser Entscheidung in einer Entschließung (TZ 19.8) formuliert hatten.

5.5 Datenschutz bei den Gerichten und Staatsanwaltschaften

Das Saarländische Datenschutzgesetz gilt nach § 2 Abs. 1 Satz 2 für Gerichte und Staatsanwaltschaft inhaltlich nur, "soweit sie Verwaltungsaufgaben wahrnehmen". Die Staatsanwaltschaften unterliegen darüber hinaus meiner Kontrollkompetenz, auch wenn sie keine Verwaltungsaufgaben wahrnehmen. Im Bund und den übrigen Ländern bestehen vergleichbare Regelungen.

Weil in anderen Ländern bei der Abgrenzung Unklarheiten aufgetaucht waren, haben die Datenschutzbeauftragten von Bund und Ländern in einer Ent-

schließung (Anlage 19.16) den tragenden Gesichtspunkt für die gesetzliche Regelung deutlicher herausgestellt.

Für die Kontrollkompetenz der Datenschutzbeauftragten des Bundes und der Länder bei den Gerichten wird die verfassungsmäßige Grenze durch die richterliche Unabhängigkeit gezogen, deren Respektierung eine rechtsstaatliche Selbstverständlichkeit ist.

Im Vorfeld dieser richterlichen Unabhängigkeit liegt indes die Beratungs- und Kontrollbedürftigkeit der Justizverwaltung, für die in § 2 Abs. 1 SDSG einfachgesetzlich die Kontrollkompetenz des Landesbeauftragten für Datenschutz festgelegt ist. In der Entschließung wird deshalb als ein Aspekt betont, daß sich die Kontrolle der Datenschutzbeauftragten bei den Gerichten insbesondere auch auf die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung, vor allem bei automatisierter Datenverarbeitung, erstrecke.

Daß in den Diensträumen der Justiz Datenschutz zu wahren ist, bedarf keiner Erwähnung; hierauf bezogene Vorkehrungen werden allgemein akzeptiert. Da Richter wegen ihrer Unabhängigkeit keinen festen Dienstzeiten unterliegen, sondern ihren Dienst auch im privaten Arbeitszimmer verrichten dürfen, ergeben sich aber vor allem dann datenschutzrechtliche Probleme, wenn sie hierbei private DV-Anlagen benutzen. Auch für Staatsanwälte dürfte der Einsatz solcher Systeme zur Erfüllung dienstlicher Aufgaben zwischenzeitlich keine Seltenheit mehr sein. Um so dringlicher ist es daher, das erforderliche Datenschutzbewußtsein für den gesamten Personenkreis, der personenbezogene Daten im häuslichen Bereich bearbeitet, zu schärfen.

Ebenso wie dies durch Dienstanweisung in verschiedenen Verwaltungsbereichen bereits geschehen ist, bietet sich hierfür eine entsprechende schriftliche Anweisung an. Inhaltlich sollten in ihr die Meldepflicht gegenüber dem Dienstherrn für solche privaten DV-Anlagen und angewandte Verfahren geregelt sein sowie die schriftlich festzulegende Bereitschaft, sich der Kontrolle durch den Landesbeauftragten für Datenschutz im Hinblick auf die auch im häuslichen Bereich zu treffenden Datensicherungsmaßnahmen zu unterwerfen.

Solche Hinweise können sich m. E. auch auf Richter erstrecken, deren rechtsprechende Tätigkeit und damit die richterliche Unabhängigkeit durch Darstellung des organisatorischen Umgangs mit Arbeitsunterlagen unter Berücksichtigung datenschutzrechtlicher Obliegenheiten nicht tangiert wird. Das Bundesdatenschutzgesetz (vgl. § 1 Abs. 2 Nr. 2 b) geht ebenfalls von der Geltung seines Anwendungsbereichs auf die Organe der Rechtspflege aus, auch wenn sie nicht in Verwaltungsangelegenheiten handeln.

Bei der anstehenden Anpassung des Saarländischen Datenschutzgesetzes an die EG-Datenschutzrichtlinie sollte die Gelegenheit genutzt werden, in der gesetzlichen Formulierung klarzustellen, daß ausschließlich der Bereich

richterlicher Unabhängigkeit nicht der Kontrolle des Landesbeauftragten für Datenschutz unterliegt.

5.6 Empfangsbekenntnis gem. § 212a ZPO in Postkartenform

Wie mir aus einer Anwaltskanzlei mitgeteilt wurde, verwenden die Amtsgerichte des Saarlandes Empfangsbekenntnisse gem. § 212a Zivilprozeßordnung (ZPO) als Vordrucke in Postkartenformat auch in Strafsachen. Auf der Postkarte ist der Name des Beschuldigten oder Angeklagten offen erkennbar.

Diese Praxis wurde mir durch das Ministerium der Justiz bestätigt, das die datenschutzrechtliche Unzulänglichkeit der Verfahrensweise durchaus erkannt hat. Deshalb hat es sich darum bemüht, im Rahmen der Installation des EDV-Systems SIJUS-Zivil zunächst probeweise dazu überzugehen, Empfangsbekenntnissen einen Rückumschlag beizufügen. Wenn Auswertungen zu diesem Versuch vorliegen, werde man auf die Angelegenheit zurückkommen.

Es wäre sehr zu begrüßen, wenn landesweit zumindest bei allen Strafgerichten eine datenschutzfreundliche Verfahrensweise eingeführt würde, die vor allem auch den eigenen Vorschriften der Justiz Rechnung trägt. So ist nach den bundeseinheitlichen Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) in Nr. 44 Abs. 1 ausdrücklich vorgegeben, den Beschuldigten durch Brief, nicht durch Postkarte, zu laden. Auch in diesem Zusammenhang ist eine unnötige Bloßstellung von Personen zu vermeiden (s.a. Nr. 23 RiStBV). Daß das Verfahren auch mit Kostensteigerungen für das Rückporto (derzeit 1,00 DM/1,10 DM) verbunden sein kann, darf angesichts der Sensitivität der Daten aus einem Strafverfahren nicht den Ausschlag für einen geringeren Datenschutz geben.

Dieser Gesichtspunkt sollte auch Eingang in das Gesetzgebungsverfahren zum Zustellungsreformgesetz finden, zu dem ein Referentenentwurf des Bundesministeriums der Justiz erarbeitet wurde.

Von der Justizverwaltung erwarte ich, daß sie neben der Umstellung des Verfahrens in der Praxis auch für entsprechende Bestimmungen in diesem Gesetz eintritt.

5.7 Pfändungs- und Überweisungsbeschluß gegen verschiedene Drittschuldner

Ein Petent, der dem Finanzamt Steuern schuldete und gegen den aus diesem Grund eine Pfändungs- und Überweisungsverfügung zur Einziehung von Forderungen des Petenten gegen seine (Dritt-)Schuldner erlassen wurde,

hat sich darüber beschwert, daß seinen Schuldnern angeblich auch die vom Petenten geschuldeten Steuerarten mitgeteilt wurden.

Eine Nachfrage ergab, daß die Anlagen zur Pfändungsverfügung gem. § 309 Abgabenordnung (AO) nur der Ausfertigung für den Schuldner, nicht aber den Ausfertigungen für die Drittschuldner beigefügt waren. In den Anlagen waren die Drittschuldner und die geschuldeten Steuerarten und Beträge im einzelnen aufgeführt.

Die Finanzbehörde hat mithin die Bestimmung des § 309 Abs. 2 AO beachtet, wonach die an den Drittschuldner zuzustellende Pfändungsverfügung den beizutreibenden Geldbetrag nur in einer Summe, ohne Angabe der Steuerarten und der Zeiträume, für die er geschuldet wird, bezeichnen soll. Desgleichen ist es Praxis der Finanzbehörden, an mehrere Drittschuldner jeweils getrennte Pfändungs- und Überweisungsverfügungen zu erlassen.

Auch im allgemeinen Vollstreckungsrecht (außerhalb der AO) hat der Gesetzgeber dem Gedanken, daß mehrere Drittschuldner nicht voneinander Kenntnis erhalten müssen, durch die 2. Zwangsvollstreckungsnovelle Rechnung getragen. § 829 Abs. 1 ZPO ist daher mit Wirkung vom 1.1.99 um folgenden Satz ergänzt worden:

"Die Pfändung mehrerer Geldforderungen gegen verschiedene Drittschuldner soll auf Antrag des Gläubigers durch einheitlichen Beschluß ausgesprochen werden, soweit dies für Zwecke der Vollstreckung geboten erscheint und kein Grund zu der Annahme besteht, daß schutzwürdige Interessen der Drittschuldner entgegenstehen."

Ein einheitlicher Beschluß, durch den die Drittschuldner voneinander Kenntnis erlangen, bedarf nunmehr eines eigenen Antrags des Gläubigers, wobei zusätzlich zu bewerten ist, ob schutzwürdige Drittschuldnerinteressen einem einheitlichen Antrag entgegenstehen.

Letzteres kann beispielsweise vor allem dann der Fall sein, wenn das Arztgeheimnis gegenüber mehreren Patienten als Drittschuldner eines Arztes gewahrt werden sollte. Wenn derart schutzwürdige Interessen der Drittschuldner entgegenstehen, darf das Vollstreckungsgericht dem Antrag auf Erlaß eines einheitlichen Pfändungs- und Überweisungsbeschlusses durch den Gläubiger nicht entsprechen.

5.8 Überwachung der Telekommunikation (TÜ); Beschlußausfertigung für den Telekommunikationsdienst

Die Anzahl der Telekommunikationsüberwachungen nach der StPO ist in den letzten Jahren ständig angestiegen. Dies belegen auch die dem LfD vorzulegenden Errichtungsanordnungen der Polizei.

Sowohl bei der Staatsanwaltschaft als auch beim Landeskriminalamt habe ich Kontrollen hinsichtlich der Durchführung von Überwachungsmaßnahmen vorgenommen. Diese dürfen die Freiheitsrechte der Betroffenen, von denen ja keineswegs feststeht, daß sie sich strafbar gemacht haben, und ihrer meist völlig unbeteiligten Gesprächspartner nur im unbedingt notwendigen Umfang beeinträchtigen. Dazu gehört auch, daß der Tatvorwurf Dritten nur bekannt wird, soweit dies für die Überwachung erforderlich ist.

Mit dem Ministerium der Justiz als Aufsichtsbehörde für die Staatsanwaltschaft wurde insbesondere ein Schriftwechsel darüber geführt, ob die Ausfertigung des richterlichen Überwachungsbeschlusses, die dem Telekommunikationsdienst zwecks Ermöglichung der Telekommunikationsüberwachung bekannt zu geben ist, auf den Namen, Anschrift, Rufnummer oder Kennung des Telekommunikationsanschlusses sowie Art, Umfang und Dauer der Maßnahme zu beschränken ist (§ 100 Abs. 2 StPO). Ich habe diese Beschränkung gefordert, weil ich festgestellt hatte, daß die Beschlußausfertigung vielfach die vollständige Begründung des Beschlusses enthalten hat und damit dem Telekommunikationsdienst Überschußinformationen über die Tat und den Verdächtigen geliefert hat, die er für seine technische Mitwirkung nicht benötigt.

Meinem Vorschlag, dem durch die Gestaltung des Beschlusses Rechnung zu tragen und hierauf bereits bei der Vorbereitung durch die Staatsanwaltschaft hinzuwirken, hat das Justizministerium entgegengehalten, hiermit werde in die richterliche Unabhängigkeit eingegriffen. Weder könnten von seiner Seite Hinweise auf den erforderlichen Datenumfang an die zuständigen Gerichte gerichtet werden, noch eine Hilfestellung durch die Staatsanwaltschaft mittels eines Vordrucks erfolgen, der eine Ausfertigung an den Telekommunikationsdienst nur mit beschränktem Datenumfang vorsehe.

Diese Auffassung vermag mich nicht zu überzeugen. Selbstverständlich ist bei dem gravierenden Eingriff, den die Telefonüberwachung darstellt, die Notwendigkeit hierzu und deren Bestätigung durch das Gericht eindeutig zu dokumentieren, und ebenso selbstverständlich ist, die Unabhängigkeit dieser gerichtlichen Entscheidung zu achten. Aber in die inhaltliche Entscheidung wird nicht eingegriffen, wenn sie durch formale Hilfen erleichtert wird. So enthält der von der Staatsanwaltschaft dem Gericht vorzulegende Vordruck für einen Haftbefehl ebenfalls Angaben, die dem Gericht die schnelle Überprüfung der gesetzlichen Haftvoraussetzungen erleichtern, ohne daß jemals der Gedanke aufgekommen wäre, die dort aufgeführten (hilfreichen, gesetzeskonformen) Hinweise zum Erlaß eines Haftbefehls würden die richterliche Unabhängigkeit beeinträchtigen.

Ich halte an meiner Auffassung fest, daß die Justizverwaltung in Kenntnis der insofern unrechtmäßigen Datenübermittlungen dafür Vorsorge treffen muß, daß nur die vom Telekommunikationsdienst benötigten Daten übermittelt werden.

Darüber hinaus wurden bei der Staatsanwaltschaft insbesondere Mängel bei der Benachrichtigung der Betroffenen sowie der Aufbewahrung und Vernichtung der TÜ-Unterlagen festgestellt. Diese Mängel veranlaßten den Leitenden Oberstaatsanwalt, seine Behörde eindringlich auf die Notwendigkeit hinzuweisen, die entsprechenden gesetzlichen Pflichten strikt zu beachten. Dagegen folgte man meiner Forderung, die Handhabung der TÜ-Maßnahmen im Bereich der Staatsanwaltschaft durch eine Verwaltungsvorschrift zu regeln, - trotz der zugegebenen Mängel - nicht; Justizministerium und Staatsanwaltschaft hielten die Ermahnung der Dezernentinnen und Dezernenten für ausreichend.

5.9 Mitteilung über Strafverfahren gegen Landtagsabgeordnete "auf dem Dienstweg"

Muß auch privates Verhalten von Landtagsabgeordneten strenger von der Exekutive beobachtet werden als das anderer Bürger? Wenn sich ein Strafverfahren gegen sie richtet, werden Parlamentarier nach dem Willen der Landesjustizverwaltungen des Bundes und der Länder schlechter behandelt als Beamte.

Für Beamte gilt nach der Anordnung über Mitteilungen in Strafsachen (Nr. 15, Nr. 10 Abs. 2 MiStra) ein direkter Mitteilungsweg vom Gericht oder der Staatsanwaltschaft an die personalverwaltende Stelle des Dienstherrn, damit diese beispielsweise über organisatorische oder disziplinarrechtliche Maßnahmen entscheiden kann. Weitere Empfänger dieser Mitteilung sind hier zum Schutz des Rechts auf informationelle Selbstbestimmung nicht vorgesehen. Dies entspricht dem im Datenschutzrecht grundlegenden Prinzip der Erforderlichkeit, wonach nur diejenigen mit personalbezogenen Daten umgehen dürfen, für deren Arbeit dies notwendig ist.

Nach Nr. 192 Abs. 5 der von den Justizverwaltungen erlassenen bundeseinheitlichen Richtlinien im Straf- und Bußgeldverfahren (RiStBV) soll die in § 8 EGStPO geregelte Endentscheidung im Strafverfahren gegen den Abgeordneten dem Landtagspräsidenten "auf dem Dienstweg" zugeleitet werden.

Hierfür gibt es meines Erachtens keine überzeugende Begründung. Ich bin der Auffassung, daß weder die Entscheidung über die Einleitung eines Verfahrens gegen einen Abgeordneten noch - erst recht - die Endentscheidung über den Ausgang des Verfahrens dem Landtagspräsidenten auf dem für die Exekutivgewalt geltenden Dienstweg zugeleitet werden sollte.

Die Mitteilung ist für den Landtag bedeutsam im Hinblick auf die Entscheidung, ob er die Immunität der Abgeordneten aufhebt. Diese Entscheidung ist - zur Sicherung der demokratischen Funktion des Parlaments - dem Landtag selbst vorbehalten; bei sogenannten Bagatellstraftaten trifft er sie für die jeweilige Legislaturperiode bereits vorab durch generelle Aufhebung der Im-

munität. Zumindest in all diesen Fällen hat das Ministerium lediglich die Funktion einer Durchlaufstation.

Das Strafverfahren hat ohne Ansehen der Person im Zusammenwirken der in der Strafprozeßordnung vorgesehenen Institutionen (Staatsanwaltschaft, Gericht) abzulaufen. Das Justizministerium hat in diesem Rahmen verfahrensrechtlich keinerlei Funktion, es hat insbesondere nicht das Recht, in das Verfahren selbst einzutreten.

Auch die zur Rechtfertigung angeführte Dienstaufsicht des Justizministeriums über die Staatsanwaltschaften vermag diesen Weg aus der Sicht des Datenschutzes nicht zu tragen. Der Verfahrensgang für Strafverfahren gegen Abgeordnete ist in Nr. 191 ff RiStBV festgelegt. Ich sehe keinen Anlaß, vom Weisungsrecht gegenüber der Staatsanwaltschaft von Seiten des Ministeriums Gebrauch zu machen; deshalb ist auch keine Kenntnisnahme erforderlich.

Abgesehen davon, daß unabhängige Richter in Strafverfahren letztlich über den Ausgang des Verfahrens zu entscheiden haben, findet das Weisungsrecht des Justizministeriums gegenüber der Staatsanwaltschaft seine gesetzlichen Grenzen in den Straftatbeständen der Verfolgung Unschuldiger (§ 344 StGB) oder der Strafvereitelung (§ 258a StGB).

Weitergehende Datenübermittlungen bedürfen im übrigen einer bereichspezifischen Rechtsgrundlage, die bislang weder in der Strafprozeßordnung noch in der Strafverfahrensbestimmung für Abgeordnete in § 8 EGStPO enthalten ist und für die es auch keine sachliche Rechtfertigung gibt. Bei der Einfügung des § 8 EGStPO durch das Justizmitteilungsgesetz hat der Dienstweg zu Recht keinen Eingang in diese gesetzliche Bestimmung gefunden.

Um die nicht gebotenen Eingriffe in Rechte der Abgeordneten aufzuheben, möchte ich dem Landesparlament einen Beschluß empfehlen, wonach der Landtagspräsident unmittelbar von der zuständigen Staatsanwaltschaft (bzw. Generalstaatsanwaltschaft) über ein Strafverfahren gegen Abgeordnete zu unterrichten ist.

5.10 Beschwerde an Berufskammern

In einer Reihe von sogenannten freien Berufen bestehen Kammern, die über die Erfüllung der Berufspflichten ihrer Kammermitglieder wachen. Macht jemand die Kammer auf unzulässige oder fehlerhafte Berufsausführung aufmerksam, kann er manchmal selbst Nachteile erleiden. Ein datenschutzgerechtes Verfahren muß dies ausschließen. Die Rechtsanwaltskammer hat mich aus Anlaß einer an sie gerichteten Beschwerde, die auch Gegenstand einer Eingabe an mich war, auf Rechtsprechung und Literatur zu den Risiken hingewiesen, die mit einer Anzeige verbunden sind.

Im konkreten Fall wurde das - nach Darstellung des Petenten - nicht korrekte Verhalten eines Rechtsanwaltes gerügt. Wenn man seinen Vortrag als wahr unterstellt, so kam die Rechtsanwaltskammer nach der Art der Vorwürfe nicht umhin, seine Sachverhaltsschilderung mit der Nennung seines Namens an den betroffenen Rechtsanwalt zur Stellungnahme weiterzuleiten. Dies führte als Reaktion des Rechtsanwaltes zur Schadenersatzklage wegen unwahrer Behauptungen gegen den Petenten.

Das Sonderopfer, als Zeuge in einem etwaigen anwaltsgerichtlichen Verfahren zur Verfügung zu stehen, kann dem Petenten zwar nicht grundsätzlich erspart bleiben.

Für einen zusätzlichen Zivilprozeß hat die Rechtsprechung jedoch ein Rechtsschutzinteresse verneint, so daß in solchen Fällen eine Abweisung der Klage wegen Unzulässigkeit erwartet werden darf. Dies gilt für alle Verwaltungsverfahren, Beschwerden und sonstige Eingaben wegen angeblicher Mißstände bei den für ihre Beseitigung zuständigen Stellen, da der Beschwerdeführer berechtigte Interessen wahrnimmt. Anders ist es nur, wenn über die sachliche Schilderung der Vorwürfe hinaus Anwürfe in beleidigender Form etc. erhoben werden.

Zu empfehlen ist allerdings, Schreiben, in denen Unkorrektheiten oder gar Straftaten/Ordnungswidrigkeiten moniert werden, direkt der zuständigen Stelle mit dem Vermerk "Persönlich und Verschlossen" zu übersenden, so daß der Sachverhalt nicht innerhalb einer Dienststelle verbreitet wird. Der konkrete Fall des Petenten gab jedoch zu diesem Hinweis keinen Anlaß.

Aus datenschutzrechtlicher Sicht sollte darüber hinaus von Seiten der angerufenen Beschwerdeinstanz geklärt werden, ob bei Nachfrage bei dem betroffenen Kammermitglied stets die Namensnennung des Beschwerdeführers erforderlich ist, oder ob dem Recht auf informationelle Selbstbestimmung des Beschwerdeführers gegenüber den Beschuldigtenrechten Vorrang eingeräumt werden kann.

6 Kommunen

6.1 Einrichtung eines Bürgerbüros bei den Gemeinden

In den letzten Jahren haben zur bürgernahen und optimierten Abwicklung von Dienstleistungen immer mehr Städte und Gemeinden sogenannte Bürgerbüros eingerichtet. Das Konzept dieser Einrichtungen besteht darin, dem Bürger eine einheitliche Anlaufstelle für die verschiedensten Anliegen anzubieten, ihn also nicht mehr von einem Amt zum anderen zu schicken. Gleichzeitig soll dadurch der Publikumsverkehr in den Fachabteilungen verringert und ein Rückbesinnen dieser Ämter auf ihre eigentliche Arbeit gefördert werden.

Die Aufgaben der Bürgerbüros sind im Regelfall nicht abschließend definiert. Sie können über die Bereitstellung von Formularen, zentrale Anlaufstelle und Vermittlung bei Anfragen hinaus auch die Nutzung der unterschiedlichen IT-Verfahren und Datenbestände (z.B. Meldewesen, Steuerwesen, Abfallbeseitigung, Friedhofswesen, Verbrauchsabrechnung) sowie die Befugnis der rechtlichen Beratung, Entgegennahme und Vorprüfung von Anträgen der verschiedensten Zuständigkeitsbereiche umfassen.

Der Gedanke, daß sich die Verwaltung mehr und mehr als Dienstleister für den Bürger vorstellt, ist grundsätzlich zu begrüßen. Auch unter dem Blickwinkel des Persönlichkeitsschutzes könnte vordergründig sogar als vorteilhaft gelten, daß der Bürger mit Zusammenfassung verschiedener Aufgaben bei nur einer Stelle eben nur dieser Einblick in seine Lebensverhältnisse geben muß und nicht einer größeren Anzahl.

Gerade diese Zusammenschau verschiedener Bereiche, die der Betroffene vielfach auch unterschiedlich behandelt wissen will, führt aber umgekehrt zu einer potentiellen Beeinträchtigung seiner Sphäre, kann ihm die nötige Unbefangenheit bei seinen Entscheidungen nehmen. Die Möglichkeit hierzu darf es nicht unbegrenzt geben; aus diesem Grunde wurde für das Datenschutzrecht das Prinzip der informationellen Gewaltenteilung entwickelt, das auch innerhalb der Gemeindeverwaltung gilt. Zwar gehört die Organisationshoheit der Gemeinden zum Kernbereich des Selbstverwaltungsrechts. Ihrer Gestaltungsfreiheit sind jedoch, wie das Bundesverfassungsgericht hervorgehoben hat, Grenzen gesetzt. Aus der Einheit der Gemeindeverwaltung folgt keine informationelle Einheit (Beschluß des BVerfG vom 18.12.1987. NJW 1988, S. 959).

Das Recht auf informationelle Selbstbestimmung ist bei jeder Verwaltungstätigkeit zu beachten und gilt selbstverständlich auch bei einer Zusammenfassung der verschiedenen Aufgaben hinsichtlich Organisation und Geschäftsverteilung. Das Streben nach Wirtschaftlichkeit, Effizienz und Bürgernähe der Verwaltung genießt dieser Verpflichtung gegenüber keinen Vorrang.

Zu beachten ist auch, daß personenbezogene Daten grundsätzlich nur für die gesetzlich bestimmten Zwecke genutzt werden dürfen. Die Verwendung zu einem anderen Zweck unterliegt bestimmten Zulässigkeitsvoraussetzungen. Zur Sicherung dieser Zweckbindung gilt im Datenschutzrecht der sogenannte funktionelle Behördenbegriff (§ 14 Abs. 5 SDSG).

Dieser Grundsatz fachbezogener Aufgabenverteilung innerhalb einer Kommune wird durch Einrichtung von Bürgerbüros tangiert.

Zum einen muß hierbei ausgeschlossen bleiben, daß generell unverträgliche Aufgabenbereiche zusammengefaßt werden. Ein dennoch auftretender Widerspruch läßt sich nur durch eine strikte Beachtung des Verwertungsverbotes für die dem Bürgerberater bekannt gewordenen Daten lösen: Vor jeder Nutzung personenbezogener Daten zu anderen Zwecken ist vom Mitarbeiter des Bürgerbüros zu prüfen, ob dafür die gesetzlichen Voraussetzungen vor-

liegen (z.B. § 13 Abs. 2 SDSG); ansonsten darf - außer bei Vorliegen einer Einwilligung des Betroffenen - die Information nicht verwertet werden.

Generelle Aussagen über die zulässige Aufgabenbündelung beim Bürgerbüro sind nicht möglich, da die Vielzahl der denkbaren Gestaltungsmöglichkeiten zu groß ist.

Auf jeden Fall kommt es auf die Art der Daten und die Gefahr von Interessenkollisionen an. Aufgaben, die einem Berufs- oder Amtsgeheimnis wie z.B. dem Steuer- oder Sozialgeheimnis unterliegen, dürfen wegen des bestehenden Interessenkonfliktes jedenfalls nicht von einem Mitarbeiter des Bürgerbüros wahrgenommen werden, der noch andere Aufgaben hat. Sollen solche Aufgaben im Bürgerbüro dennoch erledigt werden, muß eine personelle und gegebenenfalls räumliche Trennung der verschiedenen Aufgabenbereiche innerhalb des Bürgerbüros jeden Konflikt ausschließen.

Dem Betroffenen muß auch das Recht verbleiben, selbst zu entscheiden, ob er sich mit seinem Anliegen an das Bürgerbüro oder direkt an das zuständige Fachamt wenden will. Auf diese Wahlmöglichkeit ist er bei Beginn der Beratung hinzuweisen.

Von Bedeutung für den vielfach vorgesehenen Online-Anschluß innerhalb der Kommune ist ebenso, ob dem Bürgerbüro lediglich Hilfsfunktionen oder auch Exekutivbefugnisse übertragen werden:

- Bei Befugnis des Büros zur sachlichen Bearbeitung des Anliegens, wie dies für das Meldewesen meist der Fall sein dürfte, ist ihm als originär zuständiger Stelle auch Zugriff auf die entsprechenden EDV-Verfahren einzuräumen. Eine erforderliche Trennung bei "nicht harmonierenden" Aufgaben innerhalb des Bürgerbüros ist hierbei zu beachten.
- Verbleibt allein dem Fachamt die Entscheidungsbefugnis und steht dem Bürgerbüro nur eine allgemeine Beratungsfunktion oder die Aufgabe zu, Anträge entgegenzunehmen und allenfalls eine formale Vollständigkeitsprüfung vorzunehmen, bedarf es hierfür keines Zugriffs auf bereits vorhandene personenbezogene Daten; ein Online-Anschluß kommt nicht in Betracht.
- Wird - ohne eigentliche Sachbearbeitung - dem Bürgerbüro die Möglichkeit eingeräumt, Hilfe beim Erstellen von Anträgen (etwa durch Einfügen der Adreßdaten) zu leisten und diese über äußerliche Merkmale hinaus auf inhaltliche Plausibilität zu prüfen, ist der technische Zugang zu den hierfür erforderlichen Daten zulässig. Für den eigentlichen Zugriff auf die Daten ist jedoch das Einverständnis des Betroffenen zu fordern, das die Weitergabe rechtfertigt. Dies setzt voraus, daß der Bürger schon vor Abruf weiß, welche Daten das Bürgerbüro abrufen kann, um dann entscheiden zu können, ob er nicht doch eine Bearbeitung durch das zuständige Fachamt vorzieht.

Selbstverständlich sind exakte technisch-organisatorische Schutzmaßnahmen für die EDV-Anwendungen zu fordern.

Ebenso selbstverständlich muß auch die räumliche Gestaltung datenschutzrechtlichen Anforderungen entsprechen. Probleme ergeben sich insbesondere bei der Nutzung von Großraumbüros. Hier besteht die Gefahr, daß Gespräche mitgehört, Bildschirme eingesehen werden und Akten und Anträge für andere Besucher einsehbar auf Beratungstischen liegen. Dadurch würde die Kenntnisnahme durch Dritte und somit das unbefugte Offenbaren personenbezogener Daten in unzulässiger Weise gefördert. Es ist Aufgabe der Gemeinde, dies durch eine entsprechende räumliche Gestaltung zu verhindern.

So ist darauf zu achten, daß Beratungstische weit genug auseinander stehen und Wartezonen nicht bis dicht an die Beratungstische heranreichen, was z.B. durch Wartelinien mit entsprechenden Hinweisschildern gelöst werden kann. Der Sicht- und Mithörschutz läßt sich z.B. durch Trennwände, Pflanzen und Hintergrundmusik merklich verbessern, ebenso wie sich die Sicht Unbefugter auf Bildschirme durch - aktivierte - Bildschirmschoner (mit Paßwortschutz!) vermeiden läßt.

Beratungsgespräche mit sensiblem Inhalt (z.B. bei Steuer-, Sozial-, Gesundheitsdaten) sollten grundsätzlich nicht in einem Großraumbüro stattfinden. Insoweit ist baulich vorzusehen und der Bürger ist in geeigneter Weise darauf hinzuweisen, daß er die Möglichkeit hat, sein Anliegen dem Mitarbeiter auch ungestört vorzutragen.

Welche auch öffentliche Resonanz die Nichtbeachtung solch elementarer Datenschutzmaßnahmen zur Folge hat, zeigt ein Artikel der Saarbrücker Zeitung vom 4.11.1998 mit der Überschrift "Der Nachbar kann immer mithören". Meine Überprüfung bestätigte die darin geschilderten Mißstände bei der Einrichtung eines Bürgeramtes in einem gerade neu errichteten Gebäude. Ich mußte eine datenschutzgerechte Nachbesserung verlangen, die nachträglich mit Sicherheit schwerer und nur durch den Einsatz von zusätzlichen Mitteln erreichbar ist. Besser würden durch sorgfältige Planung solche Fehler von vornherein vermieden.

Werden Aufgaben eines Bürgerbüros nicht in einer speziell hierfür bestimmten Einrichtung wahrgenommen, sondern von Mitarbeitern in wechselnden Anlaufstellen beispielsweise im jeweiligen Ortsteil einer Gemeinde, müssen die räumlichen Bedingungen natürlich auch hier "stimmen". Wenn der Anschluß an das EDV-Netz der Gemeinde über mobile Datenverarbeitungsgeräte und das Telefonnetz erfolgt, ist selbstverständlich, daß der Datenverkehr nur geschützt erfolgen darf.

Auch ohne jegliche Einrichtung wird teilweise daran gedacht, Bürgerbüroähnliche Dienstleistungen auch über das Internet bereitzustellen. Solange dabei keine personenbezogenen Daten übermittelt werden, die Angebote

etwa das Bereitstellen von Formularen oder Infoblättern nicht überschreiten, ist dagegen aus Datenschutz-Sicht nichts einzuwenden. Für den Datenverkehr im Internet bestehen jedoch die bekannten Risiken, auf die ich an anderer Stelle hingewiesen habe (TZ 3.4) Keinesfalls darf die Gemeinde die Bürger veranlassen, diese Risiken ohne gebührende Kenntnis einzugehen; sie müssen ohne Nachteile auf eine Übermittlung personenbezogener Daten auf diesem Weg verzichten können.

Die Verfahrensgestaltung sollte so ausgelegt sein, daß gängige Sicherungstechniken (z. B. Verschlüsselung, SSL-Übertragung, elektronische Unterschrift) so weit wie möglich unterstützt werden. Auf die entsprechende Orientierungshilfe "Internet", die gerade vom Arbeitskreis "Technik" der Datenschutzbeauftragten des Bundes und der Länder überarbeitet worden und in mein Internet-Angebot eingestellt ist, möchte ich verweisen.

6.2 Behandlung personenbezogener Daten durch den Gemeinderat

Dem Gemeinderat obliegen als Organ Aufgaben, die den Umgang mit den Daten einzelner Personen bedingen, beispielsweise im Personalbereich, bei Eingaben oder in Bau- und Vertragsangelegenheiten. Nicht immer läßt sich bei Verarbeitung und Durchführung der Sitzungen vermeiden, daß die konkrete Person erkennbar wird. Selbstverständlich hat die Arbeit des Gemeinderates dem Datenschutz Rechnung zu tragen, auch übrigens, soweit sie Daten der Gemeinderatsmitglieder selbst betrifft. Ein Beispielsfall, mit dem ich mich befassen mußte, betraf die Erörterung in einem Gremium, zu dem nach einer "Koalitionsvereinbarung" der örtlichen Parteien nicht nur Ratsmitglieder gehörten.

Die einzelnen Gemeinderatsmitglieder unterliegen grundsätzlich der Verschwiegenheitspflicht für solche Daten, die ihnen in ihrer Eigenschaft als Funktionsträger bekannt werden (§ 33 Abs. 2 KSVG). Für die Übermittlung personenbezogener Daten enthält das KSVG keine bereichsspezifischen Sondervorschriften, so daß insoweit das SDSG zur Anwendung kommt. Die Datenübermittlung an private Dritte, zu denen auch politische Parteien zählen, ist nur in eng begrenzten Ausnahmefällen zulässig (§ 16 SDSG), zumal die Verwendung der Daten an den Zweck - Aufgabenerfüllung der Gemeinde - gebunden ist.

Dem grundsätzlichen Ausschluß einer Datenübermittlung an Nicht-Ratsmitglieder kann auch nicht entgegen gehalten werden, daß eine Koalitionsvereinbarung zwischen politischen Parteien die Mitwirkung vorsieht. Derartige Vereinbarungen ersetzen nicht die erforderliche gesetzliche Ermächtigung.

Bei meinen Prüfungen habe ich auch zur Behandlung personenbezogener Daten im Zusammenhang mit Gemeinderatssitzungen Stellung bezogen.

So sollte bereits bei Aufstellung der Tagesordnung unter Beachtung des Konkretisierungsgebots der Personenbezug möglichst vermieden werden. Personenbezogene Sitzungsunterlagen sollten nur in verschlossenem Umschlag an die Ratsmitglieder übersandt werden. Die Löschung von Daten ist zwingend vorgeschrieben, wenn diese für die Aufgabenerfüllung des Gemeinderates nicht mehr benötigt werden. Eine empfehlenswerte Datenschutzvorsorge stellt das Angebot der Verwaltung dar, Vorlagen mit sensitiven personenbezogenen Daten nach der Sitzung einzusammeln und zu vernichten. Die Verantwortung für die Einhaltung des Datenschutzes durch jedes Ratsmitglied entfällt dadurch jedoch nicht.

Desweiteren sollte bei Veröffentlichung von Sitzungseinladungen und -niederschrif-ten ein Personenbezug nach Möglichkeit ganz vermieden werden. Werden - wie die Praxis zeigt - Niederschriften im Gemeindeblatt veröffentlicht, so ist das ohnehin nur für den Teil der öffentlichen Sitzung möglich. Nur in seltenen Ausnahmefällen dürfte dabei überhaupt ein Personenbezug erforderlich sein. Verstoßen einzelne Mitglieder in den Redebeiträgen gegen datenschutzrechtliche Bestimmungen, darf die veröffentlichte Niederschrift diesen Verstoß nicht fortsetzen.

In Gemeinden werden auch Überlegungen angestellt, Sitzungsniederschriften den Ratsmitgliedern auf elektronischen Datenträgern zur Verfügung zu stellen. Dadurch würden jedoch die Gefahren, daß Daten unbefugt offenbart werden, erheblich steigen. Ihnen müßte durch erhöhte technisch-organisatorische Datensicherungsmaßnahmen begegnet werden, zumal dann, wenn sie die vertraulichen Daten der nichtöffentlichen Sitzung umfassen. Da die Datenträger den Verwaltungsbereich verlassen, ist jedoch nicht sichergestellt, daß der Persönlichkeitsschutz durch diese Maßnahmen gewährleistet wird. Auch ich könnte dies wegen des Schutzes der Wohnung nach Art. 13 Grundgesetz nur im Einvernehmen mit dem einzelnen Ratsmitglied überprüfen. Wegen der mit automatisierter Datenverarbeitung stets verbundenen Zusatzrisiken für den Datenschutz habe ich deshalb empfohlen, von der Weitergabe der Niederschriften in elektronischer Form abzusehen.

6.3 Geschwindigkeitsüberwachung in den Kommunen

Immer häufiger überwachen die Gemeinden selbst, daß Verkehrsteilnehmer die zulässige Geschwindigkeit in verkehrsberuhigten Bereichen und innerörtlichen Zonen mit einer Höchstgeschwindigkeit von 30 km/h einhalten. Zur Überwachung wird ein speziell dafür zugelassenes Videoverfahren eingesetzt, das durch besonders geschulte Hilfspolizeibeamte bedient wird. Datenschutzrechtliche Probleme ergeben sich dadurch, daß hierbei nicht nur Verkehrssünder, sondern auch die Daten einer Vielzahl Unverdächtiger auf-

genommen werden. Erst recht ist problematisch, den Verkehr über längere Zeit in einer Sequenz aufzuzeichnen, die ausschließlich Unverdächtige zeigt.

Ich habe gefordert, daß nur dann Aufnahmen gefertigt werden, wenn ein ausreichender Anfangsverdacht für einen Verkehrsverstoß vorliegt. Zudem müssen technisch-organisatorische Maßnahmen getroffen werden, durch die die Kenntnisnahme von Verkehrsteilnehmern, bei denen sich der Anfangsverdacht durch die Messung nicht bestätigt hat, weitestgehend ausgeschlossen ist.

Das Ministerium des Innern hat meinen Forderungen zwischenzeitlich dadurch Rechnung getragen, daß der Einsatz in den Gemeinden nur dann zugelassen wird, wenn

- eigens geschultes Personal zur Verfügung steht,
- ein Anfangsverdacht für einen Verkehrsverstoß vorliegt und
- die Auswertung für alle am Verfahren beteiligten Stellen (Polizei, Staatsanwaltschaft, Verteidiger, Gericht) nach Möglichkeit über eine besondere Vorführanlage des Herstellers erfolgt.

Als Rechtsgrundlage für das Anfertigen der Lichtbildaufnahmen von Verkehrssündern wird § 100c Abs. 1 Nr. 1a StPO herangezogen. Diese Vorschrift wurde durch das Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG) in die StPO eingefügt. Auch wenn man - trotz dieser Entstehungsgeschichte - der Auffassung folgt, die Vorschrift erlaube die Anfertigung von Lichtbildern bei allen Ermittlungen (nicht nur bei Straftaten, sondern auch Ordnungswidrigkeiten), kann die Schwere des Verstoßes nicht außer Betracht bleiben.

Das Fertigen von Lichtbildern bei Geschwindigkeitsüberschreitungen muß ausscheiden, wenn diese von ihrer Gewichtung nicht vergleichbar sind mit Verkehrsverstößen, die mindestens mit einem Bußgeld geahndet werden. So kann die Geschwindigkeit so gering überschritten sein, daß dies nur zu einer Verwarnung führt. Da jedoch bei Geschwindigkeitsmessungen die Schwere der Tat nicht von vornherein bestimmbar ist, habe ich meine datenschutzrechtlichen Bedenken insoweit zurückgestellt.

Dagegen sehe ich im Bereich des ruhenden Verkehrs das Anfertigen von Lichtbildern bei minderschweren Verkehrsverstößen als unangemessen an; § 100c erlaubt meines Erachtens nach der gesetzgeberischen Wertung eine derartige Erhebung nicht.

6.4 Einsatz von Parkkrallen

Berichte in der Saarbrücker Zeitung wie "Falschparker werden gekrallt", "Stadt jagt jährlich den Millionen nach" und "Kralle bringt Geld in Kasse" veranlaßten mich, die Rechtmäßigkeit des Einsatzes von Parkkrallen bei den Gemeinden, die die Parkkralle bereits einsetzen oder dies beabsichtigen, zu überprüfen.

Dabei stellte sich schnell heraus, daß es gar nicht darum ging, die Parkkralle zur Verfolgung von Ordnungswidrigkeiten einzusetzen. Die Gemeinde selbst sah hierin keine geeignete Modalität einer polizeirechtlichen Sicherstellung oder des Verwaltungszwanges in Form der Ersatzvornahme.

Sie sollte vielmehr im Rahmen der Verwaltungsvollstreckung bei der Beitreibung rückständiger Abgaben und sonstiger Forderungen zum Einsatz kommen. Die Voraussetzungen hierfür richten sich nach dem Verwaltungsvollsteckungsgesetz. Dabei ist das Verfahren so zu gestalten, daß für den Schuldner keine unverhältnismäßige Bloßstellung eintritt.

Ein längeres Stehenlassen des "gekrallten" Fahrzeuges im öffentlichen Verkehrsraum stellt ein über das erforderliche Maß hinausgehendes Anprangern des Schuldners als eines säumigen Zahlers dar, das seine Persönlichkeitsrechte in vermeidbarer Weise einschränkt. Solche Wirkungen muß man dadurch vermeiden, daß das Fahrzeug nach der Pfändung unverzüglich aus dem öffentlichen Verkehrsraum entfernt wird, es sei denn, der Schuldner ist mit dem Verbleib an dieser Stelle einverstanden. Das Anbringen der Parkkralle darf frühestens mit der Pfändung des Fahrzeuges erfolgen; eine vorherige Sicherung des Fahrzeuges durch das Anlegen einer Parkkralle bis zu eigentlichen Pfändung halte ich für nicht zulässig, denn dies führt zu einer vermeidbar langen und damit nicht erforderlichen Bloßstellung des Schuldners.

Wenn die vollstreckungsrechtlichen Voraussetzungen unter Wahrung der dargelegten datenschutzrechtlichen Gesichtspunkte eingehalten werden, bestehen gegen den Einsatz der Pfandkralle keine grundsätzlichen Bedenken.

6.5 Fehlerhafte Speicherung von Wahlrechtsausschlüssen

Nach Prüfung mehrerer Meldebehörden mußte ich feststellen, daß Mitteilungen der Staatsanwaltschaft zum Wahlrechtsausschluß nach Nr. 12 der (bundeseinheitlichen) Anordnung über Mitteilungen in Strafsachen (MiStra) vielfach zu fehlerhaften Speicherungen bei den Meldebehörden führten.

Der Wahlrechtsausschluß kann sich auf das aktive und/oder das passive Wahlrecht erstrecken. Je nach Inhalt der Mitteilung der Staatsanwaltschaft - so die Erläuterung des Leitenden Oberstaatsanwaltes - kann die Meldebehörde erkennen, ob der Betroffene, der rechtskräftig verurteilt wurde, vom

aktiven und/oder passiven Wahlrecht ausgeschlossen ist. Teilt die Staatsanwaltschaft lediglich die Tatsache der rechtskräftigen Verurteilung wegen eines Verbrechens mit, bei der auf Freiheitsstrafe von mindestens einem Jahr erkannt worden ist, so ist - kraft Gesetzes - nur das passive Wahlrecht auf 5 Jahre ausgeschlossen (§ 45 Abs. 1 StGB). Wird hingegen die Aberkennung durch Richterspruch einschließlich der Zeit, für die die Aberkennung wirksam ist, mitgeteilt, so ist das aktive und/oder das passive Wahlrecht ausgeschlossen (§ 45 Abs. 2 und 5 StGB).

Diese Differenzierung war den Meldebehörden, die fehlerhaft gespeichert hatten, gar nicht bekannt. Es kam daher in Fällen des Ausschlusses vom passiven Wahlrecht zur Streichung aus dem Wählerverzeichnis, so daß auch das aktive Wahlrecht nicht ausgeübt werden konnte. Ich habe deshalb begrüßt, daß das Innenministerium auf meinen Hinweis durch entsprechenden Erlaß eine sofortige Aufklärung der Meldebehörden veranlaßt hat.

Nicht einfach ist allerdings, den Endzeitpunkt der zu berechnenden Frist zu ermitteln. Die Meldebehörden selbst verfügen nicht über die Kenntnis von Tatsachen, die den Fristablauf beeinflussen (z.B. Verbüßung, Verjährung, Erlaß der Freiheitsstrafe, § 45a Abs. 2 StGB).

Das Ministerium der Justiz, das sich auf meine Bitte mit dieser Frage befaßt hat, hat hierzu vorgeschlagen, daß die Meldebehörden im Einzelfall ein Führungszeugnis nach dem Bundeszentralregistergesetz (§ 31 BZRG) einholen. Der Tag des Ablaufs des Verlustes der Amtsfähigkeit, der Wählbarkeit und des Wahl- und Stimmrechts ist nämlich zum Bundeszentralregister zu melden und findet Eingang in das Führungszeugnis (§§ 31, 32, 12 Abs. 1 Nr. 7 BZRG), das darüber hinaus allerdings eine Vielzahl weiterer Informationen enthält; dieses Zeugnis können die Gemeinden anfordern, wenn sie es für ihre Aufgaben benötigen.

Ich habe demgegenüber die Auffassung vertreten, daß auch an die Meldebehörden nach dem Justizmitteilungsgesetz und der MiStra (§ 20 EGGVG, Nr. 7 MiStra) eine Folgemitteilung zu richten sei, die m.E. unmittelbar vor bevorstehenden Wahlen eine zeitnähere Beurteilung der Rechte Betroffener erlaubt. Vom Ministerium des Innern wurde den Meldebehörden in dem entsprechenden Erlaß ebenfalls empfohlen, sich in Zweifelsfällen an die einmeldende Stelle (also die Staatsanwaltschaft) zu wenden.

Die Mitteilung seitens der Staatsanwaltschaft (sei es als Spontanmitteilung durch die Staatsanwaltschaft oder auf Ersuchen der Meldebehörde im Einzelfall) halte ich für den einzig datenschutzgerechten Weg, die Richtigkeit der Daten im Wählerverzeichnis zu gewährleisten. Zwar ist der Tag des Ablaufs des Verlustes der Amtsfähigkeit, der Wählbarkeit und des Wahl- und Stimmrechts auch im Bundeszentralregister einzutragen (§ 12 Abs. 1 Nr. 7 BZRG), sobald er unter Berücksichtigung aller Einflußfaktoren exakt berechnet werden kann. Solange die Meldebehörden jedoch nicht nur dieses Einzeldatum erfragen können, sondern dies nur im Rahmen eines Führungs-

zeugnisses für die Behörden mitgeteilt bekommen, erhalten sie damit eine Fülle von Überschußinformationen zu allen Vorstrafen des Betroffenen, die für die konkrete Überprüfung des Wahlrechtsausschlusses nicht erforderlich sind.

Demgegenüber ist die Mitteilung zum Wählerverzeichnis nach der MiStra ausdrücklich auf die Tatsache der rechtskräftigen Verurteilung (ohne Angabe der rechtlichen Bezeichnung der Tat und ohne Angabe der angewendeten Strafvorschriften) in einem Einzelfall beschränkt. Es bedeutete eine Umgehung dieser - datenschutzgerechten - Beschränkung, wenn die Meldebehörde zur Überprüfung des Wahlrechtsausschlusses gezwungen wäre, ein Führungszeugnis anzufordern.

Die Erörterung der Problematik war bei Redaktionsschluß noch nicht abgeschlossen.

6.6 Nachweis des Wohnungseigentums bei der melderechtlichen Anmeldung

Bei der Anmeldung in einer Gemeinde verlangte das Meldeamt von einem Bürger, der selbst Eigentümer der Wohnung war, als "Nachweis durch den Wohnungsgeber" die Vorlage des Kaufvertrages.

Durch die Vorlage des Kaufvertrages erhält die Meldebehörde eine Fülle von personenbezogenen Daten, die jedenfalls nicht nötig sind, um das Melderegister richtig zu führen. Nur die zur ordnungsgemäßen Führung des Melderegisters erforderlichen Auskünfte und die zum Nachweis erforderlichen Unterlagen braucht aber der Anmeldende vorzulegen. Ohnehin besteht für den Wohnungsgeber nur eine Mitwirkungspflicht, die An- oder Abmeldung eines Mieters zu bestätigen. Ist der Wohnungsgeber mit dem Meldepflichtigen identisch, entfällt diese Verpflichtung. Die Vorlage eines Kaufvertrages mit einer Reihe sensibler Daten fällt jedenfalls im Regelfall nicht darunter.

Lediglich bei Vorliegen berechtigter Zweifel an der Eigentümereigenschaft kann die Vorlage eines Nachweises gefordert werden; auch dieser muß jedoch nur solche Daten enthalten, die zur Aufgabenerfüllung der Meldebehörde erforderlich sind. Das Verlangen nach Vorlage des gesamten Kaufvertrages verstößt deshalb gegen das Übermaßverbot.

Das Ministerium des Innern hat diese Auffassung ausdrücklich bestätigt.

6.7 Regelmäßige Unterrichtung der GEMA durch die Gemeinden

Der Saarländische Städte- und Gemeindetag hat mich um Stellungnahme zu der Frage gebeten, ob der Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte (GEMA) beim Abschluß von Miet- oder

Pachtverträgen über kommunale Räumlichkeiten Kopien aller Verträge zugeleitet werden dürfen. Dadurch wolle die GEMA ihre Ermittlungstätigkeit erleichtern und den Gemeinden mühevolle Recherchen ersparen, wenn durch die Vielzahl der von der GEMA ermittelten Veranstaltungen teilweise noch bis zu einem Jahr zurückliegende Veranstaltungen bei den Gemeinden abgefragt werden müssen.

Ich habe die Zulässigkeit der regelmäßigen Übermittlung von Daten aus den Verträgen und erst recht der Übersendung von Kopien der Verträge verneint. Nach § 13a Urheberrechtswahrnehmungsgesetz hat der Veranstalter von öffentlichen Wiedergaben urheberrechtlich geschützter Werke die Pflicht, der Verwertungsgesellschaft (GEMA) eine Aufstellung über die bei der Veranstaltung benutzten Werke zu übersenden.

Der Gemeinde als bloßer Vermieterin gemeindeeigener Räume obliegt eine solche Offenbarungspflicht nicht.

Sofern der Veranstalter nicht seine Einwilligung zur Übermittlung des gesamten Vertrages über die Nutzung gemeindeeigener Räume erteilt hat, fehlt dieser Datenübermittlung sowohl vom Umfang als auch vom Inhalt des Vertrages her die Rechtsgrundlage. Wenn alle Verträge über die Nutzung gemeindeeigener Räume übermittelt werden, erhält die Verwertungsgesellschaft auch Kenntnis von Verträgen über Veranstaltungen, die urheberrechtlich gar nicht von Belang sind. Darüber hinaus enthalten einschlägige Verträge Klauseln, deren Bekanntgabe zur Beurteilung der urheberrechtlichen Folgen der Veranstaltung nicht erforderlich ist.

Da die Gemeinde in ihrem fiskalischen Handeln als Vermieterin gemeindeeigener Räume gem. § 2 Abs. 2 SDSG als öffentlich-rechtliches Wettbewerbsunternehmen anzusehen ist, das gem. § 28 BDSG Daten wie eine private Stelle übermitteln darf, könnte allenfalls im Einzelfall auf Ersuchen eine Datenübermittlung nach § 28 Abs. 1 Nr. 1a BDSG im jeweils notwendigen Umfang in Betracht kommen. Die Bestimmung setzt voraus, daß die Übermittlung zur Wahrung berechtigter Interessen eines Dritten (GEMA) erforderlich ist und kein Grund zu der Annahme besteht, daß der Betroffene (Veranstalter) schutzwürdige Interessen an dem Ausschluß der Übermittlung hat.

Ich gehe davon aus, daß die saarländischen Gemeinden aus den dargestellten Gründen von einer regelmäßigen Datenübermittlung an die GEMA absehen.

6.8 Überprüfungen bei den Gemeinden

Die Querschnittsprüfungen, die ich im Berichtszeitraum bei mehreren Gemeinden in verschiedenen Landkreisen vorgenommen habe, zeigten nicht nur bei der automatisierten Datenverarbeitung unzureichende Verhältnisse

(vgl. TZ 3.6). Auch im konventionellen Bereich fand ich bei mehreren geprüften Gemeinden insbesondere die folgenden Mängel vor:

6.8.1 Aktenaufbewahrung und Vernichtung

Akten und sonstige Unterlagen, wie z.B. Führerschein-, Bußgeld-, Verwarngeldakten, Meldeunterlagen, Gewerbeunterlagen, die zur Aufgabenerfüllung nicht mehr erforderlich waren, wurden nicht rechtzeitig vernichtet.

Sofern keine spezialgesetzliche Regelung im Einzelfall besteht, findet § 19 SDSG unmittelbar Anwendung. Danach sind personenbezogene Daten von Amts wegen zu löschen, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die speichernde Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist. Diese gesetzliche Verpflichtung kann nicht durch den Hinweis auf fehlende Personalkapazitäten unerfüllt bleiben. Der Bürger hat Anspruch darauf, daß öffentliche Stellen nur die personenbezogenen Daten über seine Person vorhalten, die zur Erfüllung öffentlicher Aufgaben (noch) erforderlich sind.

6.8.2 Führerscheinkarteien

Dieser Grundsatz gilt auch für den Umfang der in Dateien oder Akten gespeicherten personenbezogenen Daten von Führerscheininhabern. So habe ich festgestellt, daß in den Führerscheinkarteien/-dateien Daten über nicht mehr relevante Führerscheinentziehungen enthalten waren, obwohl der Führerschein zwischenzeitlich wieder erteilt wurde. Diese Problematik war bereits Gegenstand meines 3. und 9. TB für die Jahre 1981 und 1987 (TZ 3.2 / TZ 9.2). Nach Einführung des Verkehrszentralregisters dürfen Verkehrsdelikte nicht mehr in örtlichen Listen und Karteien geführt werden. Da die Aussonderung insbesondere manueller Karteien Schwierigkeiten bereitet, hat das Ministerium für Wirtschaft in Ergänzung seines Erlasses vom 21.3.1983 durch Erlaß vom 3.9.1987 geregelt, Führerscheinentziehungen nur noch auf einem besonderen Beiblatt zu vermerken, das spätestens bei Wiedererteilung der Fahrerlaubnis zu vernichten ist. Wie meine Überprüfungen belegen, wird gegen die Anordnung noch vielfach verstoßen.

Auch die Einführung automatisierter Führerscheinverfahren wird dieses Problem nicht lösen, weil in diesen Verfahren die Löschung derartiger Eintragungen gleichfalls manuell erfolgen muß. Damit steigt die Wahrscheinlichkeit, daß die Löschung ebenfalls vergessen wird und somit personenbezogene Daten unzulässigerweise gespeichert bleiben. Es ist zu gewährleisten, daß - unabhängig vom eingesetzten Verfahren - spätestens nach Wiedererteilung der Fahrerlaubnis oder nach Ablauf einer angemessenen Frist die Löschung der Daten über die Führerscheinentziehung erfolgt.

6.8.3 Einwohnermelderegister

Bei allen geprüften Gemeinden waren automatisierte Verfahren zur Führung des Einwohnermelderegisters eingesetzt. Obwohl diese Verfahren von verschiedenen Herstellern stammen, waren die festgestellten Mängel vielfach identisch. Insbesondere fiel auf, daß die DV-Verfahren im Regelfall nicht an die saarländischen Bestimmungen des Meldegesetzes angepaßt waren, sondern die Bestimmungen des Melderechtsrahmengesetzes auswiesen. Da der Landesgesetzgeber jedoch in verschiedenen Bereichen abweichende oder ergänzende Bestimmungen in das saarländische Meldegesetz aufgenommen hat, entspricht die praktische Handhabung bei den Gemeinden nicht immer den gesetzlichen Vorgaben.

Es gibt aber auch Beispiele dafür, daß gesetzliche Bestimmungen unzulänglich in DV-Verfahren umgesetzt sind. So regelt z.B. § 3 Abs. 2 Nr. 7 MG, daß die Meldebehörden zur Beantwortung von Aufenthaltsanfragen anderer öffentlicher Stellen für die Dauer von 2 Jahren die Tatsache der Aufenthaltsanfrage speichern dürfen. Bei der praktischen Umsetzung dieser Vorschrift fiel auf, daß die eingesetzten Verfahren über keine Möglichkeit verfügen, die 2-Jahresfrist einzugeben, so daß eine automatisierte Löschung nach Ablauf der Frist nicht gewährleistet war.

Insbesondere bei der Beschaffung automatisierter neuer Meldeverfahren ist besonderer Wert auf eine entsprechende Anpassung an die landesspezifischen Gegebenheiten zu legen. Die Details sollten in einem Leistungsverzeichnis festgelegt werden; es ist darauf zu achten, daß nur solche Verfahrensteile installiert werden, für die im Saarland gesetzliche Regelungen bestehen. Dies trifft vor allem auf die zugelassenen regelmäßigen Datenübermittlungen zu, die von Bundesland zu Bundesland stark abweichen können.

Von meinem Angebot, in derartigen Fällen ausnahmsweise auch bereits mit dem Verfahrensanbieter in Kontakt zu treten (TZ 3.5), wurde nur vereinzelt Gebrauch gemacht.

Erhebliche Mängel wurden auch bei den regelmäßigen Datenübermittlungen an andere öffentliche Stellen festgestellt. Obwohl diese abschließend im Gesetz sowie der Meldedatenübermittlungsverordnung (Bund/Land) geregelt sind, erfolgten z.B. regelmäßige Übermittlungen Neugeborener an das Gesundheitsamt, ins Ausland weggezogener Einwohner an das Finanzamt sowie zugezogener schulpflichtiger Kinder an das Schulamt. Nach Hinweis auf die fehlenden landesrechtlichen Bestimmungen in der Meldedatenübermittlungsverordnung wurden in allen Fällen die unzulässigen regelmäßigen Datenübermittlungen unverzüglich eingestellt.

Die Prüffeststellungen ergaben des weiteren, daß dem Melderegister zunehmend die Funktion eines Adreßregisters innerhalb der Gemeinde zugewiesen wird. In den meisten geprüften Gemeinden wurden Online-

Anschlüsse zu verschiedenen Ämtern der Gemeinde festgestellt, die wohl auch aus diesem Grund eingerichtet worden sind. Dies mag praktisch sein, ist aber nur in engen Grenzen erlaubt.

Die Datenweitergabe innerhalb einer Gemeinde ist in § 31 Abs. 7 MG gesetzlich geregelt, ohne daß die zulässige Form festgelegt wurde. Daraus kann jedoch nicht gefolgert werden, daß jedes Amt einer Gemeinde online mit dem Melderegister verbunden werden darf. Online-Verbindungen enthalten ein besonderes Gefährdungspotential, weil der Schutz der Daten durch den "an sich" zuständigen Mitarbeiter gelockert wird. Ob dies in Kauf genommen werden darf, ist vielmehr anhand von Angemessenheitskriterien abzuwägen; solche sind beispielsweise Eilbedürftigkeit oder Vielzahl der erforderlichen Datenweitergaben.

Das Ministerium des Innern sah sich aufgrund meiner Prüfungen wegen der grundsätzlichen Bedeutung für alle Gemeinden veranlaßt, die Weitergabe von Melderegisterdaten innerhalb der Gemeinde im automatisierten Abrufverfahren durch Erlaß landeseinheitlich verbindlich zu regeln. Es hat ausdrücklich festgelegt, daß eine Weitergabe nur erfolgen darf, soweit dies zur Aufgabenerfüllung erforderlich ist. So ist es im Regelfall nicht notwendig, Kenntnis von allen Melderegisterdaten zu erhalten. Vielmehr reicht es grundsätzlich aus, den Zugriff nur auf Namen und Anschrift freizugeben.

Als Ergebnis schreibt der Erlaß für die Einrichtung eines automatisierten Abrufs innerhalb der Gemeinde folgendes vor:

- Durch Dateierrichtungsanordnung und entsprechende technische Maßnahmen ist sicherzustellen, daß Anlaß, Zweck, Empfänger und Datenart festgelegt werden.
- Für jede Organisationseinheit, die einen Zugriff auf Melderegisterdaten erhält, sind bestimmte Datengruppen, deren Kenntnis pauschal als erforderlich beurteilt werden kann, festzulegen. Beim Abruf aus den festgelegten Datengruppen kann die Zulässigkeit vorausgesetzt werden. Soweit weitergehende Informationen benötigt werden, ist eine herkömmliche Einzelabfrage zumutbar.
- Durch EDV-technische Vorkehrungen ist sicherzustellen, daß sämtliche Abfragen aus den Melderegistern protokolliert werden. Eine stichprobenartige Relevanzprüfung ist regelmäßig vorzunehmen.
- Durch Dienstanweisung sollen die Einzelheiten über die Verfahrensweise bei derartigen Abrufen festgelegt werden.

6.8.4 Melderegisterauskünfte an Parteien

§ 35 Abs. 4 Nr. 1 des Meldegesetzes sieht vor, daß 8 Monate vor der jeweiligen Wahl die Einwohner durch öffentliche Bekanntmachung darauf hinzu-

weisen sind, daß sie der Weitergabe ihrer Anschriften an Parteien widersprechen können.

Wie eine Stichprobe bei mehreren Gemeinden zeigte, erfolgte eine Bekanntmachung für die Bundestagswahl am 27.9.1998 nur in Ausnahmefällen entsprechend dieser gesetzlich festgelegten 8-Monats-Frist. Dies ist erklärlich daraus, daß der genaue Wahltag erst im Bundesgesetzblatt vom 10.3.1998 veröffentlicht wurde. Eine Verkürzung der Frist hat das Innenministerium für zulässig gehalten, wenn bis zur erstmaligen Übermittlung die erforderliche Mindestfrist von 2 Monaten beachtet wird; für die gesetzliche Frist sei ausschlaggebend gewesen, daß der Gesetzgeber die Zeitspanne von 2 Monaten zwischen öffentlicher Bekanntmachung und frühestmöglicher Übermittlung der Daten als angemessene Frist zur Wahrung des Grundrechts auf informationelle Selbstbestimmung Betroffener angesehen habe.

Mehrere Gemeinden räumten den Einwohnern dagegen nur eine Frist von 4 Wochen für die Abgabe ihres Widerspruchs ein. Ich mußte deshalb fordern. daß jedenfalls die oben genannte Mindestfrist eingehalten wird. In einzelnen Gemeinden wurde der Mangel dadurch behoben, daß dann überhaupt keine Daten für Wahlwerbezwecke weitergegeben wurden. Dagegen hat zumindest eine der Gemeinden sogar Adressen an Parteien weitergegeben, obwohl den Einwohnern eine Widerspruchsfrist von nur 9 Tagen eingeräumt war.

Wie bereits ausgeführt, erfolgte die amtliche Bekanntmachung des Wahltermins so spät, daß der gesetzlichen Bestimmung des § 35 Abs. 4 MG nicht voll entsprochen werden konnte. Da hiermit auch bei sonstigen allgemeinen Wahlen (Bürgermeister, Kreistag, Landtag) gerechnet werden muß, bei denen die Frist grundsätzlich zu beachten ist, stellt sich die Frage nach der Sinnhaftigkeit der geltenden gesetzlichen Bestimmung.

Ohnehin zeigten (im Saarland insbesondere telefonische) Beschwerden von Betroffenen wieder einmal, daß sie mit der Zusendung von Wahlwerbeunterlagen nicht einverstanden waren. Die Veröffentlichung mit dem Hinweis auf die Widerspruchsmöglichkeit hat viele Bürger nicht erreicht, so daß sie davon keinen Gebrauch machen konnten.

Um die Rechte der Bürgerinnen und Bürger zu verbessern, empfehlen deshalb die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 5./6. Oktober 1998 (vgl. Anlage 19.13), künftig anstatt der Widerspruchs- die Einwilligungslösung gesetzlich vorzusehen. Einen vergleichbaren Ansatz, der schon beispielhaft für andere Länder wurde, hat der Gesetzgeber im Saarland mit Änderung des Meldegesetzes vom 18.6.1997 gewählt, allerdings bisher lediglich für die Weitergabe von Melderegisterdaten an Adreßbuchverlage.

6.9 Prüfung einer Kreisverwaltung

Exemplarisch nenne ich einzelne Mängel, die wir bei einer Stichproben-Prüfung in der Verwaltung eines Landkreises vorgefunden haben. Sie sollen vor allem deutlich machen, daß die Anforderungen des Datenschutzes nicht nur während der eigentlichen Sachbearbeitung zu beachten sind, sondern auch noch nach deren Abschluß.

6.9.1 Straßenverkehrswesen

Sind seit der Einziehung der Fahrerlaubnis mehr als 10 Jahre vergangen, so wird bei der Führerscheinstelle im Regelfall von einer Ersterteilung der Fahrerlaubnis ausgegangen, die in die Zuständigkeit der Gemeinden fällt.

Mit dieser 10-Jahresfrist steht die tatsächliche Aufbewahrungsdauer der Akten häufig nicht in Einklang. Um der Verwertung weit zurückliegender Vorfälle und etwaiger Auskünfte an Gemeinden vorzubeugen, sollte stets systematisch nach Ablauf der 10-Jahresfrist die Aktenaussonderung veranlaßt werden.

6.9.2 Waffenwesen

Erfahrungsgemäß arbeitet die Verwaltung in diesem Bereich zumindest mit einer - wenn nicht sogar mit mehreren - Dateien, die jedoch den Ist-Zustand korrekt wiedergeben müssen. Wenn die Ereignisse der letzten Jahrzehnte nicht dateimäßig bearbeitet, sondern lediglich nach den Namen aller jemals vorhandenen Inhaber von Waffenerlaubnissen und Genehmigungen abgelegt werden, so ist die derart angewachsene Datenfülle nicht nur unzulässig, sondern überflüssiger Ballast für die Behörde.

Es sei daran erinnert, daß jeder Datenverarbeitungsschritt, also auch die Speicherung personenbezogener Daten, einen Eingriff in das Recht auf informationelle Selbstbestimmung beinhaltet, der in nicht aktualisierten Dateien unrechtmäßig lange anhält.

6.9.3 Versammlungen und Aufzüge

Für öffentliche Veranstaltungen oder Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, ist in § 27 Saarländisches Polizeigesetz die Vernichtung der entsprechenden personenbezogenen Unterlagen im Regelfall zwei Monate nach Ablauf der Veranstaltung oder Ansammlung vorgesehen. Bild- und Tonaufnahmen durch die Polizei sind gem. § 12a Versammlungsgesetz im allgemeinen, soweit sie nicht zum Zwecke der Strafverfol-

gung benötigt werden, nach Beendigung der öffentlichen Versammlung unverzüglich zu vernichten.

Die angeführten Bestimmungen verdeutlichen die zugrunde liegende Absicht des Bundes- und Landesgesetzgebers: Der Bürger soll sich an der Teilnahme an Veranstaltungen nicht dadurch gehindert fühlen, daß er aus diesem Anlaß mit einer "Registrierung" der Verwaltung zu rechnen hat. Eine über die angeführten Fristen hinausgehende Aufbewahrung ist angesichts der gesetzgeberischen Wertungen zum Grundrecht der Versammlungsfreiheit (Art. 8 GG) nicht gerechtfertigt.

6.9.4 Jagdwesen

Weil bei Erwerb eines Jagdscheins bei dem Inhaber geprüft werden muß, ob er über die erforderliche Zuverlässigkeit verfügt, hat sich die Behörde veranlaßt gesehen, die Inhaber in gewissen Zeitabständen von Amts wegen auf ihre weiterbestehende Zuverlässigkeit zu überprüfen. Zu diesem Zweck hat sie von jedem die Vorlage eines Führungszeugnisses gefordert. Solche periodischen Überprüfungen sieht das Waffengesetz (§ 30 Abs. 4) für die Inhaber von Waffenbesitzkarten, jedoch ausdrücklich nicht für die Inhaber von Waffenscheinen und Jagdscheinen vor.

Solange der Gesetzgeber sich nicht für die Gleichbehandlung von Inhabern von Waffenscheinen oder Jagdscheinen mit den Inhabern von Waffenbesitzkarten entscheidet, darf die Verwaltung derartige Überprüfungsaktionen nicht von sich aus starten. Sie muß sich vielmehr nach den Bestimmungen des Jagdrechts auf Tatsachen stützen können, welche die Gültigkeit des Jagdscheins berühren könnten, um ein Verfahren zur Einziehung des Jagdscheins in die Wege leiten zu können. Eine eindringliche Suche nach eventuellen Tatsachen ist der Behörde indes nicht erlaubt.

7 Ausländerwesen

7.1 Ausländeramt eines Landkreises

Bei Prüfung eines Landkreise mußte ich in den Räumen, in denen Publikumsverkehr im Ausländeramt stattfindet, mangelnde optische und akustische Abschottung feststellen. Offenbar muß man besonders darauf hinweisen, daß das Recht auf informationelle Selbstbestimmung als Persönlichkeitsrecht zu den Grundrechten zählt, die jedermann zustehen und nicht nur Personen, die Deutsche sind.

Schon früher wurde des öfteren festgestellt, daß die nach der Ausländerdateienverordnung (AuslDatV) zu führenden Dateien A und B von den Ausländerämtern nicht nach den dort festgelegten Fristen bereinigt wurden. Inso-

fern bestehen unterschiedliche Aufbewahrungsfristen, die bei Wegzug aus dem Bezirk der Ausländerbehörde 10 Jahre, für den Todesfall 5 Jahre betragen. Im letzten Fall ist auch der Datenumfang zu reduzieren (§ 5 Abs. 3 AuslDatV). Zudem sind Löschungsfristen aus Anlaß der Zustimmung zur Visumserteilung zu beachten (§ 6 Abs. 1 Satz 2 AuslDatV).

Nicht gewährleistet war auch die Richtigkeit der Daten, die in der Kartei der ausgestellten Pässe, Kinder- und Reiseausweise gespeichert werden, da z.B. Verlängerungen nicht stets eingetragen wurden.

Obwohl in Asylangelegenheiten schon seit einiger Zeit ausschließlich das Landesamt für Ausländer- und Flüchtlingsangelegenheiten zuständig ist, bestand aus der vergangenen Zuständigkeit der allgemeinen Ausländerbehörden für die Verteilung der Asylbewerber auf die Gemeinden noch eine Kartei, die angeblich nur für statistische Zwecke genutzt wird. Wenn statistische Auswertungen abgeschlossen sind, dürften solche Karteien zukünftig entbehrlich sein.

Auch wurden Anfragen des Landesamtes für Verfassungsschutz in Ausländerangelegenheiten in getrennten Ordnern über 15 Jahre hinaus aufbewahrt. Wenn die Aufbewahrung der Akten für die heutige Aufgabenerfüllung der Ausländerbehörde nicht mehr erforderlich ist, sind die Akten zu vernichten.

Einer Aussonderungsprüfung sind auch die auf Kreisebene vorhandenen sehr sensiblen Daten aus dem Einbürgerungsverfahren zu unterziehen. Es darf nicht bei der Kreisverwaltung noch jahrelang nach der Einbürgerung aktenkundig sein, daß die Frage der Sozialhilfebedürftigkeit oder der Vorstrafen in ehemaligen Verfahren Probleme bereitete.

7.2 Prüfung des Landesamtes für Ausländer- und Flüchtlingsangelegenheiten

Das Landesamt für Ausländer- und Flüchtlingsangelegenheiten, dessen Zuständigkeit sich auf das gesamte Saarland erstreckt, bearbeitet bei Aufnahme, Verteilung und Unterbringung von Flüchtlingen sowie Maßnahmen und Entscheidungen, die Asylbewerber und ihre Angehörigen betreffen, eine Vielzahl personenbezogener Daten. In erheblichem Umfang wird hierbei EDV eingesetzt; innerhalb des Amtes besteht ein internes Netz. Ich habe sowohl die automatisierte Verarbeitung geprüft als auch den konventionellen Aktenumgang beobachtet.

Während ich bei meiner stichprobenartigen Prüfung in der eigentlichen Sachbearbeitung keine Anhaltspunkte für datenschutzrechtliche Verstöße fand, war der formale Umgang mit Akten und EDV-System noch nicht zufriedenstellend. Das Landesamt hat zu allen gerügten Mängeln eine kurz- oder auch längerfristige Abhilfe zugesagt. Einige Mängel wurden schon unmittelbar nach der Prüfung behoben.

Ich gehe davon aus, daß auch zeitaufwendige Maßnahmen, wie etwa das Aussortieren von Akten oder das Bereinigen von Dateien ebenso wie die in Aussicht gestellten technisch-organisatorischen Maßnahmen während des übrigen Alltagsgeschäfts nicht aus den Augen verloren werden.

8 Kataster/Bauwesen

8.1 Bauwesen

Um das bauaufsichtliche Verfahren zu vereinfachen und zu beschleunigen, sind Formulare zu benutzen, die amtlich eingeführt und deshalb in ihrer Gestaltung verbindlich sind. Durch einen Hinweis wurde ich auf datenschutzrechtliche Mängel in verschiedenen Formularen aufmerksam gemacht. Ich bin gern der Anregung gefolgt, dies mit dem Ministerium für Umwelt, Energie und Verkehr zu erörtern, um die Fehler zu beseitigen.

So ist beispielsweise nicht verständlich, weshalb der Antragsteller im Formular zum Antrag auf Grundstücksteilung nach § 9 Landesbauordnung (LBO) den Grund der Veränderung (z.B. Grenzbereinigung, Bebauung, Erbauseinandersetzung, Beleihung) zu offenbaren hat. Nach § 9 LBO darf die Genehmigung nur unter baurechtlichen Gesichtspunkten verweigert werden: die anzugebenden Gründe oder Motive für den Antrag auf Grundstücksteilung erscheinen rechtlich nicht relevant und dürften daher auch nicht erfragt werden. Auch andere Formulare erfragen Daten, auf deren Kenntnis es nach dem Gesetzestext nicht ankommt.

Obwohl die Änderung der Bauordnung für das Saarland bereits vom 27.3.1996 datiert, das Ministerium auch eine entsprechende Bereitschaft gezeigt hat, die Vordrucke zu überarbeiten, sind derzeit bei einem Bauvorhaben immer noch die mängelbehafteten, amtlich veröffentlichten Formulare zu verwenden. Eine Erledigung erscheint mir zwischenzeitlich vordringlich; bisher wurde ich allerdings noch nicht beteiligt.

8.2 Nutzung von Daten der Bauinteressenten zu privaten Zwecken

Personenbezogene Daten einer öffentlichen Stelle dürfen nach dem Grundsatz der Zweckbindung der Daten im Regelfall nur bei der Stelle genutzt werden, die sie auch erheben durfte.

Dieser Grundsatz wurde von einem Bürgermeister nicht beachtet, der alle Interessenten, die sich um eine gemeindeeigene Baustelle beworben hatten, in ein örtliches Kreditinstitut eingeladen hat. Dort wollten sowohl der Bürgermeister zu Fragen der Baulandvergabe als auch Vertreter der Bank über Wege zum Wohneigentum referieren. Auch wenn dem Institut die Daten der Bauinteressenten nicht direkt zugänglich gemacht wurden, war diese Vorge-

hensweise datenschutzrechtlich nicht gerechtfertigt. Daten einer öffentlichen Stelle dürfen nicht gleichzeitig auch privatwirtschaftlichen Interessen nutzbar gemacht werden.

Zwar konnten die vom Bürgermeister eingeladenen Interessenten der Veranstaltung auch fernbleiben. Es war jedoch keineswegs auszuschließen, daß die Interessenten sich faktisch veranlaßt sahen, an der Veranstaltung teilzunehmen, um über das Schicksal ihres Antrags auf Zuteilung einer gemeindeeigenen Baustelle ausreichend informiert zu sein. Dabei waren sie aber auch gleichzeitig möglichen Werbeversuchen der Bank ausgesetzt.

Ich habe der Gemeinde mitgeteilt, daß ich die gleiche umfassende Information durch die Gemeinde gegenüber Bauinteressenten erwarte, die wegen dieser Situation an der Veranstaltung zum eigenen Schutz ihrer Persönlichkeitsrechte nicht teilnehmen wollten. Von einer förmlichen Beanstandung habe ich abgesehen, zumal eine direkte Datenübermittlung an eine private Stelle nicht stattgefunden hat.

9 Wirtschaft, Verkehr, Umwelt

9.1 Prüfung der Sparkasseninformations- und Kommunikationsservice GmbH (SIK)und der Plus-Card GmbH

Bei Prüfung einer Gemeinde hatte ich mich mit Datenverarbeitungsaufgaben zu befassen, mit denen die Gemeinde die Sparkasseninformations- und Kommunikationsservice GmbH (SIK) beauftragt hatte. In diesem Zusammenhang mußte ich den Umfang meiner Prüfkomptenz klären. Dabei stellte sich auch die Frage, ob nicht zugleich eine Prüfung der Eigenorganisation dieser Stelle selbst und ihrer Tochter Plus-Card-GmbH hätte stattfinden können, die ihren Sitz im selben Gebäude haben. Dies kam deswegen in Betracht, weil ja die privatrechtliche Rechtsform allein nicht ausschließt, daß es sich um "öffentliche Stellen" im Sinne des § 2 SDSG handelt, für die meine Prüfkompetenz angeordnet ist (vgl. TZ 6.5 meines 16. TB).

Ergebnis war jedoch, daß beide Unternehmen trotz der überwiegend öffentlichen Beteiligungsverhältnisse der Gesellschafter als juristische Personen des Privatrechts und in datenschutzrechtlichem Sinne als nichtöffentliche Stellen anzusehen sind.

Die Datenverarbeitung für Kommunen und öffentlich-rechtliche Sparkassen ist nicht als Wahrnehmung des Kernbestandes der Tätigkeit öffentlicher Stellen anzusehen, sondern lediglich als Hilfstätigkeit, die als Auftragsdatenverarbeitung für diese Stellen charakterisiert werden kann. Konsequenz daraus ist, daß hinsichtlich der SIK und der Plus-Card-GmbH keine datenschutzrechtliche Kontrolle der Eigenorganisation, soweit sie die Durchführung dieser Auftragsdatenverarbeitung nicht beeinflußt, durch den LfD stattfindet.

Dementsprechend habe ich meine Prüfungen also auf die Erfüllung der datenschutzrechtlichen Anforderungen gem. § 5 SDSG und der technischen und organisatorischen Maßnahmen gem. § 11 SDSG beschränkt (TZ 3.2).

9.2 Vollstreckungsdaten auf dem Kontoeröffnungsantrag

Ein Petent hat sich darüber beschwert, daß eine Sparkasse auf seinem Kontoeröffnungsantrag einen Vermerk über einen vollstreckungsrechtlichen Haftbefehl aus dem Jahr 1980 zur Erzwingung der eidesstattlichen Vermögensversicherung (früher: Offenbarungseid) angebracht habe. Dies sei ihm aus Anlaß von gewünschten Geldtransaktionen entgegengehalten worden. Er hat weiter vorgetragen, daß ein solcher Haftbefehl nie existiert habe.

Auf unsere Intervention hat die Sparkasse diesen Vermerk sofort gelöscht, denn eine Speicherung wäre selbst für den Fall eines ehemals vorhandenen Haftbefehls schon 3 Jahre nach Abgabe der eidesstattlichen Vermögensversicherung und Streichung aus dem amtsgerichtlichen Schuldnerverzeichnis nicht mehr zulässig gewesen (§§ 915g, 915a ZPO).

Nach Auffassung der Sparkasse hätte überdies ein solcher Vermerk an dieser - nicht zur Löschung geeigneten - Stelle gar nicht angebracht werden dürfen, da nach handelsrechtlichen Bestimmungen der Kontoeröffnungsantrag noch 10 Jahre nach Auflösung des Kontos aufzubewahren ist. Eine fristgemäße Löschung der Eintragungen nach der vollstreckungsrechtlichen 3-Jahresfrist wäre an dieser Stelle nicht zu gewährleisten gewesen.

9.3 Kraftloserklärung von Sparkassenbüchern

Im Amtsblatt des Saarlandes werden regelmäßig auf Antrag des Berechtigten abhanden gekommene oder vernichtete Sparkassenbücher aufgeboten und für kraftlos erklärt. Die Berechtigten nutzen damit eine im Saarländischen Sparkassengesetz eröffnete kostengünstigere Alternative zu dem in §§ 1003 ff der Zivilprozeßordnung geregelten Aufgebotsverfahren.

Die entsprechende Bestimmung sieht dabei vor, daß die Bezeichnung des Antragstellers zu veröffentlichen ist und eventuell die Angabe, für wen das Sparkassenbuch bei der ersten Einzahlung ausgestellt wurde. Das Aufgebot ist auch in der Sparkasse auszuhängen.

Bei Durchsicht verschiedener Amtsblätter mußte festgestellt werden, daß noch weitere Daten wie z.B. Namen des Alten- und Pflegeheimes sowie der Zusatz "Betreuer" beim Antragsteller mit veröffentlicht wurden.

Ich habe das Ministerium für Wirtschaft und Finanzen auf meine Bedenken gegen die Bekanntgabe der über die gesetzlichen Anforderungen hinausgehenden Daten in Kenntnis gesetzt.

Das Ministerium hat eingeräumt, daß insoweit datenschutzrechtliche Bedenken gegen die Veröffentlichung der Daten nicht zu verkennen seien. Dem Anliegen solle im Zuge der Novellierung des Saarländischen Sparkassengesetzes Rechnung getragen werden.

Ein Entwurf zur Novellierung des Saarländischen Sparkassengesetzes ist mir bislang nicht vorgelegt worden.

9.4 Anonymität von Geldkarten

Weit verbreitet ist zwischenzeitlich der Gebrauch von Chipkarten im Geldverkehr; fast jeder, der bei Sparkassen und Banken ein Konto hat, kann mit seiner Ausweis- oder EC- Karte an Geldautomaten Bargeld erhalten oder an Kassen angeschlossener Händler unmittelbar mit der Karte bezahlen. Daneben gibt es die Zahlung über Kreditkarten von speziellen Unternehmen, die ebenfalls individuelle Konten führen und jeweils mit den Kreditunternehmen bzw. unmittelbar dem Kunden abrechnen.

Als Alternative zu diesen Verfahren, die die einzelnen Bewegungen nachvollziehbar dem jeweiligen Konto zuordnen, haben die Datenschutzbeauftragten schon früh eine "anonyme" Form kartengestützten Geldverkehrs gefordert, die eben derartige "Spuren" vermeidet. Gedacht war an die Möglichkeit, ein einmal auf der Karte gespeichertes Guthaben beim Abheben am Automaten bzw. beim Bezahlen im Geschäft schlicht zu "verbrauchen".

Viele Kreditinstitute haben inzwischen Karten ausgegeben, die - so die Information an die Kunden - über die Funktionalität der Geldkarte verfügen. Allerdings ist gegenwärtig der praktische Nutzen u. a. deswegen noch nicht groß, weil die Zahl derjenigen Stellen, die diese Bezahlungsform akzeptieren und entsprechende Einrichtungen hierfür geschaffen haben, noch gering ist. Auch scheint die derzeitige Form den Kundenwünschen noch nicht in vollem Umfang zu entsprechen.

Dies liegt auch daran, daß jedenfalls die hierzulande gebräuchliche Geldkarte des deutschen Kreditgewerbes den Forderungen nach wirklicher Anonymität noch nicht voll entspricht. Vielmehr werden für die unterschiedlichen Abrechnungswege zwischen Händler, Kreditinstituten und Kunden sogenannte "Schattenkonten" geführt, die - wenn auch nur mittelbar - einen Zusammenhang zwischen Kontobewegung und Karte und (bei nicht anonymem Erwerb oder Aufladen des Guthabens) ggf. auch zum Karteninhaber herstellen lassen. Mit einer Entschließung vom 19./20.März 1998 (Anlage 19.11) haben deswegen die Datenschutzbeauftragten des Bundes und der Länder ihre Forderung nach tatsächlicher Anonymität bei Verwendung von Geldkarten bekräftigt.

Kartenhersteller, Sparkassen, Banken und Händlerorganisationen sollten dem bald nachkommen. Gerade bei der anstehenden Umstellung der Währung könnten Geldkarten den Bedarf nach kurzfristigem Geldumtausch ver-

ringern und dazu beitragen, auftretende Unsicherheiten in der Anfangsphase des Euro zu vermeiden. Die Vorteile bargeldlosen Verkehrs (Bequemlichkeit, verringertes Überfallrisiko) sollten sich mit höherem Datenschutz für die Nutzer verbinden.

9.5 Verbraucherberatung für Arbeitskammermitglieder

Aufgrund vertraglicher Vereinbarung übernimmt die Verbraucherzentrale des Saarlandes kostenfreie Beratung für Mitglieder der Arbeitskammer des Saarlandes in Verbraucherschutz- und Umweltschutzangelegenheiten sowie bei Finanzdienstleistungen. Die Beratungsgebühren werden von der Arbeitskammer, einer Körperschaft des öffentlichen Rechts, erstattet. Es war vorgesehen, daß die Verbraucherzentrale bei jeder Beratung einen Beratungsbogen ausfüllt, der u.a. Name und Anschrift des Klienten, Name und Anschrift seines Arbeitgebers, seinen Status als Arbeitnehmer oder als Familienangehöriger, den Beratungsgegenstand sowie eine Einwilligungserklärung zur Übermittlung der Daten an die Arbeitskammer enthalten sollte. Dieser Vordruck sollte als Beratungsnachweis an die Arbeitskammer übermittelt werden.

Ich habe die Datenanforderung der Arbeitskammer für nicht erforderlich und damit für nicht zulässig angesehen (§ 12 SDSG). Mitglieder der Arbeitskammer sind alle im Saarland beschäftigten Arbeitnehmer (§ 3 Saarl. Arbeitskammergesetz). Ein Mitgliederverzeichnis wird nicht geführt. Bei der Arbeitskammer würde durch die Übermittlung ein Datenbestand entstehen, aus dem entnommen werden kann, wer ihrer (ansonsten namentlich nicht bekannten) Mitglieder wann welche Beratungsleistungen bei der Verbraucherzentrale in Anspruch genommen hat. Die Feststellung, daß ein Klient Arbeitnehmer und damit Mitglied der Arbeitskammer ist, kann die Verbraucherzentrale ohne weiteres selbst treffen. Die Arbeitskammer hat ein vertraglich geregeltes Prüfungsrecht vor Ort bei der Verbraucherzentrale. Eine regelmäßige Weitergabe aller Beratungsbogen mit den personenbezogenen Daten an die Kammer ist für eine Überprüfung des Abrechnungsbetrages nicht erforderlich.

Die Klienten sollten zwar eine Einwilligungserklärung für diese Datenübermittlung unterschreiben, aber auch diese hätte das ins Auge gefaßte Verfahren nicht gerechtfertigt. Es ist schon zu bezweifeln, ob eine solche Erklärung rechtsgültig gewesen wäre. Eine öffentliche Stelle kann die Gewährung einer Leistung nicht davon abhängig machen, daß der Betroffene eine Einwilligungserklärung unterzeichnet, obwohl die Aufgabenerfüllung auch mit einem schonenderen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen möglich ist.

Die beteiligten Institutionen haben sich meinen Vorschlägen zur Gestaltung des Verfahrens angeschlossen. Die Beratungsbogen verbleiben bei der Ver-

braucherzentrale. Anstelle der Einwilligungserklärung wurde ein Hinweis für den Verbraucher aufgenommen, daß die Daten nicht weitergegeben und die Bogen nur für Zwecke der Rechnungsprüfung aufbewahrt werden.

9.6 Verwaltungsvorschrift zum Vollzug von Gewerbeuntersagungsverfahren

Durch die Änderung gewerberechtlicher Vorschriften wurde die Zuständigkeit für die Durchführung von Gewerbeuntersagungsverfahren nach § 35 Gewerbeordnung auf die Gemeinden übertragen. Um in den Gemeinden eine einheitliche Handhabung zu gewährleisten sowie die Arbeit zu erleichtern, hat das Ministerium für Wirtschaft und Finanzen eine Verwaltungsvorschrift zum Vollzug des § 35 Gewerbeordnung erlassen. Meine zum Entwurf geäußerten datenschutzrechtlichen Bedenken wurden größtenteils in die endgültige Fassung übernommen. Dadurch wurde insbesondere verdeutlicht, daß

- auch in Gewerbeuntersagungsverfahren der Grundsatz gilt, wonach die Erhebung der Daten beim Betroffenen Vorrang vor der Erhebung bei Dritten hat;
- für Vorermittlungen konkrete Anzeichen für etwaige Unzuverlässigkeiten von Gewerbetreibenden vorhanden sein müssen;
- für die Beurteilung der Unzuverlässigkeit nicht Vermutungen ausreichen, sondern tatsächliche Anhaltspunkte vorliegen müssen;
- bei Anfragen an die Staatsanwaltschaft nicht alle, sondern nur die einschlägigen anhängigen Ermittlungsverfahren abgefragt werden dürfen;
- Anfragen an Behörden, die einem besonderen Amtsgeheimnis unterliegen, konkrete Anhaltspunkte voraussetzen.

9.7 Einwurf von Altglas in Container

Auf den vom Betrieb für das Duale System im Saarland aufgestellten Sammelcontainern sind zur Vermeidung von Ruhestörungen Hinweisaufschriften zu Zeiten aufgeklebt, in denen der Einwurf zulässig ist. Wie ich durch eine Eingabe erfahren habe, wollte der verantwortliche Betrieb bei Beschwerden über Verstöße gegen die Einwurfzeiten den Einwerfer dadurch ermitteln und ihn auf die festgelegten Zeiten hinweisen, daß er über das amtliche Kennzeichen den Halter des Fahrzeuges feststellt.

Im konkreten Fall erfolgte der Hinweis auf die Einwurfzeiten, obwohl feststand, daß die einwerfende Person eine Frau, der Halter des Fahrzeuges jedoch ein Mann war. Deshalb war zumindest nach Halterfeststellung klar,

daß hiermit eine andere Person als der eigentliche Störer festgestellt worden wäre.

Die Mitteilung an den Halter stellt sich vielmehr als unzulässige Datenübermittlung an eine private Stelle dar, für die eine gesetzliche Grundlage fehlt. Der Halter wurde unzulässigerweise über persönliche bzw. sachliche Verhältnisse der einwerfenden Person informiert und erfuhr dadurch, daß diese Person bei Gelegenheit der Nutzung seines Fahrzeuges eine Ordnungswidrigkeit begangen haben soll. Wie dieser Fall eindeutig belegt, ist die Halterfeststellung ein ungeeignetes Mittel zur Identifizierung des Störers.

Da es sich bei der Ordnungswidrigkeit nicht um eine Ordnungswidrigkeit im Zusammenhang mit dem Straßenverkehr handelte und dem Betrieb für das Duale System die Verfolgung und Ahndung der Ordnungswidrigkeiten nicht übertragen ist, fehlt außerdem eine gesetzliche Grundlage für die Übermittlung der Halterdaten durch die Zulassungsstelle.

Der Betrieb für das Duale System im Saarland hat nach längerem Schriftwechsel mitgeteilt, er werde künftig von Halterfeststellungen bei der Zulassungsstelle absehen.

10 Soziales

Im Sozialbereich hatte ich mich neben strukturellen Prüfungen und der Beteiligung an EDV-Verfahren und Verwaltungsvorschriften mit einer größeren Zahl von Eingaben zu befassen, von denen einzelne hier herausgegriffen werden sollen, weil sie immer wieder vorkommende Problemlagen aufzeigen.

Von besonderer Bedeutung war das zunehmende Bestreben, für den Ausschluß mißbräuchlicher Inanspruchnahme öffentlicher Leistungen ausgeklügelte Ermittlungsverfahren und den automatisierten Abgleich von Dateien unterschiedlicher Träger einzusetzen. Kein Zweifel, daß die gerechte Verteilung knapper Finanzmittel nicht ohne Kontrollen gelingen kann; wie Gesetzgeber und Verwaltung hierbei vorgegangen sind, mußte jedoch deutliche Zweifel daran aufwerfen, ob nicht die Persönlichkeitssphäre der Betroffenen ungebührlich aus dem Blick gerät.

Denn vor dem Hintergrund, daß niemand dadurch, daß er auf Sozialleistungen angewiesen ist, mehr als andere Bürger staatlichem Eingriff oder Zugriff ausgesetzt sein soll, hat der Gesetzgeber für Sozialdaten einen besonderen Schutz geschaffen. Ein Aspekt des Sozialdatenschutzes ist, daß bei den Sozialleistungsträgern vorhandene Daten an andere Behörden und für andere Zwecke nur unter einschränkenden Voraussetzungen weitergegeben werden dürfen.

10.1 Erweiterter Datenaustausch bei Sozialleistungen

Eine Arbeitsgruppe der Arbeits- und Sozialminister hat 1997 in einem Bericht Vorschläge zur Verbesserung des Datenaustausches im Bereich der Sozialleistungen vorgelegt. Hintergrund der Überlegungen war vor allem, durch verstärkte Datenübermittlungen Überzahlungen und Doppelleistungen zu verhindern. In dem Bericht der Arbeitsgruppe werden Verfahren der Datenerhebung vorgesehen, die schwerwiegend in die Rechte der Betroffenen eingreifen. Dies betrifft etwa Datenerhebungen ohne konkrete Verdachtsmomente für einen Sozialleistungsmißbrauch. Damit besteht die Gefahr, daß die Betroffenen zum Objekt staatlicher Kontrolle gemacht werden, was eine Abkehr von der Vorstellung des "mündigen Bürgers" bedeutet.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich kritisch mit den Ergebnissen des Berichts auseinandergesetzt und ihre Bedenken in einer gemeinsamen Entschließung vom 20.10.1997 (Anlage 19.6) zusammengefaßt.

10.2 Sozialhilfedatenabgleichsverordnung gem. § 117 BSHG

In meinem 15. Tätigkeitsbericht (TZ 11.1) habe ich unter dem Stichwort Abbau des Sozialdatenschutzes die Vorschrift des § 117 BSHG erwähnt, die einen automatisierten Datenabgleich zwischen Sozialhilfeträgern sowie zwischen diesen und anderen Sozialleistungsträgern, nämlich mit der Bundesanstalt für Arbeit sowie den gesetzlichen Renten- und Unfallversicherungen, erlaubt. Das Gesetz sieht vor, daß die Durchführung des Datenabgleichs im einzelnen in einer Verordnung zu regeln ist, die sicherstellen soll, daß die Datenabgleiche auf datenschutzgerechte Art und Weise erfolgen. Diese Datenabgleichsverordnung ist am 1. Januar 1998 in Kraft getreten.

Im Saarland beteiligen sich alle Träger der Sozialhilfe an dem Datenabgleich, der mit einem beträchtlichen Aufwand verbunden ist. Einbezogen in den Abgleich sind die Empfängerinnen und Empfänger laufender Hilfe zum Lebensunterhalt außerhalb von Einrichtungen zwischen 18 und 65 Jahren.

Auf meine Anfrage hat mir das Ministerium für Frauen, Arbeit, Gesundheit und Soziales mitgeteilt, daß dort die Ergebnisse des bisherigen Datenabgleichs noch nicht vorliegen. Sobald dies der Fall ist, werde ich prüfen, wie die Sozialhilfeträger bei gemeldeten Fällen von Überschneidungen verfahren. Ich werde darauf achten, ob zunächst ein Gespräch mit dem Betroffenen geführt wird, bevor Feststellungen bei anderen Leistungsträgern getroffen werden. So ist etwa die Datei der geringfügig Beschäftigten beim Verband deutscher Rentenversicherungsträger besonders fehleranfällig, so daß in vielen Fällen von gemeldeten Überschneidungen nicht ohne weiteres von einem unberechtigten Leistungsbezug ausgegangen werden kann.

10.3 Datenübermittlung von Sozialbehörden an Polizei - Änderung des § 68 SGB X

Durch eine in der Öffentlichkeit fast unbemerkte, in ihren Auswirkungen auf den Sozialdatenschutz aber nicht zu unterschätzende Gesetzesänderung hat der Gesetzgeber für eine weitere Aushöhlung des Sozialdatenschutzes gesorgt.

Schon in der Vergangenheit gab es selbstverständlich Mitteilungen auch der Sozialbehörden an andere Stellen etwa zur Gefahrenabwehr oder Durchsetzung des staatlichen Strafanspruchs. Zur Erfüllung von Aufgaben der Polizeibehörden, der Staatsanwaltschaften und Gerichte, der Behörden der Gefahrenabwehr, der Justizvollzugsanstalten oder zur Durchsetzung von öffentlich-rechtlichen Ansprüchen in Höhe von mindestens 1000,-- DM war es aber bisher nur zulässig, neben Name, Vorname, Geburtsdatum, Geburtsort, Namen und Anschriften des derzeitigen Arbeitgebers, die derzeitige Anschrift des Betroffenen mitzuteilen (§ 68 Abs. 1 Satz 1 SGB X).

In der Vergangenheit gab es Fälle, in denen die Polizei Mitteilung erhalten wollte, wenn ein polizeilich Gesuchter bei einem Sozialleistungsträger vorspricht oder einen Termin vereinbart. Auf § 68 Abs. 1 SGB X konnten solche Übermittlungsersuchen nicht gestützt werden, da der vorübergehende Aufenthalt im Amt oder zukünftige Vorsprachen nicht unter den Begriff "derzeitige Anschrift" fielen.

Um hier Abhilfe zu schaffen, hat der Gesetzgeber im "Ersten Gesetz zur Änderung des Medizinproduktegesetzes" § 68 Abs. 1 Satz 1 SGB X dahingehend geändert, daß nunmehr auch neben der derzeitigen Anschrift des Betroffenen sein "derzeitiger oder zukünftiger Aufenthalt" mitgeteilt werden dürfen.

Diese Gesetzesänderung hat weitreichende Konsequenzen für den Sozialdatenschutz. Man muß sich klar machen, daß beispielsweise Jugendämter, Arbeitsämter, gesetzliche Krankenkassen, Berufsgenossenschaften, Sozialämter an Ordnungsbehörden, Polizei und Strafverfolgungs- sowie Strafvollstreckungsbehörden Mitteilung über die momentane Anwesenheit oder über zukünftige Vorsprachetermine machen müssen. Dabei kommt es für das Ersuchen auf einen Zusammenhang mit Sozialleistungen nicht an (bei Sozialhilfebetrug etwa besteht seit jeher eine entsprechende Übermittlungsbefugnis der Träger); auch ist als Anlaß jede Art der Aufgabenerfüllung sowie das Durchsetzen von Geldforderungen über 1000,-- DM ausreichend. Das im Sozialleistungsbereich erforderliche Vertrauensverhältnis der Klienten zu den Trägern wird empfindlich belastet. Das Vorhalten derartiger Ersuchen über ein halbes Jahr führt auch bei Leistungsträgern mit verzweigtem Geschäftsstellennetz zu einer erheblichen Verbreitung möglicherweise stigmatisierender Hinweise.

Mehr als ein Verstoß gegen die guten Sitten in der Gesetzgebung ist, daß die Vorschrift ohne öffentliche Diskussion zustande gekommen ist und im

"Gesetz zur Änderung des Medizinproduktegesetzes" versteckt wurde. Dabei soll der Gesetzesvorbehalt für Grundrechtseinschränkungen doch über seine demokratische und rechtsstaatliche Funktion hinaus auch Transparenz für den Bürger sichern!

Zusammenfassend ist festzustellen, daß die vom Deutschen Bundestag beschlossene Gesetzesänderung eine grundlegende Veränderung in der Systematik der Sozialdatenschutzes bewirkt, der bisher mit gutem Grund von differenzierten und gestuften Übermittlungsbefugnissen geprägt war.

10.4 Mitteilung des Sozialamtes an die Führerscheinstelle bei Zweifeln an der Kraftfahreignung

Das Ministerium für Umwelt, Energie und Verkehr als Aufsichtsbehörde über die Straßenverkehrsbehörden hat mich um Stellungnahme zu der Frage gebeten, ob die Sozialämter die Führerscheinstellen informieren dürfen, wenn sie Kenntnis von der mangelnden Kraftfahreignung eines Hilfeempfängers erhalten. Im konkreten Fall war der Hilfeempfänger auf seine Tauglichkeit zur Verrichtung gemeinnütziger Arbeiten vom Gesundheitsamt untersucht worden. Dabei hatte die Amtsärztin festgestellt, daß der Hilfeempfänger zum Führen von Kraftfahrzeugen nicht geeignet ist. Auf den ersten Blick liegt nahe, daß bei der einen Behörde gewonnene Erkenntnisse auch an anderer Stelle nutzbar gemacht werden, zumal dies dazu dienen kann, mögliche Gefahren für den Betroffenen selbst wie für andere zu vermeiden.

Der Umstand, daß das Gesundheitsamt einen Sozialhilfeempfänger für ungeeignet zum Führen von Kraftfahrzeugen hält, unterliegt jedoch bei dem Sozialamt dem Schutz des Sozialgeheimnisses (§ 35 Abs. 1 Satz 1 SGB I). Sofern nicht der Betroffene eingewilligt hat, ist eine Offenbarung an andere Stellen nur zulässig, wenn eine gesetzliche Offenbarungsbefugnis nach den §§ 68-77 SGB X besteht (§ 67b Abs. 1 Satz 1 SGB X). Eine spezielle gesetzliche Befugnis zur Offenbarung der mangelnden Kraftfahreignung eines Betroffenen gegenüber der Führerscheinstelle ist nicht erkennbar. Sie ergibt sich insbesondere nicht aus § 69 Abs. 1 Nr. 1 SGB X, weil die Übermittlung nicht zur Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch erforderlich ist.

Auch § 34 StGB (rechtfertigender Notstand) vermag nach meiner Auffassung eine Offenbarung von Sozialgeheimnissen nicht zu rechtfertigen. Für staatliche Maßnahmen gilt der Vorbehalt des Gesetzes. Speziell für Eingriffe in das informationelle Selbstbestimmungsrecht hat das Bundesverfassungsgericht im Volkszählungsurteil aus dem Jahre 1983 diesen Grundsatz herausgestellt, in dem das Gericht ausführt, daß Einschränkungen des Rechts auf informationelle Selbstbestimmung einer gesetzlichen Grundlage bedürfen, "aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für

den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entsprechen."

Wenn in Fällen der vorliegenden Art die Führerscheinstellen von den Sozialämtern informiert werden sollen, müßte der Gesetzgeber, der zwischen dem Recht des Betroffenen auf Schutz der informationellen Selbstbestimmung und Rechten anderer sowie der Gemeinschaft abzuwägen hat, die Offenbarungsbefugnisse der §§ 68 ff SGB X um einen entsprechenden Tatbestand erweitern. Gerade hierauf wurde allerdings in dem Gesetzgebungsverfahren zur Änderung des Straßenverkehrsgesetzes nach Abwägung des Für und Wider verzichtet.

10.5 Datenermittlung in der Sozialhilfe

Eine Petentin hat mich gefragt, ob die nachstehend geschilderte Verfahrensweise des Sozialamtes datenschutzrechtlich korrekt war:

Das Sozialamt hatte den Verdacht, daß die Frau die Wohnung, für die sie Sozialhilfe bezog, nicht mehr bewohnte, sondern mit einem Partner in eheähnlicher Gemeinschaft in dessen Wohnung lebte. Um diesen Verdacht zu erhärten, wurde die Petentin aufgefordert, eine Einwilligungserklärung zur Einholung von Auskünften über ihren Wasser- und Stromverbrauch bei den örtlichen Versorgungswerken zu unterzeichnen.

Ich habe dem betreffenden Sozialamt mitgeteilt, daß ich dieses Vorgehen nicht für vereinbar mit den Bestimmungen des Sozialdatenschutzes halte. Sozialdaten sind grundsätzlich beim Betroffenen zu erheben (§ 67a Abs. 2 Satz 1 SGB X). Der Petentin hätte somit Gelegenheit gegeben werden müssen, die erforderlichen Informationen durch Vorlage ihrer Verbrauchsabrechnungen selbst zu liefern. Dadurch würde vermieden, daß ein Dritter unnötigerweise Kenntnis vom Sozialhilfebezug erhält.

Das Sozialamt hat eingeräumt, daß die Petentin selbstverständlich die Möglichkeit besitze, ihre Verbrauchsabrechnung selbst vorzulegen. Auf diese Möglichkeit müssen die Hilfesuchenden dann aber auch ausdrücklich hingewiesen werden.

10.6 Auskunftserteilung in der Sozialhilfe

Ein Bürger, dessen Sohn Leistungen des Sozialamtes bezieht, hat sich mit folgender Anfrage an meine Dienststelle gewandt:

Der Petent hat gegenüber dem Sozialamt im Rahmen der Heranziehung als Unterhaltsverpflichteter Angaben über seine Einkommensverhältnisse gemacht. Er wollte aber vermeiden, daß sein Sohn im Rahmen des Verwaltungsverfahrens Kenntnis von seinen Einkommensverhältnissen erlangt. Auf

entsprechende Nachfrage beim Sozialamt wurde ihm gesagt, daß er dies nicht verhindern könne; einem entsprechenden Auskunftsersuchen des Sohnes müsse entsprochen werden.

Dieser Rechtsmeinung des Sozialamtes konnte ich mich nicht anschließen. Dem Betroffenen, hier dem Sohn, steht zwar gemäß § 83 SGB X grundsätzlich ein Auskunftsrecht hinsichtlich der zu seiner Person gespeicherten Sozialdaten zu. Die Auskunftserteilung muß allerdings unterbleiben, soweit die Daten wegen der überwiegenden berechtigten Interessen eines Dritten geheimgehalten werden müssen (§ 83 Abs. 4 Nr. 3 SGB X). Eine solche Fallkonstellation habe ich im vorliegenden Fall als gegeben angesehen. Das Geheimhaltungsinteresse des Petenten, daß die sensiblen Daten über seine Einkommensverhältnisse seinem Sohn nicht zur Kenntnis gelangen, überwiegt dessen Interesse an einer vollständigen Datenauskunft.

Das betreffende Sozialamt habe ich aufgefordert, diesem Geheimhaltungsinteresse in der Praxis dadurch Rechnung zu tragen, daß bei einem Auskunftsverlangen des Sohnes die Daten über die Einkommensverhältnisse des Petenten ausgespart werden bzw. bei einer Akteneinsicht die entsprechenden Unterlagen, aus denen die Einkommensverhältnisse ersichtlich sind, aus den Akten genommen werden.

Die Leitung des betreffenden Sozialamtes hat sich meiner Auffassung angeschlossen und alle Mitarbeiter und Mitarbeiterinnen seines Sozialamtes auf die Einhaltung der entsprechenden Datenschutzbestimmungen hingewiesen.

10.7 Blankovollmachten in Sozialhilfeanträgen

Bei mehreren Sozialämtern stellte ich fest, daß noch immer Antragsformulare verwendet werden, die pauschale Einwilligungserklärungen nach folgendem Muster enthalten:

"Die Behörden und Bankinstitute ermächtige und beauftrage ich zur Auskunftserteilung über meine Vermögensverhältnisse. Den behandelnden Arzt, die Kliniken und ärztl. Gutachter entbinde ich hiermit gegenüber dem Sozialhilfeträger von der ärztlichen Schweigepflicht! Diese Ermächtigung gilt zugleich als datenschutzrechtliche Einwilligung."

Der Hilfesuchende, der nicht von vornherein die Ablehnung der Hilfegewährung riskieren will, hat keine andere Wahl, als solche Klauseln im Antrag "mit zu unterzeichnen". Von einer echten Freiwilligkeit der Einwilligung kann keine Rede sein. Die Erklärungen sind auch nicht ausreichend bestimmt: der Antragsteller kann nicht erkennen, bei welchen Stellen konkret welche Informationen aus welchem Anlaß, für welchen Zweck, zu welchem Zeitpunkt eingeholt werden. Die Erklärungen werden nur "auf Vorrat" eingeholt; ein Bedarf, davon Gebrauch zu machen, besteht nur in Einzelfällen. Solche Einwilligungsklauseln im Antragsformular sind daher unzulässig.

Daten sind grundsätzlich beim Betroffenen zu erheben (§ 67a SGB X). Der Hilfesuchende hat im Rahmen seiner Mitwirkungspflicht die erforderlichen Unterlagen zum Nachweis seiner Hilfebedürftigkeit selbst beizubringen, z.B. Kontoauszug, Sparbuch, ärztliche Bescheinigung. Nur wenn dies nicht möglich oder nicht zumutbar ist oder Anhaltspunkte dafür vorliegen, daß die Angaben des Betroffenen unrichtig sind, kann eine Anfrage bei anderen Stellen in Betracht kommen. Solche Anfragen bei Dritten sind zwangsläufig mit der Übermittlung der Tatsache verbunden, daß der Betroffene Sozialhilfe beantragt oder erhält. Diese Datenübermittlung ist nur unter den Voraussetzungen der §§ 67d ff SGB X erlaubt. Erst wenn eine Anfrage bei Dritten gerechtfertigt ist, hat der Hilfesuchende - soweit nicht ohnehin eine gesetzliche Auskunftspflicht besteht (z.B. nach § 21 Abs. 4 SGB X) - eine Einwilligungserklärung im Einzelfall zu erteilen.

10.8 Das Archiv einer Sozialverwaltung

Bei einem Landkreis habe ich auch die Altregistratur des Sozial- und Jugendamtes besucht, die in einem alleinstehenden Hinterhaus untergebracht ist . Das Gebäude wird nur für die Aufbewahrung von Altakten genutzt. Das "Archiv" befand sich in einem - in einer öffentlichen Verwaltung nicht erwarteten - chaotischen Zustand. In allen Räumen des Hauses waren in offenen Regalen, in Kartons, in nicht abgeschlossenen, alten Stahlschränken oder einfach auf dem Fußboden Akten, Karteien und Listen mit personenbezogenen Daten abgelagert worden; darunter Unterlagen über Amtsvormundschaften, Jugendhilfezahlungen, Unterhaltsvorschußleistungen, Schuldnerberatung, Unterbringungen im Frauenhaus, Kriegsopferfürsorge, Pflegegeld, Eingliederungshilfe für Behinderte, Sprachheilbehandlung, Arztabrechnungen, Vorgänge über "Armenfürsorge" 1938, aber auch umfangreiche Aktenbestände des Kreisbauamtes. Ein Plan über die Verteilung der Akten war nicht vorhanden; ein System, wo welche Akten aufbewahrt werden, kaum erkennbar.

Aus datenschutzrechtlicher Sicht war festzustellen:

- Der Zugang zu dem Archiv ist nicht ausreichend gesichert. Insbesondere die Eingangs-Holztür mit dem großen Glasausschnitt bietet keinen besonderen Einbruchsschutz.
- In dem Gebäude sind Altakten mit personenbezogenen Daten unterschiedlicher Organisationseinheiten (Sozialamt, Jugendamt, Bauamt) gelagert. Mitarbeiter aus diesen Bereichen haben Zugang zu den Räumen und können somit Akten aus anderen Aufgabenbereichen einsehen. Es handelt sich überwiegend um Unterlagen, die dem Sozialdatenschutz unterliegen.

- Ein großer Teil der Akten wird bereits so lange aufbewahrt, daß er zur Aufgabenerfüllung nicht mehr erforderlich ist und vernichtet werden könnte.
- Die Akten sind so ungeordnet gelagert, daß eine ordnungsgemäße Aussonderung bei Ablauf von Aufbewahrungsfristen nicht gewährleistet ist. Dadurch wird insbesondere die gesetzliche Verpflichtung zur Löschung der Sozialdaten erschwert. Auch das Recht der Betroffenen, auf Antrag die sie betreffenden Akten einsehen zu können, kann kaum erfüllt werden.

Die Kreisverwaltung hat eine Änderung dieses Zustandes zugesagt; ich werde dies prüfen.

10.9 Datenschutzprüfung beim Medizinischen Dienst der Krankenversicherung

Im Berichtszeitraum habe ich eine Datenschutzkontrolle beim Medizinischen Dienst der Krankenversicherung (MDK) durchgeführt.

Der MDK ist eine in der Rechtsform einer Körperschaft des öffentlichen Rechts gebildete Arbeitsgemeinschaft der Träger der gesetzlichen Krankenversicherung im Saarland. Er hat seine Tätigkeit im Jahre 1991 aufgenommen. Seine Aufgaben und Datenverarbeitungsbefugnisse im Bereich der Krankenversicherung sind im 9. Kapitel des SGB V (§§ 275 - 277), im Bereich der Pflegeversicherung in § 97 SGB XI geregelt. Im Vordergrund der Tätigkeit des MDK steht die Begutachtung von Arbeitsunfähigkeiten, Rehabilitationsanträgen und unkonventionellen Therapien. Ein weiterer Schwerpunkt ist die Begutachtung im Rahmen der Verfahren auf Feststellung der Pflegebedürftigkeit.

Neben Feststellungen zu technisch-organisatorischen Aspekten habe ich geprüft, ob der Datenfluß den sehr differenzierten gesetzlichen Bestimmungen entspricht, die vor allem gewährleisten sollen, daß auch im dienstlichen Verkehr der beteiligten Stellen untereinander bei den großenteils besonders sensiblen Daten die Kenntnis und die Einwirkungsmöglichkeit auf den Kreis beschränkt bleibt, für dessen Tätigkeit dies unbedingt erforderlich ist:

- Anforderung von ärztlichen Unterlagen - durch den MDK oder die Krankenkassen?
  In vielen Fällen ist es notwendig, für die Begutachtung durch den MDK Krankenunterlagen anzufordern, etwa bei behandelnden Ärzten oder Krankenhäusern. Aus datenschutzrechtlicher Sicht stellt sich das Problem, wer diese Unterlagen anfordert und an welche Stelle (Krankenkasse oder Medizinischer Dienst) die Unterlagen zu übersenden sind.

Der MDK des Saarlandes verfährt nach Auskunft seines Geschäftsführers in der Praxis so, daß die erforderlichen Unterlagen von den Krankenkassen bei den Leistungserbringern angefordert werden und mit dem Begutachtungsauftrag dem MDK übergeben werden. Diese Verfahrensweise entspreche der gesetzlichen Regelung in § 276 Abs. 1 Satz 1 SGB V, wonach die Krankenkassen verpflichtet seien, dem MDK die für die Beratung und Begutachtung erforderlichen Unterlagen vorzulegen. Für die Begutachtung von Arbeitsunfähigkeiten wurde auf die "Begutachtungsanleitung Arbeitsunfähigkeit" verwiesen, die auch die Arztanfrage durch die Krankenkassen (Seite 15,16) vorsieht.

Diese Verfahrensweise begegnet datenschutzrechtlich keinen Bedenken, wenn sichergestellt ist, daß die Ärzte die angeforderten Unterlagen - als Arztsache deklariert in verschlossenem Umschlag - an die Krankenkassen schicken und diese von dort ungeöffnet an den MDK weitergeleitet werden. Denn für die Aufgabenerfüllung der Krankenkassen ist eine Kenntnisnahme dieser Unterlagen nicht erforderlich und damit auch nicht zulässig. Der Gesetzgeber geht davon aus, daß Krankenkassen und MDK keine Einheit bilden, in der Informationen über Patienten frei ausgetauscht werden können. Die Mitteilungsbefugnis des MDK an die Krankenkassen ist auf das Ergebnis der Begutachtung und die erforderlichen Angaben über den Befund beschränkt (§ 277 Abs. 1 Satz 1 SGB V). Würde man den Krankenkassen das Recht einräumen, unter Umständen umfangreiche Arztberichte einzusehen, würde der Sinn dieser gesetzlichen Regelung obsolet. Darüber hinaus ist in § 276 Abs. 2 Satz 1 2. Halbsatz SGB V ausdrücklich bestimmt, daß die Leistungserbringer verpflichtet sind, Sozialdaten auf Anforderung des MDK unmittelbar an diesen zu übermitteln, wenn die Krankenkassen eine gutachtliche Stellungnahme oder Prüfung durch den MDK veranlaßt haben.

- Mitteilung an behandelnde Ärzte (Widerspruchsrecht des Versicherten)
  Gemäß § 277 Abs. 1 Satz 1 hat der Medizinische Dienst dem behandelnden Arzt und sonstigen Leistungserbringern, über deren Leistungen er eine gutachtliche Stellungnahme abgegeben hat, das Ergebnis der Begutachtung mitzuteilen. Er ist darüber hinaus befugt, den behandelnden Ärzten und Leistungserbringern die erforderlichen Angaben über den Befund mitzuteilen. Der Versicherte kann der Befundmitteilung widersprechen (§ 277 Abs. 1 Satz 3 SGB V).

  Ein Gebrauchmachen von dem Widerspruchsrecht setzt voraus, daß der Versicherte über dieses Recht informiert wird.

  Eine Information (allein) im Einladungsschreiben zur Begutachtung, wie es die "Richtlinien über die Zusammenarbeit der Krankenkasse mit den MDK" vorsehen, halte ich nicht für ausreichend. Der Hinweis sollte im Rahmen der Begutachtung durch den MDK erfolgen. Hier bietet sich der Zeitpunkt unmittelbar nach der Begutachtung an, weil der Betroffene erst nach

Kenntnis des Befundes fundiert über seinen Widerspruch entscheiden kann. Um nachträglich feststellen zu können, ob der Hinweis tatsächlich erfolgt ist, sollte der Hinweis schriftlich dokumentiert werden. Der MDK hat zugesagt, zukünftig in dieser Weise zu verfahren.

- Mitteilung des Gutachtenergebnisses an die gesetzliche Krankenkasse
  Gemäß § 277 Abs. 1 hat der MDK "das Ergebnis der Begutachtung und die erforderlichen Angaben über den Befund" mitzuteilen. Eine stichprobenweise Überprüfung der den Krankenkassen zur Verfügung gestellten Gutachten hat ergeben, daß die Gutachteninhalte über den gesetzlich festgelegten Umfang hinausgingen. So werden den Krankenkassen regelmäßig Gutachten mit eingehenden Angaben über Anamnese, Diagnosen und Befunde übermittelt.

  Die Gutachten müssen sich zwar nicht auf eine reine Ergebnismitteilung beschränken, weil die Krankenkassen für ihre Entscheidung das Ergebnis der Begutachtung nachvollziehen können müssen. Andererseits gebietet die funktionelle Trennung zwischen MDK und Krankenkassen eine Beschränkung der Informationsweitergabe. Den Krankenkassen sind nur die zum Verständnis des jeweiligen Gesamtzusammenhangs unerläßlichen Einzelangaben zu übermitteln. Umfassende Angaben zur gesamten Krankengeschichte des Versicherten benötigen die Krankenkassen im Regelfall zur Erfüllung ihrer Aufgaben nicht.

  Der MDK hat es abgelehnt, seine Verfahrensweise zu ändern; nach seiner Auffassung seien die Krankenkassen, die allein die Entscheidung über die Gewährung von Leistungen zu treffen haben, auf die bisher mitgeteilten Angaben in vollem Umfang angewiesen.

- Mitteilung des Untersuchungsergebnisses an die Pflegekasse
  Zum Umfang der den Pflegekassen mitzuteilenden Informationen bestimmt § 18 Abs. 5 SGB XI, daß der MDK der Pflegekasse das "Ergebnis" seiner Prüfung mitzuteilen und Maßnahmen zur Rehabilitation, Ort und Umfang von Pflegeleistungen sowie einen individuellen Pflegeplan zu empfehlen hat.

  Bei der Prüfung wurde festgestellt, daß der Umfang der Gutachten, die den Pflegekassen zur Verfügung gestellt werden, über eine Ergebnismitteilung hinausgeht. Der MDK benutzt einen Vordruck, der auf den ersten drei Seiten das eigentliche Gutachten enthält. Erst ab der vierten Seite werden die hieraus resultierenden Ergebnisse und Empfehlungen dokumentiert. Diese Verfahrensweise widerspricht der eindeutigen gesetzlichen Regelung des § 18 Abs. 4 SGB XI.

  Auch in diesem Punkt will der MDK an seiner bisherigen Verfahrensweise festhalten.

Die zuständige Aufsichtsbehörde habe ich über meine Feststellungen und Bewertung unterrichtet.

10.10 Einkommensnachweis in der gesetzlichen Krankenversicherung

Ein Petent hatte folgendes datenschutzrechtliches Problem:

Die Ehefrau des Petenten ist als Selbständige freiwilliges Mitglied einer gesetzlichen Krankenkasse. Die Krankenkasse hatte seine Ehefrau aufgefordert, zur Festsetzung des Krankenkassenbeitrages ihr Einkommen anzugeben; als Nachweis wurde die Vorlage des Einkommensteuerbescheides verlangt. Der Petent sah es als einen unzulässigen Eingriff in seine Persönlichkeitsrechte an, daß die Krankenkasse auf diesem Wege auch Kenntnis von seinen Einkommensverhältnissen erhält.

Die Prüfung der Rechtslage unter Beteiligung der betreffenden Krankenkasse hatte folgendes Ergebnis: Die Speicherung von Sozialdaten durch Sozialleistungsträger ist nur zulässig, wenn es zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden gesetzlichen Aufgaben erforderlich ist (§ 67c Abs. 1 SGB X). Das Einkommen des Ehegatten eines freiwilligen Mitgliedes einer gesetzlichen Krankenkasse kann, anders als ich ursprünglich angenommen hatte, durchaus erheblich für die Festsetzung der Beitragshöhe sein. Denn nach einer Satzungsbestimmung der betreffenden Krankenkasse ist bei der Beitragsberechnung für freiwillig Versicherte, deren Lebensunterhalt überwiegend von den Einnahmen des nicht getrennt lebenden Ehegatten bestritten wird, von der Hälfte der monatlichen Einnahmen beider Ehegatten auszugehen. Ich war deshalb mit dem Vorschlag der Kasse einverstanden, zunächst eine Prüfung dieser Frage vorzunehmen und danach die nicht erforderlichen Angaben zu schwärzen. Der Petent hatte damit zumindest erreicht, daß bei der Kasse dauerhaft keine Informationen über sein Einkommen vorgehalten werden.

10.11 Gesetzliche Unfallversicherung

Zum 01.01.97 ist mit dem SGB VII neues Recht für die gesetzliche Unfallversicherung in Kraft getreten. Die wichtigsten datenschutzrechtlichen Neuregelungen hatte ich bereits in meinem 16. TB TZ. 18.7 dargestellt.

Ich habe im Herbst 1998 geprüft, in welcher Weise die Unfallkasse des Saarlandes die neuen bereichsspezifischen Datenschutzbestimmungen im 8. Kapitel des SGB VII in der Praxis umgesetzt hat; z.B. ob den Versicherten mindestens 3 Gutachter zur Auswahl benannt werden, bevor der Auftrag für das Gutachten erteilt wird, wie die Datenerhebung bei Ärzten erfolgt oder wie den Informationspflichten gegenüber den Betroffenen nachgekommen wird. Meine Feststellungen vor Ort, insbesondere die Gespräche mit den Mitar-

beitern und die Einsicht in zahlreiche Leistungsakten, haben ergeben, daß die Unfallkasse diese Vorschriften datenschutzgerecht anwendet. Lediglich bei Anfragen bei Ärzten war aus den eingesehenen Akten nicht ersichtlich, ob die Vorschrift des § 203 Abs. 2 Satz 1 SGB VII beachtet wird. Danach hat der Unfallversicherungsträger den Versicherten auf das Auskunftsverlangen und auf das Recht, über die von den Ärzten übermittelten Daten unterrichtet zu werden, rechtzeitig hinzuweisen.

Positiv hervorzuheben ist, daß der Zugang zu dem Gebäude durch elektronisches Zugangskontrollsystem für die Mitarbeiter, durch Klingelanlage und Pförtnerdienst gut gesichert ist, um Unbefugten Zugang und Zugriff zu den Sozialdaten zu verwehren. Nicht befriedigend ist, daß alle Mitarbeiter der Unfallkasse berechtigt sind, alle im automatisierten System gespeicherten Daten der Verletztendatei oder eingescannte Schriftstücke (optische Speicherung) am Bildschirm zu lesen, in denen Daten über Krankheiten, Verletzungen, Arztleistungen usw. erfaßt sind. Ich habe gefordert, die Zugriffsbefugnisse auf das zur jeweiligen Aufgabenerledigung des einzelnen Mitarbeiters erforderliche Maß zu reduzieren.

Die Unfallkasse hat "Dienstvorschriften für die Datenverarbeitung, für den Datenschutz personenbezogener Daten" erlassen, die allerdings noch nicht an die Datenschutzvorschriften im SGB VII angepaßt sind. Dazu habe ich Änderungen und Ergänzungen vorgeschlagen.

Ein interner Datenschutzbeauftragter ist entsprechend der gesetzlichen Verpflichtung bestellt; seine konkreten Aufgaben bei der Unfallkasse waren jedoch nicht festgelegt. Außerdem bestand eine Interessenkollision mit seinen übrigen Aufgaben, zu denen auch die Systemverwaltung gehört.

Darüber hinaus habe ich die Beseitigung technisch-organisatorischer Mängel, z.B. der unzureichenden Funktionstrennung, und von Mängeln im Bereich der Personalverwaltung gefordert.

10.12Dialogverfahren in der Rentenversicherung

Die Landesversicherungsanstalt für das Saarland beteiligt sich an einem zwischen den Landesversicherungsanstalten im Bundesgebiet und der Bundesversicherungsanstalt für Angestellte vereinbarten Verfahren, das es ermöglicht, auch die Daten von Versicherten abzurufen, für die die Landesversicherungsanstalt örtlich oder sachlich nicht zuständig ist. Das Verfahren soll einer umfassenden Versichertenberatung dienen; die Erstellung, Anforderung, Aushändigung und Erläuterung von Versicherungsverläufen, Rentenauskünften, Lückenauskünften und Auskünften über Beitragserstattungen auch durch unzuständige Versicherungsträger soll ermöglicht werden.

Durch dieses neue Verfahren ist die Zugriffsmöglichkeit auf Rentendaten, die bisher auf den Zuständigkeitsbereich eines Versicherungsträgers beschränkt

war, deutlich ausgeweitet worden und damit auch die Gefahr einer mißbräuchlichen Datenverwendung gestiegen.

Ich habe mich bei der LVA für das Saarland über die dort getroffenen technisch-organisatorischen Maßnahmen, um unbefugte Zugriffe zu verhindern, informiert:

- Die Zugriffsmöglichkeit ist auf die Mitarbeiter der Auskunfts- und Beratungsstelle und 3 Reha-Fachberater, die im Außendienst tätig sind, beschränkt.
- Bei Vorsprache eines Versicherten wird zur Identitätsprüfung die Vorlage des Personalausweises verlangt.
- Beim zuständigen Versicherungsträger wird im Falle eines Abrufs im Versichertenkonto der abrufende Versicherungsträger, der Name des abrufenden Mitarbeiters sowie Datum und Uhrzeit des Abrufs protokolliert.
- Bei der Landesversicherungsanstalt des Saarlandes notieren die Mitarbeiter der Auskunfts- und Beratungsstelle in einem Handprotokoll die Namen der vorsprechenden Versicherten. Dieses Handprotokoll wird für jeden Tag erstellt und dem zuständigen Referatsleiter am darauffolgenden Tag zur Kenntnisnahme vorgelegt.

Darüber hinaus wurde zwischen den Datenschutzbeauftragten des Bundes und der Länder und den Rentenversicherungsträgern das Grundsatzproblem diskutiert, ob und wie den Versicherten eine Beteiligung hinsichtlich der bundesweiten Abrufmöglichkeit eingeräumt werden soll. Denn es ist davon auszugehen, daß es Versicherte gibt, die den von den Rentenversicherungen angebotenen Service niemals benötigen oder die eine solche weitreichende Abfragemöglichkeit einfach nicht wollen. Mittlerweile hat der Verband der Rentenversicherungsträger akzeptiert, daß die technischen Zugriffsmöglichkeiten fremder Rentenversicherungsträger auf Versichertenkonten vom Willen des Betroffenen abhängig gemacht werden sollen. Auf ausdrücklichen Wunsch des einzelnen Versicherten soll durch Einführung eines Merkmals die Anzeige des Versicherungskontos beim unzuständigen Rentenversicherungsträger unterbunden werden.

10.13 Sozialversicherungsangestellte als nebenberufliche Versicherungsmitarbeiter

Ein Versicherungsbüro hatte mir in einer Eingabe folgendes mitgeteilt:

"Die ...Kasse bietet und verkauft unter Verwendung der vorhandenen Personendaten ihrer Versicherten Versicherungsgeschäfte (z.B. Betriebshaftpflichtversicherungen, Lebensversicherungen etc.) an Landwirte. Aus meiner

Sicht stellt sich hier erstens Datenmißbrauch und zweitens eine immense Wettbewerbsverzerrung dar."

Nach Darstellung des Sozialversicherungsträgers weisen seine Mitarbeiter bei Anfragen, Beratungen u.a. von Versicherten auf die Möglichkeiten des Abschlusses von Betriebshaftpflichtversicherungen, privaten Unfallversicherungen, Lebensversicherungen und anderen Versicherungen hin. Nur soweit die Betroffenen dann selbst entsprechendes Interesse zeigten, werde ihnen gegebenenfalls ein konkretes Angebot unterbreitet. Die betreffenden, eigens geschulten Mitarbeiter hätten eine Nebentätigkeitsgenehmigung.

Versicherte wenden sich demnach in Angelegenheiten der Sozialversicherung an den Sozialleistungsträger und erhalten bei dieser Gelegenheit Angebote für Versicherungen, die der Mitarbeiter des Sozialversicherungsträgers in Nebentätigkeit, d.h. auf privater Basis, vermittelt. Ich sehe darin die Gefahr einer unzulässigen Nutzung von Sozialdaten.

Sozialdaten dürfen von dem Sozialversicherungsträger nur für die gesetzlich vorgesehenen Zwecke genutzt werden (§ 35 Abs. 2 SGB I, §§ 67 b Abs. 1 und 67 c Abs. 1 SGB X). Das Angebot oder Vermitteln von privaten Versicherungen gehört nicht zu diesen Zwecken. Eine zweckfremde Nutzung von Sozialdaten ist zwar mit Einwilligung des Betroffenen zulässig. Die Einwilligung muß jedoch stets der Datenverwendung vorausgehen. Im vorliegenden Fall würde dies bedeuten, daß der Versicherte von sich aus den nebenberuflich tätigen Mitarbeiter wegen einer Versicherung anspricht und erst danach in eine eventuelle Verwendung von Sozialdaten einwilligt. Wenn die Initiative dagegen von dem Mitarbeiter der Sozialversicherung ausgeht, bedeutet dies, daß er seine Kenntnis der Sozialdaten für seine mit der dienstlichen Tätigkeit nicht in Zusammenhang stehende Versicherungstätigkeit nutzt. Dies wäre unzulässig. Aber auch dann, wenn die Datenverwendung mit Einwilligung erfolgt, kann zweifelhaft sein, ob die Erklärung in völliger Freiwilligkeit abgegeben wurde. Die Zwangsmitgliedschaft bei dem Sozialversicherungsträger und die Abhängigkeit von den Sozialleistungen könnte einen Versicherten in seiner Entscheidungsfreiheit beeinflussen.

Weil in der Praxis nur schwer feststellbar sein dürfte, ob im Einzelfall die Grenze des Erlaubten überschritten wird, sollte ein Sozialversicherungsträger grundsätzlich - um jeden Verdacht einer unzulässigen Datenverwendung zu vermeiden - seinen Beschäftigten nicht gestatten, private Versicherungen für die Sozialversicherten abzuschließen oder solche Versicherungen zu vermitteln. Entsprechende Nebentätigkeiten dürften nicht genehmigt werden.

Die Stellungnahme der Aufsichtsbehörde, die ich zur Klärung der Angelegenheit eingeschaltet habe, steht noch aus.

10.14 Elternbeiträge für den Besuch von Kindergärten

Die Jugendämter übernehmen bei geringem Einkommen der Eltern im Rahmen der Jugendhilfe die Beiträge zum Besuch von Kindergärten und anderen Kindertageseinrichtungen. Die Jugendhilfeleistung wird jedoch nicht den Eltern überwiesen, sondern unmittelbar mit der jeweiligen Einrichtung bzw. dem Träger abgerechnet. Aus der Sicht des Datenschutzes ist diese Praxis deshalb von Bedeutung, weil stets eine Datenübermittlung an die Einrichtung über die Gewährung der Hilfe erfolgt, ohne daß die Eltern darüber (im Antrag) informiert werden oder ihre Einwilligung geben. Es ist leicht vorstellbar, daß ein Großteil der Erziehungsberechtigten daran interessiert ist, im Kindergarten nicht als "sozial schwach" eingestuft zu werden und daß sie die Beiträge wie "normale" Eltern selbst an die Einrichtung bezahlen wollen. Auch bei anderen Sozialleistungen werden die Hilfen nicht ohne weiteres an einen Dritten, sondern an die Berechtigten gezahlt. So wird etwa das Wohngeld oder die im Rahmen des BSHG übernommene Miete nicht stets an den Vermieter überwiesen, sondern dem Leistungsempfänger ausgezahlt, der - als mündiger Bürger - regelmäßig seine Zahlungsverpflichtungen selbst zu erfüllen hat.

Wenn die Kinder im Haushalt der Eltern leben und die Hilfe nur wegen des geringen Einkommens und nicht wegen familiärer Probleme gewährt wird, ist aus meiner Sicht kein zwingender Grund ersichtlich, die Beiträge über den Kopf der Betroffenen hinweg unmittelbar mit den Einrichtungen abzurechnen. Die Einrichtungen benötigen keine Kenntnis darüber, welche Eltern mit welchem Ergebnis Leistungen beantragt haben. Es dürfte ausreichen, wenn sie die Eltern in allgemeiner Form über die Möglichkeit der Kostenübernahme durch das Jugendamt informieren.

Der Jugendhilfeträger weist darauf hin, daß es sich bei der Übernahme der Beiträge gem. § 23 Abs. 2 des Gesetzes zur Förderung von Kinderkrippen und Kinderhorten vom 29.11.89 um eine Ausfallfinanzierung der Einrichtungen handele. Die Leistung des Jugendamtes sei aufgrund dieser gesetzlichen Bestimmung an die Einrichtung zu zahlen; eine Wahlmöglichkeit der Erziehungsberechtigten bestehe nicht. Das Ministerium für Frauen, Arbeit, Gesundheit und Soziales hatte sich in seiner Stellungnahme zunächst dieser Meinung angeschlossen, dann aber aufgrund meiner Bedenken die saarländischen Jugendämter gebeten, die Jugendhilfeleistung im Regelfall den Berechtigten auszuzahlen und nur im Einvernehmen mit diesen eine direkte Zahlung an den Träger der Einrichtung vorzunehmen. Nachdem von seiten eines Jugendamtes eine andere Rechtsauffassung vorgetragen wurde, hat das Ministerium das praktizierte Verfahren für rechtmäßig erklärt und sein Rundschreiben an die Jugendämter korrigiert.

Nach meiner Auffassung stehen die Bestimmungen des SGB VIII einer Auszahlung der Jugendhilfeleistung an die Eltern nicht entgegen. Dabei ist auch das Recht der Eltern zu berücksichtigen, daß Wünschen hinsichtlich der Ge-

staltung der Hilfe entsprochen werden soll, soweit dies nicht mit unvertretbaren Mehrkosten verbunden ist (§ 5 SGB VIII). Sofern die saarländischen Gesetze zur Förderung der vorschulischen Erziehung bzw. zur Förderung von Kinderkrippen und Kinderhorten nur eine Auszahlung an die Einrichtung zulassen, sollte bei nächster Gelegenheit eine Gesetzesänderung ins Auge gefaßt werden.

10.15 Jugendhilfeunterlagen auf dem Flur

Anläßlich der Datenschutzprüfung bei einer Kreisverwaltung fand ich auf dem Flur des Jugendamtes mehrere unverschlossene Kästen mit zahlreichen alten Karteikarten über nichteheliche Kinder. Auf der gleichen Etage waren in einem offenstehendem Raum, in dem sich ein Getränkeautomat für Mitarbeiter und Besucher befindet, stapelweise Akten der Jugendhilfe (z.B. Familienpflegevorgänge aus den Jahren 1992/93, Vorgänge über die Übernahme von Kindergartenbeiträgen) abgelegt. Die Unterlagen mit teilweise sehr sensiblen Daten waren für Publikum und andere unbefugte Personen frei zugänglich, so daß sich jeder hätte bedienen können. Auch nach entsprechenden Hinweisen an den Amtsleiter sind im Verlauf der Prüfung die Unterlagen nicht entfernt worden. Erst nach mehreren schriftlichen Aufforderungen sind die Vorgänge ca. 4 Monate nach der Prüfung dem "Zugriff der Öffentlichkeit" entzogen worden. Ein solcher Umgang mit Sozialdaten durch eine Sozialbehörde ist nicht akzeptabel.

10.16 Vertraulichkeit des Gesprächs beim Jugendamt

Bei der Prüfung eines Jugendamtes konnte ich unbeabsichtigt das im benachbarten Büroraum von einem Sozialarbeiter mit einem Klienten geführten Gespräch mitverfolgen. Die Büros waren im Bereich eines Bücherregals nur durch eine Holzplatte voneinander getrennt, die keinen ausreichenden Schallschutz bot. Außerdem konnte ich bei dieser Gelegenheit feststellen, daß Sozialarbeiter des Allgemeinen Sozialdienstes bei weit geöffneter Bürotür mit vorsprechenden Personen verhandelten, Telefonate führten oder Berichte diktierten, so daß Wartende im Flur mithören konnten.

Der Jugendhilfeträger hat inzwischen Maßnahmen zur Verbesserung des Schallschutzes getroffen und die Mitarbeiter auf ihre Sorgfalts- und Verschwiegenheitspflicht hingewiesen.

10.17 Jugendhilfeteam

Entscheidungen über die Gewährung von Hilfe zur Erziehung werden bei einem von mir geprüften Jugendamt von einem "Jugendhilfeteam" getroffen (§ 36 Abs. 2 SGB VIII), dem angehören

- Leiter der Verwaltung des Jugendamtes als Vorsitzender
- Leiter des Sachgebietes Sozialdienst
- Leiter wirtschaftliche Jugendhilfe
- Amtspfleger/Amtsvormund (soweit betroffen)
- Zuständiger Sozialarbeiter.

Die Eltern werden ebenfalls zu der Teamsitzung eingeladen. Die Sitzung wird vorbereitet durch eine von dem zuständigen Sozialarbeiter zu erstellende Vorlage, in der u.a. die Personalien des Kindes, der Eltern und Geschwister, eventuelle vormundschaftsgerichtliche Beschlüsse, eine eingehende Problemanalyse (familiäre Situation, Entwicklung des Minderjährigen, Erziehungssituation, Wünsche der Betroffenen, vorgeschlagene Maßnahmen usw.) darzustellen sind.

Die Beteiligung eines Mitarbeiters der wirtschaftlichen Jugendhilfe stößt auf Bedenken. Die Aufgaben dieses Sachgebiets liegen in der verwaltungsmäßigen, insbesondere finanziellen Abwicklung, nicht in der Gestaltung der Hilfe zur Erziehung. In der Teamsitzung werden vertrauliche, tief in die Privatsphäre der Betroffenen eingreifende Fakten angesprochen. Der Kreis der Teilnehmer sollte daher so klein wie möglich gehalten werden, um zu vermeiden, daß Bedienstete Kenntnis von Informationen erhalten, die sie zur Erledigung der ihr übertragenen Aufgaben nicht unbedingt benötigen. Wirtschaftliche Belange stehen bei diesen Sitzungen nicht im Vordergrund; sie können - falls geboten - auch durch die übrigen Teammitglieder, z.B. den Leiter des Jugendamtes, sichergestellt werden. Das Sozialgeheimnis ist auch innerhalb des Leistungsträgers zu wahren (§ 35 Abs. 1 SGB I). Die von dem Minderjährigen und den Eltern dem Sozialarbeiter zum Zweck persönlicher und erzieherischer Hilfe anvertrauten Daten unterliegen zudem einem besonderen Vertrauensschutz (§ 65 SGB VIII). Die "wirtschaftliche Jugendhilfe" sollte deshalb in die Beratungen des Hilfeteams nicht einbezogen werden.

Aus den gleichen Gründen wird es für nicht erforderlich gehalten, die schriftliche Vorlage für die Teamsitzung in die Fallakte der wirtschaftlichen Jugendhilfe aufzunehmen. Für deren Aufgabenerfüllung dürfte eine kurze Begründung der Hilfegewährung sowie die Mitteilung der Entscheidung des Teams im Antragsvordruck genügen.

Das Jugendamt hat meinen Bedenken entsprochen.

10.18 Statistikprogramm Jugendhilfe

Das oben bereits erwähnte Jugendamt setzte ein mit MS-Access selbst erstelltes Statistikprogramm ein. Bei jeder Jugendhilfegewährung wurde erfaßt: Aktenzeichen, Familienname, Vorname, Geburtsdatum, Wohnort, Straße, Geschlecht, Staatsangehörigkeit, Kindschaftsverhältnis, Familienstand der Eltern, Aufenthalt, Schule, Ausbildung vor Hilfe, jetzige und frühere Hilfeart, Hilfeanlaß, Hilfebeginn und -ende, Form der Unterbringung, Ursache. Seit Beginn der Speicherung wurden noch keine Daten gelöscht.

Die Speicherung der sensiblen, personenbezogenen Daten war in dieser Form nicht mit den Datenschutzbestimmungen des SGB VIII vereinbar. Die Daten sollten ausschließlich für statistische Zwecke im Zusammenhang mit der Jugendhilfeplanung gem. §§ 79, 80 SGB VIII verwendet werden. Für diesen Zweck dürfen zwar Sozialdaten - soweit erforderlich - gespeichert und genutzt werden; sie sind jedoch nach § 64 Abs. 3 SGB VIII unverzüglich zu anonymisieren. Die Speicherung von Identifikationsdaten wie Namen, Geburtsdatum, Adresse ist für statistische oder planerische Zwecke überhaupt nicht erforderlich; sie ist insoweit unzulässig. Um den Verlauf der Hilfe im Einzelfall dokumentieren zu können, hätte die Erfassung des Aktenzeichens genügt. Die gespeicherten Daten wären damit immer noch "personenbezogen" im Sinne des § 67 SGB X , weil über das Aktenzeichen der Personenbezug herstellbar ist. Wenn die Hilfegewährung abgeschlossen ist, muß der Zweck der Speicherung (noch) personenbezogener Sozialdaten für die Jugendhilfeplanung als erfüllt angesehen werden. Die Daten sind danach unverzüglich (vollständig) zu anonymisieren, d.h. das Aktenzeichen ist ebenfalls zu löschen.

Ich habe verlangt, die Identifikationsdaten in dem vorhandenen Datenbestand zu löschen. Anstelle des genauen Geburtsdatums sollte die Speicherung des Geburtsjahres ausreichen; das genaue Beginn- und Endedatum könnte durch die Angabe von Monat und Jahr ersetzt werden. Bei bereits abgeschlossenen Hilfefällen ist auch das Aktenzeichen zu löschen.

Das Jugendamt hat - nachdem die Abrechnung der Jugendhilfeleistungen künftig im ProSoz-Verfahren erfolgen wird - inzwischen die Daten in dem speziellen Statistikprogramm gelöscht.

10.19 EDV-Kontrolle personenbezogener Daten aus Verwendungsnachweise

Mehrere Träger von Beschäftigungsmaßnahmen für Sozialhilfeempfänger haben sich wegen der vom Ministerium für Frauen, Arbeit, Gesundheit und Soziales geforderten personenbezogenen Erfassung der Teilnehmerdaten in den Verwendungsnachweisenn an mich gewandt. Während bisher die Bezuschussung solcher Maßnahmen ohne Nennung personenbezogener Daten in

den Nachweisen möglich war, sollten nun die Namen der Teilnehmer mit Adresse, Geburtsjahr, Geschlecht, Nationalität, Schulabschluß, beruflicher Qualifikation usw. aufgenommen werden. Darüber hinaus wurde den Trägern mit Diskette ein EDV-Programm für die elektronische Erfassung der Daten zur Verfügung gestellt. Daraus war ersichtlich, daß die Daten beim Ministerium in automatisierter Form weiterverarbeitet werden sollten. Der Einsatz eines solchen EDV-Verfahrens war mir nicht bekannt; das Ministerium hatte mich entgegen der Vorschrift des § 8 Abs. 2 SDSG nicht beteiligt.

Das Ministerium erläuterte, daß die Maßnahmen im Rahmen arbeitsmarktpolitischer Landesprogramme durch den Europäischen Sozialfonds (ESF) mitfinanziert werden. Es handelt sich um mehrere, unterschiedliche Programme mit verschiedenen Schwerpunkten und Zielgruppen sowie einer großen Zahl von Teilnehmern, die oft über mehrere Jahre hinweg bei den unterschiedlichsten Trägern gefördert werden. Um eine zweckentsprechende Verwendung der Zuwendungen fristgerecht - auch gegenüber europäischen Institutionen - nachweisen zu können und um Subventionsmißbrauch zu verhindern, habe es sich als unumgänglich erwiesen, eine personenbezogene Erfassung der Teilnehmer einzuführen.

Damit stellt sich die Frage, auf welcher Rechtsgrundlage die Träger der Maßnahmen die Teilnehmerdaten an das Ministerium übermitteln. Ich halte es aus Gründen der Rechtssicherheit und der Transparenz der Datenverarbeitung für die Betroffenen für geboten, von den Teilnehmern eine schriftliche Einwilligungserklärung einzuholen. Diese Einwilligung muß den Anforderungen des § 4 Abs. 2 BDSG genügen; d.h. die Betroffenen sind über den Zweck der Speicherung und der vorgesehenen weiteren Verarbeitung ihrer Daten zu informieren und auf die Folgen einer Verweigerung der Einwilligung hinzuweisen. Ich habe vorgeschlagen, daß das Ministerium den Trägern ein Muster der Einwilligungserklärung mit den Projektunterlagen zur Verfügung stellen sollte.

Im späteren Verlauf des Jahres 1998 plante das Ministerium, die Daten einer bestimmten, früheren Teilnehmergruppe für Zwecke der Evaluierung bei den Trägern der Maßnahme zu erheben und personenbezogen einem Institut weiterzugeben. Das Institut sollte diese Teilnehmer telefonisch zu ihrer Integration in den Arbeitsmarkt befragen. Ich habe die Übermittlung der Daten an das Ministerium für zulässig angesehen, wenn sie in der oben erwähnten Einwilligungserklärung der Teilnehmer vorgesehen ist. Die weitere Datenübermittlung an das Institut konnte jedoch nicht mehr auf diese Einwilligungserklärung gestützt werden. Das Ziel ließ sich allerdings auch auf andere Weise - ohne Übermittlung von Daten - erreichen. Das Ministerium ist meinem Vorschlag zur "Adreßmittlung" gefolgt. Es hat die Träger der Maßnahme gebeten, den ehemaligen Teilnehmern ein Anschreiben des Ministeriums zusenden, in dem diese unter Hinweis auf die Freiwilligkeit gebeten werden, sich mit einer vorgedruckten Rückantwort (Freiumschlag) bei dem

Institut zu melden und damit ihre Bereitschaft zur Teilnahme an der Befragung zu signalisieren.

Die datenschutzrechtliche Beurteilung des EDV-Verfahrens zur Verarbeitung der Teilnehmerdaten beim Ministerium ist noch nicht abgeschlossen. Bisher hat das Ministerium weder das für die Freigabe des Verfahrens notwendige Sicherheitskonzept noch eine Dateibeschreibung (§ 9 SDSG) vorgelegt.

11 Gesundheit

11.1 Externe Mikroverfilmung und Archivierung von Krankenhausunterlagen

Krankenhäuser sind verpflichtet, die Unterlagen über die Behandlung eines Patienten 30 Jahre lang aufzubewahren. Schon aus Kapazitätsgründen ist dies mit den Originalunterlagen schwierig; eigene Möglichkeiten zum Verfilmen bestehen meist nicht und wären auch wenig wirtschaftlich. Es verwundert daher nicht, daß immer mehr Krankenhäuser dazu übergehen, diese Unterlagen durch externe Unternehmen verfilmen oder archivieren zu lassen. Aus datenschutzrechtlicher Sicht besteht das Problem, daß mit der externen Mikroverfilmung und Archivierung dritten, nicht am Behandlungsverhältnis beteiligten Personen eine Vielzahl sensibler, der ärztlichen Schweigepflicht unterliegenden Daten offenbart werden. Die ärztliche Schweigepflicht darf nur durchbrochen werden, wenn entweder der Patient einwilligt oder eine gesetzliche Befugnisnorm die Datenoffenbarung erlaubt.

Für die externe Mikroverfilmung oder Archivierung von Krankenhausunterlagen bestehen im Saarland keine speziellen Rechtsvorschriften. Allerdings können sich die Krankenhäuser gemäß § 29 Abs. 6 Saarländisches Krankenhausgesetz (SKHG) zur Verarbeitung von Patientendaten anderer Personen oder Stellen bedienen. Die Auftragserteilung ist jedoch an folgende Bedingungen geknüpft:

- Eine Auftragsdatenverarbeitung ist nur zulässig, wenn anders Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der Datenverarbeitung hierdurch kostengünstiger besorgt werden können.
- Die Krankenhausleitung hat den Auftragnehmer unter besonderer Berücksichtigung der Eignung und Zuverlässigkeit sorgfältig auszuwählen.
- Der Auftragnehmer muß durch technische und organisatorische Maßnahmen gewährleisten, daß das Patientengeheimnis gewahrt wird.
- Der Auftragnehmer und seine Mitarbeiter sind auf Verschwiegenheit zu verpflichten.

Mit konkreten Modalitäten einer externen Archivierung von Krankenunterlagen habe ich mich bei Krankenhäusern in unserem Land noch nicht befassen müssen. Als erörterungswürdigen Ansatz sehe ich die offensichtlich in anderen Bundesländern praktizierte sogenannte "Container-Lösung" an: Die Patientenakten werden in verschlossenen Containern transportiert und aufbewahrt, wobei die Container nur im Krankenhaus geöffnet werden können. Wenn im Krankenhaus eine Akte benötigt wird, muß der Container zum Krankenhaus transportiert und dort die benötigte Krankenakte entnommen werden.

Völlig unproblematisch ist dies aus folgendem Grund jedoch nicht:

11.2 Beschlagnahmeschutz für Gesundheitsdaten

Zum Schutz des Vertrauensverhältnisses zwischen Arzt und Patient enthält die Strafprozeßordnung (§ 97 StPO) Regelungen, die die Beschlagnahme ärztlicher Unterlagen ausschließen. Nach dem derzeitigen gesetzlichen Konzept endet die Beschlagnahmefreiheit medizinischer Daten, sobald sie in den Gewahrsam von Stellen gleich welcher Art gelangen, die selbst nicht der ärztlichen Schweigepflicht (§ 203 Abs. 1 StGB) unterliegen.

In letzter Zeit sind zunehmend Konstellationen zu beobachten, in denen Patientendaten außerhalb der geschützten Räume des Arztes oder ärztlicher Einrichtungen verarbeitet werden (z.B. externe Mikroverfilmung, externe Archivierung, Vergabe von Schreibarbeiten an externe Schreibbüros, Einschaltung externer Inkassounternehmen usw.). Mit Entschließung vom 17/18. April 1997 (Anlage 19.5) haben die Datenschutzbeauftragten vom Gesetzgeber daher gefordert, als Antwort auf diese zunehmenden Tendenzen den Geltungsbereich der Schweigepflicht gemäß § 203 Abs. 1 StGB und den Anwendungsbereich des damit verknüpften Beschlagnahmeschutzes in sachgerechter Weise auszudehnen.

11.3 Gesundheitsnetze

Zur Zeit arbeiten die verschiedensten öffentlichen und privaten Stellen daran, die schnelle Verfügbarkeit der Informationen zur Verbesserung der Qualität der ärztlichen Behandlung durch moderne Kommunikationsverfahren sicherzustellen. Dabei geht es meist nicht allein darum, allgemein zugängliches sofort verfügbar zu machen, sondern auch um das Vernetzen mit Patientendaten und Arztdaten. Im Saarland ist beispielsweise im Kreis Saarlouis die Zusammenarbeit niedergelassener Ärzte in einem Praxisnetz bekannt geworden. Teilweise einbezogen in die Kommunikation werden auch Kliniken, Abrechnungsstellen und Kassenärztliche Vereinigungen.

Folgende Aspekte erscheinen mir aus datenschutzrechtlicher Sicht beim Datenaustausch in Arztnetzen wesentlich:

- Der Einsatz automatisierter Datenverarbeitung sowohl innerhalb medizinischer Einrichtungen als auch bei der Kommunikation mit Patienten, anderen medizinischen und sonstigen Stellen kann zu höherer Qualität und Effizienz im Gesundheitswesen führen. Ihre Nutzung ist aber nur hinnehmbar, wenn sie den Schutz des unabdingbaren Vertrauensverhältnisses zwischen Arzt und Patient und die Persönlichkeitsrechte anderer Beteiligter wahrt.
- Die Verfügbarkeit von personenbezogenen Daten in digitalisierter Form, die Beteiligung zusätzlicher Stellen und die vermehrte Kommunikation vergrößern die Risiken für das Recht auf informationelle Selbstbestimmung, denen durch angemessene technisch-organisatorische Maßnahmen begegnet werden muß.
- Rechtliche Grundlage der Datenverarbeitung, insbesondere einer Datenweitergabe an andere Stellen ist das jeweilige Behandlungsverhältnis oder eine spezielle Einwilligung hierfür, soweit nicht (ausnahmsweise) eine gesetzliche Befugnis vorliegt. Der Schutz des Patientengeheimnisses ist zu wahren. Zugleich ist der medizinischen Dokumentationspflicht Rechnung zu tragen.
- Ärztlicher Behandlungsvertrag und spezielle Einwilligung begrenzen inhaltlich den Umfang der Datenverarbeitung und den Kreis der hiermit befaßten Personen. Nur Daten in "ärztlichem Gewahrsam" unterliegen strafprozessualem Schutz vor Beschlagnahme. Verzicht auf nicht zwingend erforderliche Daten und Einsatz "datenschutzfördernder" Technologien vermindern generell die Risiken für die Persönlichkeitsrechte der Betroffenen.
- In einer detaillierten Risikoanalyse sind vor Einsatz der Techniken auch mögliche Gefährdungen des informationellen Selbstbestimmungsrechtes zu bewerten und nach dem Stand der Technik durch Maßnahmen auszuschließen, die in einem Sicherheitskonzept beschrieben sind. Da regelmäßig (auch) sensible Daten betroffen sind, die dem Patientengeheimnis unterliegen, muß für die entsprechenden Anwendungen ein über den mittleren Schutzbedarf hinausreichender Schutz gewährleistet werden.
- Analyse und Konzept müssen alle Komponenten der Anwendung innerhalb der Einrichtung wie der Kommunikationsbeziehung mit anderen Stellen einbeziehen. Gesichert sein muß vor allem, daß
  - gespeicherte oder übermittelte Informationen nur den hierfür Autorisierten zugänglich sind oder werden (Vertraulichkeit),

- gespeicherte oder übermittelte Informationen echt sind und ihre Urheberschaft nachvollziehbar ist (Authentizität),
- gespeicherte oder übermittelte Informationen beweisbar unversehrt und vollständig sind (Integrität),
- die zugewiesenen Informationen und Ressourcen den Autorisierten grundsätzlich jederzeit bereitstehen (Systemverfügbarkeit),
- Kommunikationspartner und Informationsquelle gegenseitig sicher und beweisbar erkannt werden (Authentifikation),
- Versand und Erhalt von Informationen beweisbar sind (Nicht-Abstreitbarkeit),
- alle relevanten Aktivitäten revisionssicher, benutzer- und transaktionsabhängig festgehalten werden (Nachvollziehbarkeit),
- die Verarbeitungslogik des Systems verbindlich und nicht verfälschbar festgelegt wird (Verbindlichkeit und Integrität der Verarbeitungslogik).

• Grundsätzlich sollten personenbezogene Daten auch innerhalb der Einrichtung durch Verschlüsselung gesichert sein.

• Besondere Sicherheit verlangt die Übermittlung von Patientendaten in digitalen Netzen, weil hier unbemerkte Kenntnisnahme, Manipulationen oder Fehler während des Transports nicht ausgeschlossen sind. Zwingend ist, personenbeziehbare Daten während des Transports mit hinreichend sicheren kryptographischen Verfahren zu verschlüsseln. Zu fordern ist die Nutzung geschlossener Netze; nach derzeitigem Stand bietet ein Austausch über das - offene - Internet nur bei starker Verschlüsselung ausreichende Sicherheit für den Schutz von Patientendaten.

• Zusätzliche Sicherungsmaßnahmen sind an den Endeinrichtungen nötig: EDV-Einrichtungen, in denen Patientendaten verarbeitet werden, müssen in offenen Netzen durch Fire-Walls gegen unzulässigen Zugriff von außen geschützt sein; Virenprüfprogramme und spezielle Einstellungen müssen Beeinträchtigungen der Daten zuverlässig ausschließen.

• Zugriffsmöglichkeiten auf die Daten sind eng auf den Personenkreis zu beschränken, zu deren Aufgabe die Verarbeitung gehört. Die nur nachträgliche Kontrolle technisch möglicher Zugriffe reicht nicht aus. Eine Wartung der Anlage durch fremdes Personal bedarf strenger Festlegungen und Kontrolle aller Aktivitäten.

• Die Verarbeitung hat grundsätzlich in der Einrichtung zu erfolgen. Eine zentrale Haltung von Patientendaten verschiedener ärztlicher Einrichtungen birgt unverhältnismäßige Risiken und gewährleistet nicht die der ein-

zelnen Stelle obliegende Verantwortlichkeit. Das Einschalten externer Hilfspersonen bedarf ausdrücklicher Einwilligung.

- Datenverarbeitungen mit Kommunikation über die Einrichtung hinaus bedürfen, soweit sie nicht - etwa im Rahmen der gesetzlichen Krankenversicherung - gesetzlich zugelassen sind, nach geltendem Recht einer speziell hierauf bezogenen Einwilligung. Diese kann wirksam nur gegeben werden, wenn die Verarbeitung dem Betroffenen hinreichend transparent sind.

11.4 Krebsregister des Saarlandes

Das Bundeskrebsregistergesetz verpflichtet - mit bestimmten Vorgaben - alle Bundesländer, bis zum 1. 1. 1999 Rechtsgrundlagen für Krebsregister zu schaffen. Obwohl es für das saarländische Krebsregister, das wegen seiner in den "alten" Bundesländern einmaligen Vollständigkeit als Grundlage wissenschaftlicher Untersuchungen geschätzt wird, bereits seit langem eine landesrechtliche Regelung gibt, muß auch diese angepaßt werden.

Das Ministerium für Frauen, Arbeit, Gesundheit und Soziales hat die Anpassung mit mir mündlich erörtert und mir den Entwurf einer Novelle vorgelegt, die nicht eine neue Vollregelung werden soll, sondern die "Ausführung des (Bundes-)Krebsregistergesetzes". Einer der Kernpunkte hierbei ist die Änderung des Meldeverfahrens. Nach dem Bundeskrebsregistergesetz soll nämlich der Patient vor einer Meldung seiner Krebserkrankung an das Register hierüber unterrichtet werden; dem Patienten steht ein Widerspruchsrecht zu.

Die Datenqualität der saarländischen Einrichtung beruht demgegenüber wesentlich darauf, daß die Meldung zum Register durch Ärzte und klinische Einrichtungen ohne Beteiligung des Patienten erfolgt. Die datenschutzrechtlichen Probleme gerade dieser Regelung wurden in früheren Berichten bereits dargestellt.

Für das informationelle Selbstbestimmungsrecht des Patienten stellt allein diese Verfahrensänderung schon eine deutliche Verbesserung dar; deshalb hätte ich eine zügige Verabschiedung des Gesetzes begrüßt. Seit mehr als einem Jahr sind mir allerdings keine weiteren Aktivitäten bekannt geworden.

Wünschenswert wäre auch, möglichst schnell das Registrierverfahren nach dem Bundeskrebsregistergesetz vollständig umzusetzen. Mit dem neuen Verfahren sollen neue Meldungen richtig zugeordnet werden können, ohne daß es nötig ist, innerhalb des Krebsregisters Patienten zu reidentifizieren. Der Entwurf zielt demgegenüber auf eine "Erprobung" dieses Verfahrens parallel zur früheren Handhabung. Der Argumentation, das im Bundeskrebsregistergesetz vorgesehene Chiffrier- und Kontrollnummernsystem könne erst dann eingeführt werden, wenn sich seine Machbarkeit in der Praxis erwiesen habe, kann ich allerdings eine gewisse Berechtigung nicht absprechen.

Schon vor einem solchen gesetzlich angeordneten Verfahrensvergleich hat das Krebsregister im Berichtszeitraum bereits begonnen, das Zusammenführungs- und Abgleichssystem nach dem Bundeskrebsregistergesetz im Rahmen einer Studie ("INNOVA") zu erproben. Ich habe die Datenverarbeitung hierbei überprüft und dabei einige Mängel festgestellt, die aber mittlerweile behoben sind. So fand ich bei meiner Besichtigung eine Sicherungsdiskette mit personenbezogenen und medizinischen Daten vor. Dies stand in eklatantem Widerspruch zu der Forderung nach strikter Trennung der erfaßten Bestände. Die Daten wurden auf meine Anforderung unverzüglich gelöscht. In diesem Zusammenhang habe ich gefordert, daß auf Sicherungsdatenträgern nur verschlüsselt gespeichert wird.

Mir war auch wichtig, daß die Datenverarbeitungsbefugnisse der beiden im Projekt INNOVA eingesetzten Mitarbeiter strikt auf die zur Durchführung jeweils erforderlichen Funktionen beschränkt sind. Programme, die ein unbefugtes Kopieren, Verändern oder Löschen von Daten erlauben, dürfen wegen der besonderen Sensibilität der Daten nicht zur Verfügung gestellt werden. Insgesamt habe ich die Erstellung einer Dienstanweisung verlangt, die die Datenverarbeitungsabläufe darstellt, Maßnahmen der Datensicherung gemäß § 11 SDSG festlegt und die Frage regelt, mit welchen Verfahren und in welchen Zeitabständen die Verschlüsselung der Identifikationsdaten durchzuführen ist.

11.5 Nachweisführung für die Approbation als psychologischer Psychotherapeut

Am 1.1.1999 ist das "Gesetz über die Berufe des psychologischen Psychotherapeuten und des Kinder- und Jugendlichen-Psychotherapeuten (Psychotherapeuten-gesetz- PsychThG) in Kraft getreten. In Übergangsbestimmungen (§ 12 Abs. 3 und 4 PsychThG) hat der Gesetzgeber Psychologen, die bisher an der psychotherapeutischen Behandlung von Patienten beteiligt waren, die Möglichkeit eröffnet, eine Approbation als psychologischer Psychotherapeut zu erlangen, wenn sie entsprechende Nachweise über ihre bisherige Berufsausübung erbringen können.

Aus datenschutzrechtlicher Sicht hat sich die Frage gestellt, wie diese Nachweise erbracht werden können, ohne daß die ärztliche Schweigepflicht verletzt wird. Denn § 12 Abs. 3 und 4 PsychThG sind nach meiner Auffassung keine Offenbarungsbefugnisse im Sinne des § 203 Abs. 1 StGB und keine Befugnisse zur Datenübermittlung. Die Übermittlung personenbezogener Daten halte ich daher grundsätzlich für unzulässig.

Das wegen der bundesweiten Bedeutung der Problematik mit der Angelegenheit befaßte Bundesministerium für Gesundheit hat ausgeführt, daß die Nachweise möglichst mit Fremdbelegen zu führen sind. Das sind z.B. Bestätigungen, die von den gesetzlichen Krankenkassen, den privaten Kranken-

versicherungen und den Beihilfestellen ausgestellt werden. Wo dies nicht möglich ist, etwa weil der Patient seine Rechnung selbst bezahlt hat, dürfen nur Nachweise mit anonymisierten Daten verlangt werden.

Eine Nachfrage bei dem saarländischen Ministerium für Frauen, Arbeit, Gesundheit und Soziales hat ergeben, daß bei Behandlungen, deren Kosten durch einen Kostenträger übernommen wurden, eine Bescheinigung ohne die Identitätsdaten der jeweiligen Patienten akzeptiert wird. Auch bei den sogenannten Selbstzahlern verlangt das Ministerium lediglich Nachweise mit anonymisierten Daten.

11.6 Forschungsvorhaben zur Lebenssituation von Frauen mit Behinderung

Im Berichtszeitraum hat das Bundesministerium für Familie, Senioren, Frauen und Jugend eine wissenschaftliche Studie über die Lebenssituation von Frauen mit Behinderung in Auftrag gegeben. Mit der Durchführung der Studie wurde ein Forschungsinstitut in Freiburg beauftragt. Dieses Forschungsinstitut hat sich an die Versorgungsämter im Bundesgebiet, unter anderem auch an das saarländische Landesamt für Jugend, Soziales und Versorgung, gewandt und um Übermittlung von Namen, Anschrift und Art der Behinderung von Frauen mit Schwerbehinderung gebeten.

Meine datenschutzrechtliche Prüfung hat ergeben, daß die vorgesehene Übermittlung der von dem Forschungsinstitut gewünschten Angaben mit den Vorschriften über den Sozialdatenschutz nicht in Einklang gestanden hätte. Zwar dürfen nach § 75 SGB X Sozialdaten unter bestimmten Voraussetzungen für wissenschaftliche Forschungen im Sozialbereich weitergegeben werden. Diese Voraussetzungen waren im konkreten Fall allerdings nicht erfüllt, weil es möglich war, den Zweck der Forschung auf andere Weise zu erreichen (§ 75 Abs. 1 Satz 2 SGB X).

Die relativ einfache Lösung, die dann auch gewählt wurde, bestand darin, daß das Landesamt für Jugend, Soziales und Versorgung die in Frage kommenden Frauen angeschrieben und gebeten hat, einen von dem Institut entwickelten Fragebogen auszufüllen und an das Institut zu übersenden (sog. "Adreßmittlung").

Das Landesamt für Jugend, Soziales und Versorgung hatte die Problematik von Anfang an ebenso gesehen und die gewünschten Namen der schwerbehinderten Frauen nicht weitergegeben.

Der geschilderte Fall zeigt, daß Forschung und Schutz des informationellen Selbstbestimmungsrechtes keine Gegensätze bilden müssen; gefragt ist in diesem Zusammenhang ein gewisses Nachdenken auch der forschenden Stellen über datensparsame Verarbeitungsabläufe.

12 Schulen

12.1 Überwachung der Schulpflicht

Ein Schulamt hatte die keineswegs abwegige Idee, die Überwachung der Schulpflicht dadurch zu erleichtern, daß regelmäßige Datenübermittlungen über Zuzüge und Wegzüge aller schulpflichtigen Kinder aus dem Melderegister an die Pflichtschulen erbeten wurden. Dieser Bitte sind einige Gemeinden in seinem Zuständigkeitsbereich auch nachgekommen.

Ich mußte aber darauf aufmerksam machen, daß die regelmäßige Datenübermittlung mangels Rechtsgrundlage unzulässig ist. Außer Zweifel steht, daß § 1 Schulpflichtgesetz, in dem die allgemeine Schulpflicht festgelegt ist, nicht eine konkrete, datenschutzrechtliche Ermächtigungsgrundlage für regelmäßige Datenübermittlungen sein kann. Einen entsprechenden Tatbestand gibt es auch in der geltenden Meldedaten-Übermittlungsverordnung (MeldDÜV) nicht. Dort ist in § 7 MeldDÜV lediglich zum 15. Februar eines jeden Jahres die regelmäßige Datenübermittlung zu erstmals schulpflichtig werdenden Kindern zugelassen.

Nach Mitteilung des Schulamts wurde die oberste Schulaufsichtsbehörde mit der Angelegenheit befaßt und von Seiten des Schulamtes eine dahingehende Erweiterung der MeldDÜV empfohlen.

Sollte der Verordnungsgeber sich dem zuwenden, müßte er bedenken:

- Die regelmäßige Übermittlung einer Vielzahl von Daten hat eine andere datenschutzrechtliche Qualität als die Übermittlung in einem Einzelfall. Es werden nämlich bei der empfangenden Stelle Dateien geschaffen, die einer ständigen Datenpflege, z.B. durch Löschungen, Berichtigungen und Sperrungen, bedürfen, die ohne entsprechende Regelungen nicht gewährleistet ist.
- Ob die Errichtung von derart umfassenden Dateien an den Pflichtschulen überhaupt ein geeigneter Weg zur Überwachung der Schulpflicht sein könnte, erscheint mir zweifelhaft, ist aber primär aus fachlicher Sicht zu beurteilen. Dabei wäre zu beachten, daß dies lediglich bei Zuzügen und Wegzügen innerhalb des Saarlandes zur Kontrolle hilfreich sein kann.
- Die weit überwiegende Mehrzahl der schulpflichtigen Kinder erfüllt ihre Schulpflicht, ihre Daten wären aber dennoch in dieser Datei aus Anlaß von Umzügen gespeichert. Insofern stellt sich hier die Frage der Verhältnismäßigkeit einer entsprechenden Regelung.

12.2 Veröffentlichung von Daten ehemaliger Schüler im Internet

Mit einer Vielzahl von eigenen Angeboten und Verweisen im Internet präsentiert sich das "Juristische Internet-Projekt Saarbrücken" des juristischen Fachbereichs der Universität des Saarlandes. Der Lehrstuhl für Bürgerliches Recht, Rechtstheorie und Rechtinformatik, hat mir das "remus"-Projekt (Rechtsfragen von Multimedia und Internet in Schule und Hochschule) vorgestellt. Bund und Länder wollen ein zentrales elektronisches Informationssystem im Internet errichten, das allen Verantwortlichen die Möglichkeit bietet, sich über Rechtsfragen im Zusammenhang mit Multimedia und Internet in Schulen und Hochschulen zu informieren. remus ist eine Projektstudie, die wesentliche Elemente eines derartigen Informationssystems begründet.

remus bietet beispielsweise in einem Diskussionsforum die Möglichkeit, mit anderen Interessierten in Kontakt zu treten und sich über Probleme der Nutzung von Multimedia und Internet auszutauschen.

In diesem Rahmen wollte ein Lehrer wissen, ob und unter welchen Voraussetzungen es zulässig ist, in einer Schulhomepage die e-mail-Adressen von ehemaligen Schülerinnen und Schülern und die Namen und den Wohnort der Schülerinnen und Schüler des jeweiligen Abiturjahrganges abzulegen.

In meiner datenschutzrechtlichen Beurteilung der Anfrage, um die ich wie meine Kollegen gebeten wurde, habe ich auf folgendes hingewiesen:

Die Veröffentlichung von Daten ehemaliger Schülerinnen und Schüler im Internet stellt eine Übermittlung personenbezogener Daten dar, die nur zulässig ist mit Einwilligung der Betroffenen oder wenn eine besondere Rechtsvorschrift die Übermittlung erlaubt. § 8 der "Verordnung über die Erhebung, Verarbeitung und sonstige Nutzung personenbezogener Daten in den Schulen" vom 3. November 1986 erlaubt die Übermittlung von Schülerdaten an Einzelpersonen oder private Einrichtungen nur mit schriftlicher Einwilligung.

Bei Erlaß der Verordnung am 3. November 1986 dachte das Kultusministerium natürlich noch nicht an eine Veröffentlichung im Internet. Um so wichtiger erscheint mir jetzt, daß vor Erteilung einer Einwilligung eine entsprechende Aufklärung über die mit dem Internet verbundenen Risiken einer Manipulation oder zweckfremden Nutzung der gespeicherten Daten erfolgt.

13 Hochschulen

13.1 Novellierung des Universitätsgesetzes und des Fachhochschulgesetzes

Bei der anstehenden Novelle des Hochschulrechts geht es - am Rande - auch um Änderungen der Datenverarbeitung. Gegenüber dem Entwurf des Ministeriums für Bildung, Kultur und Wissenschaft habe ich Änderungen vorgeschlagen:

- In den Entwurf ist erstmals eine Rechtsvorschrift aufgenommen worden, die die personenbezogene Bewertung von Lehrveranstaltungen durch die Studierenden legitimieren soll. Die Studierenden werden verpflichtet, an entsprechenden Befragungsaktionen teilzunehmen. Da für mich fraglich ist, mit welchen Mitteln eine entsprechende Verpflichtung durchgesetzt werden soll, habe ich mich dafür ausgesprochen, daß die Befragung der Studierenden auf freiwilliger Basis erfolgt.
  Auch halte ich es nicht für erforderlich, daß die Studierenden im Rahmen der Beurteilung von Lehrveranstaltungen identifizierende Angaben zu ihrer Person machen. Ich habe deshalb vorgeschlagen, den Gesetzentwurf dahingehend zu ergänzen, daß die Studierenden anonym über Ablauf sowie Art und Weise der Darbietung des Lehrstoffs befragt werden.

- Nach dem Entwurf sollen Personal- und Prüfungsangelegenheiten in den Gremien in nichtöffentlicher Sitzung behandelt werden.
  Ich habe vorgeschlagen, auch Habilitationsleistungen (wie bisher) und Evaluationsberichte, sofern sie personenbezogene Daten beinhalten, ebenfalls in nichtöffentlicher Sitzung zu behandeln. Darüber hinaus halte ich es für erforderlich, die Öffentlichkeit immer dann auszuschließen, wenn berechtigte Interessen Einzelner entgegenstehen.

- In dem Gesetzentwurf fehlt - anders als im geltenden Universitätsgesetz - eine Regelung über die Verschwiegenheitspflicht der Gremienmitglieder. Eine solche habe ich angemahnt.

13.2 Informationsaustausch über abgelehnte Dissertationen

Auf Hinweis meines niedersächsischen Kollegen bin ich der Praxis des Fachbereiches Wirtschaftswissenschaft der Universität des Saarlandes nachgegangen, die Ablehnung einer Dissertation an die Dekanate der wirtschaftswissenschaftlichen Fachbereiche aller Hochschulen in der Bundesrepublik Deutschland mitzuteilen.

Tatsächlich, so wurde mir auf Nachfrage durch die Universität des Saarlandes bestätigt, entspreche dies in der rechts- und wirtschaftswissenschaftlichen Fakultät ständiger Übung. Hintergrund dieser Verfahrensweise seien die Promotionsordnungen, wonach eine Dissertation nur dann angenommen werden könne, wenn sie noch von keiner anderen Hochschule abgelehnt worden sei.

Ich halte dieser Mitteilungspraxis für rechtswidrig, weil eine die Datenübermittlungen rechtfertigende Rechtsgrundlage nicht ersichtlich ist. Auf die Vorschriften des saarländischen Datenschutzgesetzes können die Meldungen nicht gestützt werden, denn es fehlt an der Erforderlichkeit der Datenüber-

mittlungen zur Aufgabenerfüllung der übermittelnden oder der empfangenden Stelle.

Aus anderen Bundesländern ist mir bekannt geworden, daß die dortigen Hochschulen keine entsprechenden Mitteilungen verschicken, weil der Wert derartiger Mitteilungen als gering eingeschätzt wird. Die Erfahrung zeige nämlich, daß es nur wenige Doktoranden gebe, die es nach dem Scheitern ihrer Arbeit anderswo noch einmal versuchten. Sofern dies in Ausnahmefällen doch einmal geschähe, ergebe sich bei den Betreffenden aus der Darstellung ihres wissenschaftlichen Werdeganges für den Doktorvater Aufklärungsbedarf, der zum gleichen Ziel führe wie die fraglichen Mitteilungen.

Auf meine entsprechende Intervention hin hat die rechts- und wirtschaftswissenschaftliche Fakultät die bisher geübte Datenübermittlungspraxis eingestellt.

13.3 Prüfung bei der Hochschule für Technik und Wirtschaft des Saarlandes

Im Berichtszeitraum habe ich eine Datenschutzprüfung bei der Hochschule für Technik und Wirtschaft des Saarlandes (HTW durchgeführt. Die Prüfung konzentrierte sich auf die Bereiche Personalverwaltung, Studentensekretariat und Prüfungsamt sowie auf den Fachbereich Betriebswirtschaft. Mir ging es bei der Prüfung insbesondere darum festzustellen, inwieweit die bereichsspezifischen Vorschriften zur Studentendatenverarbeitung des § 61 Abs. 3 Fachhochschulgesetz in Verbindung mit § 101 a Universitätsgesetz und der Verordnung über die Erhebung, Verarbeitung und Aufbewahrungsdauer personenbezogener Daten an den Hochschulen des Saarlandes bei der Fachhochschule umgesetzt sind.

U.a. wurden folgende Feststellungen getroffen:

- Seit Beginn der automatisierten Datenspeicherung im Jahre 1993 wurde keine Löschung von Daten vorgenommen. Dies widerspricht § 8 der Studentendatenverordnung, der detaillierte Regelungen über die Zeiträume enthält, nach denen Daten zu löschen sind.
- Die Fachhochschule fordert bei Antrag auf Zuteilung eines Studienplatzes unter anderem die Beifügung eines lückenlosen Lebenslaufes.
  Die Anlage zur Studentendatenverordnung regelt in einem Datenkatalog, welche Daten die Hochschulen für die Zulassung zum Studium von den Studienbewerbern erheben dürfen. Der Lebenslauf ist in dem Datenkatalog nicht enthalten. Die Pflicht zur Vorlage eines Lebenslaufes wäre dann unproblematisch, wenn ein Lebenslauf nur die Daten enthielte, die in dem Datenkatalog aufgezählt sind. Meine stichprobenweise Einsicht in Studentenakten hat allerdings ergeben, daß die Lebensläufe regelmäßig dar-

über hinausgehende Angaben wie z.B. Konfession, Namen und Beruf der Eltern oder besondere persönliche Interessen und Fähigkeiten enthielten. Auf die Vorlage eines Lebenslaufes muß daher verzichtet werden.

- Im Rahmen der Zuteilung eines Studienplatzes verlangt die Fachhochschule von den Bewerbern ein ärztliches Attest, in dem bescheinigt wird, daß der Studienbewerber nicht an einer Krankheit leidet, welche die Gesundheit anderer Studenten ernstlich gefährdet. In den Akten habe ich Bescheinigungen mit folgenden Inhalten festgestellt: "Der Bewerber ist frei von ansteckenden oder sonstigen schwerwiegenden Erkrankungen" oder "Störungen der körperlichen oder geistigen Kräfte liegen nicht vor". Diese Formulierungen lassen erkennen, daß den bescheinigenden Ärzten oft nicht klar ist, was Gegenstand ihrer ärztlichen Beurteilung sein soll. Im Rahmen meiner Beteiligung vor Erlaß der Studentendatenverordnung habe ich unter Hinweis auf diese Problematik erreicht, daß die ursprünglich im Entwurf der Verordnung vorgesehene Angabe "Krankheiten, die die Gesundheit anderer Studenten gefährden oder den Studienbetrieb ernstlich beeinträchtigen können" gestrichen wurde. Auf die Vorlage einer ärztlichen Bescheinigung vor Zulassung zum Studium ist daher zu verzichten.
- Im Fachbereich Betriebswirtschaft wird in der dortigen Bibliothek eine Ausfertigung jeder Diplomarbeit vorgehalten. In dieser Diplomarbeit wird die Adresse, nicht aber der Name des Prüflings, geschwärzt. Auf meine Frage nach der Notwendigkeit der Namensangabe in der für die Bibliothek bestimmten Diplomarbeit hat die Fachhochschule eingeräumt, daß für die Bibliothek ein Exemplar ohne Name und Adresse des Prüflings ausreicht.
- Es wurde festgestellt, daß die bei Prüfungsunfähigkeit vorzulegenden amtsärztlichen Atteste überwiegend die Diagnose, die zur Prüfungsunfähigkeit führte, enthielt. Die Fachhochschule hat bestätigt, daß ihr eine Bescheinigung der Prüfungsunfähigkeit (ohne Diagnose) genügen würde. Sie will die Gesundheitsämter darauf hinweisen, daß die Angabe der Diagnose zur Bescheinigung der Prüfungsunfähigkeit in den amtsärztlichen Attesten entbehrlich ist.

Die Fachhochschule will meinen Forderungen insgesamt nachkommen.

14 Öffentlicher Dienst

14.1 Beihilfe und Personalverwaltung

Die Beihilfe ist nach dem neuen Personalaktenrecht von der Personalsachbearbeitung abzuschotten (§ 108 a SBG). Die Beihilfeakte ist von der übrigen

Personalakte getrennt aufzubewahren. Sie soll in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden; Zugang sollen nur Beschäftigte dieser Organisationseinheit haben. Mit dieser Vorschrift soll verhindert werden, daß Angaben aus Beihilfeanträgen, z. B. über Krankheiten und medizinische Behandlungen, bei Personalmaßnahmen verwendet werden können.

Bei Datenschutzprüfungen stellte ich fest, daß diese Regelungen in mehreren Gemeindeverwaltungen sowie bei einzelnen Körperschaften des öffentlichen Rechts im Bereich der Sozialversicherung nicht umgesetzt wurden. Bei diesen Stellen liegen die Bearbeitung von Personalangelegenheiten und der Beihilfe in einer Hand. Die Verwaltungsleitungen legen meist dar, daß die geringe Verwaltungskapazität eine andere organisatorische Lösung innerhalb der Körperschaft nicht zuläßt. Die Verantwortlichen sind sich durchaus bewußt, daß die Zuordnung in ihrer Behörde nicht rechtmäßig ist und daß mit einer Verlagerung der Beihilfeberechnung auf eine andere öffentliche Stelle Alternativen zur Verfügung stehen. Aus Kostengründen - wegen einer gegenwärtig günstigen Altersstruktur der Belegschaft - wurde bisher der Beitritt zur Beihilfe-Umlage-Gemeinschaft der Ruhegehaltskasse des Saarlandes hinausgezögert. Ich werde darauf drängen, daß auch in diesen Fällen eine Lösung gefunden wird, die im Einklang mit dem Gesetz steht.

14.2 Datenschutz beim Personalrat

Datenschutzvorschriften sind für den Personalrat in zweierlei Hinsicht von Bedeutung. Einerseits sind die Datenschutzgesetze Schutzbestimmungen zugunsten der Arbeitnehmer, über deren Einhaltung der Personalrat zu wachen hat (§ 71 Saarländisches Personalvertretungsgesetz - SPersVG). Andererseits erhält der Personalrat bei seiner Tätigkeit, z.B. im Rahmen der Beteiligung bei Einstellungen, Höhergruppierungen, Beförderungen, Versetzungen, Kündigungen, Kenntnis von zahlreichen Personaldaten und muß selbst ihre korrekte Behandlung im Rahmen seiner Arbeit sicherstellen.

Ich habe daher in die Prüfung einer Kreisverwaltung auch die Datenverarbeitung beim Personalrat einbezogen.

Bei diesem Personalrat werden Daten der Beschäftigten in automatisierter Form mit einem von der Dienststelle zur Verfügung gestellten PC verarbeitet. Bei der Größe der Verwaltung mit mehreren Hundert Mitarbeitern bestehen aus Datenschutzsicht keine grundsätzlichen Bedenken, daß der Personalrat die personenbezogenen Daten der Beschäftigten, die er für seine tägliche Arbeit benötigt, automatisiert speichert.

Wenn jedoch der Personalrat darauf angewiesen ist, sich die Daten aus den Unterlagen zusammenzusuchen, die er im Rahmen seiner Beteiligung in Einzelfällen erhalten hat, besteht die Gefahr, daß eine Datei mit unvollständigen

Datensätzen entsteht, deren Richtigkeit und Aktualität nicht gewährleistet ist. Dies halte ich für problematisch. Es sollte vielmehr angestrebt werden, daß die Personalverwaltung der Mitarbeitervertretung einen Bestand von "Grunddaten" der Beschäftigten zur Verfügung stellt, die der Personalrat zu seiner Aufgabenerfüllung ständig benötigt.

Zu den "Grunddaten" gehören aus meiner Sicht Personalnummer, Name, Vorname, Geburtsdatum, Dienst- und Berufsbezeichnung, organisatorische Zugehörigkeit zu Amt, Dezernat usw., Besoldungs-, Vergütungs-, Lohn-, Fallgruppe, Eintrittsdatum, Vollzeit- oder Teilzeitbeschäftigung. Der Datenbestand sollte in regelmäßigen Zeitabständen aktualisiert werden. Eine darüber hinausgehende, dateimäßige Verarbeitung von Personaldaten durch den Personalrat ist zu dessen Aufgabenerfüllung nicht erforderlich; sie ist daher aus datenschutzrechtlicher Sicht als unzulässig anzusehen.

Es wurde festgestellt, daß Vorlagen der Personalverwaltung, z.B. für eine Höhergruppierung, der Einladung zur Personalratssitzung beigefügt und an alle Personalratsmitglieder versandt werden. Eine solche Verfahrensweise ist zur Information der Personalratsmitglieder nicht erforderlich. Die Mitglieder des Personalrates sind nach § 33 Abs. 2 SPersVG unter Mitteilung der Tagesordnung einzuladen. Die Tagesordnung selbst soll ein genaues Bild darüber geben, was zur Beratung und Beschlußfassung in der Sitzung ansteht. Ein Anspruch darauf, daß mit der Tagesordnung weitere Unterlagen übersandt werden, besteht nicht (vgl. BVerwG vom 29.08.75, Az. VII P 2.74). Um eine unnötige Streuung von Personaldaten zu vermeiden, sollte auf die Versendung von Kopien der Verwaltungsvorlagen verzichtet werden.

Unterlagen mit personenbezogenem Inhalt sind (nur) so lange aufzubewahren, wie die Kenntnis der Daten zur Aufgabenerfüllung des Personalrates erforderlich ist. Nach Ablauf der Aufbewahrungsfrist sind die Unterlagen zu vernichten (vgl. § 19 Abs. 3 SDSG). Bei der Prüfung wurden zwar keine Verstöße gegen diese Grundsätze festgestellt. Es ist jedoch nicht konkret geregelt, welche Unterlagen wie lange aufzubewahren sind. Ich habe vorgeschlagen, in der Geschäftsordnung des Personalrates Aufbewahrungsfristen festzulegen. M. E. sollten Vorgänge über die Beteiligung des Personalrates in Einzelfällen (z.B. Höhergruppierung) nicht länger als 1 Jahr, nachdem die Angelegenheit in der Personalratssitzung behandelt wurde, aufbewahrt werden. Unfallanzeigen könnten ebenfalls nach einem Jahr vernichtet werden. Sitzungsniederschriften des Personalrates sollten nicht länger als 1 Jahr nach Ablauf der Amtszeit aufbewahrt werden.

14.3 Führung von Personalakten

Im Rahmen von Datenschutzprüfungen habe ich auch untersucht, wie die Personalakten bei öffentlichen Stellen geführt werden. Die Neuregelung des Personalaktenrechts im Saarländischen Beamtengesetz - SBG - im Jahre

1995 (vgl. auch meinen 16. TB TZ 20.1) ist in einigen Personalverwaltungen offensichtlich noch nicht vollzogen worden. Die Ursache mag auch darin liegen, daß das Ministerium des Innern - im Gegensatz zu den meisten Bundesländern - keine Verwaltungsvorschriften über die Führung von Personalakten erlassen hat. Auch die Zusage, das Rundschreiben vom 24.03.1968 "betreffend Führung der Personalakten" an die neue Rechtslage anzupassen, wurde bisher nicht eingelöst.

Bei meiner stichprobenweisen Durchsicht von Personalakten habe ich vor allem folgendes festgestellt:

- Die Personalakten sind nicht nach sachlichen Gesichtspunkten strukturiert; die Vorgänge werden einfach chronologisch der Reihe nach abgeheftet. So ist es nicht verwunderlich, daß z.B. Unterlagen über Erkrankungen jahrzehntelang aufbewahrt werden, obwohl sie nach § 108 f Abs. 2 SBG bereits nach 5 Jahren auszusondern wären. Die Personalakten sollten zumindest insoweit untergliedert werden, daß eine Aussonderung von Einzelvorgängen nach Ablauf von Aufbewahrungsfristen möglich ist.
- In den Personalakten sind Unterlagen enthalten, die nicht nur Daten der Betroffenen, sondern auch Angaben über Dritte enthalten. Beispiele: Sitzungsniederschriften von kommunalen Gremien über Personalangelegenheiten, Sammelanträge über Höhergruppierungen, Verwaltungsverfügungen über Einstellungen, Umsetzungen und Beförderungen, Listen über Dienstjubiläen, Teilnehmerlisten von Fortbildungsveranstaltungen, Berufungslisten von Professoren einer Hochschule mit Angabe der jeweiligen Abstimmungsergebnisse des zuständigen Gremiums. Die Personalakte sollte nur Angaben über den betroffenen Bediensteten enthalten. So sollten z.B. bei Niederschriften über Sitzungen, in denen Personalangelegenheiten mehrerer Beschäftigter behandelt wurden, Auszüge für die einzelnen Personalakten gefertigt werden. Damit soll insbesondere vermieden werden, daß der Beschäftigte bei der Einsicht in seine Personalakte Informationen über Dritte zur Kenntnis nehmen kann.
- Personalnebenakten sind häufig ein Spiegelbild der eigentlichen Personalakte. Alle personalrechtlichen Vorgänge werden kopiert und auch in der Nebenakte aufbewahrt. Fotokopien aller Bewerbungsunterlagen (Lebenslauf, Schul- und Arbeitgeberzeugnisse usw.), auch wenn die Einstellung Jahrzehnte zurücklag, haben wir ebenso in Personalnebenakten vorgefunden wie Kopien von Lohnsteuerkarten, von alten Ortszuschlagserklärungen oder alten Bescheiden über Umzugskostenentschädigungen. Nach § 108 Abs. 2 SBG können zwar Nebenakten (Unterlagen, die sich auch in der Grundakte oder in Teilakten befinden) geführt werden, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist. Sie

dürfen jedoch nur solche Unterlagen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerledigung der betreffenden Behörde erforderlich ist.

- Die festgelegten Aufbewahrungsfristen (§ 108 f SBG), nach deren Ablauf bestimmte Personalaktenteile zu vernichten sind, werden vielfach nicht beachtet.

14.4 Landeseinheitliche Personalausfall-Statistik

Pläne des Bundesinnenministers, mit verstärkten Kontrollen und Krankenbesuchen die Ausfallquote im öffentlichen Dienst zu senken, verursachten bundesweit Schlagzeilen in der Presse. Diese Meldungen haben sicherlich dazu beigetragen, daß das Vorhaben, in der Landesverwaltung eine einheitliche Personalausfallstatistik einzuführen, von der Personalvertretung besonders kritisch aufgenommen wurde.

Die Fehlzeiten von Bediensteten wegen Urlaub, Krankheit oder aus sonstigen Anlässen werden schon immer von den Personalstellen für Zwecke der Personalverwaltung und der Dienstaufsicht erfaßt. Die Verarbeitung der Daten mit einer Kartei oder mit einem automatisierten Verfahren ist - soweit erforderlich - datenschutzrechtlich zulässig (§ 29 SDSG, § 108 g SBG - Saarländisches Beamtengesetz).

Nunmehr werden die in jedem Ressort verfügbaren Daten eines jeden Mitarbeiters nach einheitlichem Muster zu einer Personalausfall-Statistik zusammengefaßt. Mit dieser Zusammenfassung auf der Ebene eines Ressorts oder eines Landesamtes verlieren die Daten ihren Personenbezug. Es ist dem Statistikblatt nicht mehr zu entnehmen, welcher einzelne Bedienstete z. B. wegen Krankheit wie lange dem Dienst ferngeblieben ist.

Das datenschutzrechtliche Interesse konzentriert sich deshalb darauf, was mit den personenbezogenen Einzeldaten bis zur Aggregierung geschieht. Dabei ist vor allem von Bedeutung, daß

- nur die Daten gespeichert werden, die für Personalverwaltungszwecke unerläßlich sind,
- Auswertungen des automatisierten Datenbestandes nur vorgenommen werden, soweit dies zur Aufgabenerfüllung erforderlich und mit der Personalvertretung vereinbart ist,
- die Daten nach Ablauf der Frist gelöscht werden (nach § 108 f SBG 5 Jahre; eher, wenn Zwischenergebnisse in der Personalakte aufbewahrt werden),
- Art und Umfang der automatisierten Verarbeitung für die Mitarbeiter transparent ist; dabei sind die Informationspflichten nach § 108 g Abs. 5 SBG zu beachten.

14.5 Mitarbeiterdaten im Internet und in internen Kommunikationsnetzen

Immer mehr öffentliche Stellen im Saarland - vor allem Hochschulen, Regierung, Kammern, Gemeinden und Landkreise - stellen sich und ihre Dienstleistungen in Datennetzen wie dem Internet dar (vgl. TZ 3.4). Häufig werden in den Internet-Angeboten Organisationsübersichten mit den Namen von Mitarbeitern als Ansprechpartner für Bürger und Firmen genannt; teilweise werden darüber hinaus recht umfassende Geschäftsverteilungspläne von Behörden mit den Aufgabenbeschreibungen aller Beschäftigten dargestellt.

In der Diskussion werden diese Veröffentlichungen im Internet oft lediglich als Weiterentwicklung der bisherigen Praxis des Austausches von Organisationsplänen und Telefonverzeichnissen mit Hilfe eines modernen Mediums verstanden. Tatsächlich ist jedoch die Verteilung solcher Papierausdrucke an Stellen, mit denen regelmäßig dienstliche Kontakte bestehen, oder die Veröffentlichung in lokalen Blättern nicht vergleichbar mit der Bereitstellung von Daten in einem öffentlichen, weltweit unbeschränkt zugänglichem Datennetz.

Wie ist die Veröffentlichung von Mitarbeiterdaten datenschutzrechtlich zu beurteilen?

Für die Verarbeitung von Beschäftigtendaten ist § 29 SDSG maßgebend. Die Veröffentlichung von Personaldaten stellt eine Datenübermittlung an private Dritte dar, die nur zulässig ist, wenn der Betroffene eingewilligt hat, der Empfänger ein rechtliches Interesse glaubhaft macht oder der Dienstverkehr es erfordert. Für den Dienstverkehr wird oft ausreichen, die jeweils anzusprechende Organisationseinheit in ihrer Funktion zu bezeichnen und ihre Kommunikationsadresse (Telefon, Fax) anzugeben. Auf die Angabe personenbezogener Mitarbeiterdaten wird weitgehend verzichtet werden können.

Eine namentliche Bezeichnung von Mitarbeitern kann bei Veröffentlichungen von Organisationsplänen oder ähnlichen Verzeichnissen in Papierform je nach Aufgabenstellung der öffentlichen Stelle für den Dienstverkehr als erforderlich angesehen werden, wenn diese Mitarbeiter im Rahmen ihrer Zuständigkeit häufig in Kontakt mit Bürgern oder Firmen stehen. Somit sollte sich die Veröffentlichung von personenbezogenen Angaben in Printmedien auf besondere Funktionsträger und solche Mitarbeiter beschränken, die Bürgern und Firmen als "Ansprechpartner" zur Verfügung stehen. Außerhalb der örtlichen Zuständigkeit erscheint eine unmittelbare Kontaktaufnahme allenfalls mit einem kleinen Kreis von Repräsentanten geboten; die Veröffentlichung von Daten anderer Mitarbeiter in überregionalen Publikationen sollte nur mit Einwilligung der Betroffenen erfolgen.

Erst recht gilt dies für die Einstellung von Mitarbeiterdaten in das Internet oder sonstige öffentlich zugänglichen Netze, die aufgrund der leichten Ver-

knüpfungsmöglichkeiten und Manipulierbarkeit mit zusätzlichen Risiken für das informationelle Selbstbestimmungsrecht verbunden sind. In Internet-Angebote aufgenommene Namen und Begriffe können mit Suchprogrammen aufgefunden und - losgelöst von dem Zweck der einzelnen Veröffentlichung - miteinander verknüpft werden. Ein Mitarbeiter einer Behörde, der an seinem Heimatort politisch im Gemeinderat tätig und eventuell noch Vorstandsmitglied eines Vereins ist, sollte sich darüber im Klaren sein, daß diese Informationen, wenn sie im Internet eingestellt sind, zusammengefaßt abrufbar sind, obwohl er vielleicht nicht wünscht, daß seine dienstliche, ehrenamtliche und politische Tätigkeit "in einen Topf geworfen wird".

Die Abwägung zwischen Betroffenenrechten und dem dienstlichen Erfordernis führt dazu, die Nutzung gerade dieses Mediums grundsätzlich nur mit Einwilligung als zulässig anzusehen. Im Hochschulbereich, in dem Vorlesungs- und Institutionenverzeichnisse sich auch an Interessenten aus anderen Ländern richten, ist das dienstliche Erfordernis anders zu beurteilen als bei sonstigen öffentlichen Stellen. Soll eine Einwilligungserklärung eingeholt werden, sind die Mitarbeiter vorher über die mit der Aufnahme ihrer Daten in das Internet verbundenen Risiken aufzuklären.

Eine Veröffentlichung von Mitarbeiterdaten in einem verwaltungsinternen Datennetz ist dagegen weniger problematisch. Ein Landkreis hat ein - auf seine eigene interne Kommunikation beschränktes - Intranet entwickelt, das den Informationsfluß innerhalb der Krei verwaltung verbessern soll. Soweit personenbezogene Angaben über Mitarbeiter aufgenommen werden, die üblicherweise auch in Organisationsplänen oder Telefonverzeichnissen enthalten sind, besteht hierfür im SDSG eine Rechtsgrundlage. Die Veröffentlichung eines Fotos, des Alters oder von Hobbys der Mitarbeiter halte ich jedoch nur mit ausdrücklicher Einwilligung der Betroffenen für zulässig.

14.6 Personalverwaltungssystem beim Ministerium des Innern

Für die Personal- und Stellenbewirtschaftung setzt das Ministerium des Innern seit 1998 ein von einem anderen Bundesland übernommenes PC-Verfahren ein. Das hierfür auf der Basis der IT-Sicherheitsrichtlinie (Gemeinsames Ministerialblatt Saar 1997, Seite 74) erstellte Sicherheitskonzept und eine Dienstanweisung wurden im Verlauf des Freigabeverfahrens aus datenschutzrechtlicher Sicht weiter verbessert.

Dabei habe ich mich zunächst gegen die Einschätzung bei der Feststellung des Schutzbedarfs gewandt, daß bei mißbräuchlicher Erhebung oder Nutzung der Personaldaten (nur) geringe Beeinträchtigungen des informationellen Selbstbestimmungsrechts, keine psychischen Schäden der Betroffenen und keine Beeinträchtigungen für die Aufgabenerfüllung zu erwarten seien. Der Schutzbedarf wurde nur als "niedrig bis mittel'" eingestuft, weil es

sich "nicht um besonders schutzbedürftige Daten" handele, deren Mißbrauch "nur zu geringen materiellen und immateriellen Schäden" führe.

Tatsächlich handelt sich bei den zu verarbeitenden Daten, die den wesentlichen Inhalt der Personalakten widerspiegeln, nach allgemeiner Anschauung um besonders schutzbedürftige und vertraulich zu behandelnde Daten. Immerhin sollen sensible Daten wie Schwerbehinderung, Beurteilungen, Prüfungsergebnisse, Schulabschluß, Nebentätigkeiten, Abwesenheitsgründe, gespeichert werden. Deren unbefugte Verarbeitung, durch die z.B. Personaldaten bekannt werden, kann durchaus erhebliche Auswirkungen auf die berufliche und gesellschaftliche Stellung der betroffenen Bediensteten, ihr Ansehen in der Behörde und in der Öffentlichkeit haben und sie psychisch erheblich belasten. Bei besonders schutzbedürftigen Personaldaten, wie sie auch im vorliegenden Falle gespeichert werden sollen, ist von einem hohen Schutzbedarf auszugehen.

Der Umfang der gespeicherten Daten wurde reduziert. So ist z.B. bei Schwerbehinderten die Speicherung des genauen Prozentsatzes der Behinderung in einem automatisierten System nicht erforderlich. Für die Führung des Verzeichnisses nach § 13 Schwerbehindertengesetz genügen - jedenfalls nach dem Listenvordruck der Arbeitsverwaltung - die Angaben SB/GL (= schwerbehindert/gleichgestellt).

Standardauswertungen des Datenbestandes sind in der Dienstanweisung aufgelistet. Weitergehende Auswertungen dürfen nur nach schriftlicher Anordnung des Personalreferenten und Beteiligung der Personalvertretung vorgenommen werden.

Entgegen den ursprünglichen Vorstellungen des Ministeriums werden die Daten nicht erst nach Ablauf der in § 108 f SGB für Personalakten maßgebenden, teilweise Jahrzehnte währenden Fristen im System gelöscht. Nunmehr soll jährlich einmal geprüft werden, welche Daten nicht mehr für das Verfahren erforderlich sind und gelöscht werden können.

14.7 Telefondatenerfassung

Mehrere Eingaben von Beschäftigten sowie meine Prüfergebnisse bei Gemeinden und einem Sozialversicherungsträger zeigen, daß die Verarbeitung der automatisiert erfaßten Daten über dienstliche und private Telefongespräche häufig nicht den Anforderungen entspricht. Die wesentlichen Mängel sind zusammengefaßt:

- Fehlende Dokumentation des Verfahrens
  Oft sind weder in einer Dienstvereinbarung mit dem Personalrat noch auf sonstige Weise die Einzelheiten der Telefondatenerfassung schriftlich festgelegt. Eine schriftliche Dokumentation des Verfahrens ist jedoch Voraussetzung jeder ordnungsmäßigen Verarbeitung personenbezogener

Daten. Bei der Telefondatenerfassung erfordert auch die Sicherung des Fernsprechgeheimnisses (§ 85 Telekommunikationsgesetz) und die Transparenz der Datenverarbeitung gegenüber dem Personal und dem Personalrat, daß schriftlich u.a. festgelegt wird, welche Daten erfaßt werden, welcher Personenkreis von der Erfassung ausgenommen wird (z.B. Personalrat, Erziehungsberater), welche Auswertungsausdrucke erlaubt sind, wie die Abrechnung der Privatgespräche zu erfolgen hat, unter welchen Voraussetzungen die Aufzeichnung der Dienstgespräche kontrolliert wird sowie nach welchen Fristen die Daten gelöscht und die Ausdrucke vernichtet werden.

- Fehlende Unterscheidung von Dienst- und Privatgesprächen
  Häufig wird den Mitarbeitern der Einfachheit halber gestattet, notwendige Privatgespräche vom Dienstapparat ohne Gebührenabrechnung zu führen. Die Pflicht, eine sparsame und wirtschaftliche Nutzung bereitgestellter Kapazitäten durchzusetzen, kann keineswegs stets über die Verpflichtung des Gesetzgebers gestellt werden, die Persönlichkeitsrechte der Mitarbeiter zu achten. Soweit nicht erkennbar Anlaß für Überprüfungen besteht, sollte in diesen Fällen die Behörde vielmehr zur Wahrung des Fernmeldegeheimnisses auf die Kontrolle der gespeicherten Daten (mit den Angaben über Privatgespräche) verzichten. Will die Behörde sich die Kontrolle der Gesprächsdaten (Dienstgespräche) vorbehalten oder sollen die Gebühren für Privatgespräche gesondert abgerechnet werden, muß konsequenterweise die technische Möglichkeit eingeräumt werden, die beiden Gesprächsarten durch Vorwahl einer bestimmten Ziffer zu kennzeichnen.

- Keine rechtzeitige Löschung
  Bei Prüfungen wurde festgestellt, daß die Gesprächsdaten teilweise jahrelang im automatisierten System gespeichert bleiben. Dies verstößt gegen die Pflicht zur Löschung nach § 19 Abs. 3 SDSG. Regelmäßig können die Daten nach der Auswertung und dem Listenausdruck gelöscht werden.

14.8 Weitergabe einer Personalliste an eine Privatfirma

Bei der in Aussicht genommenen Übertragung von Aufgaben einer öffentlichen Stelle auf einen privaten Betreiber gingen die Beteiligten davon aus, daß die bisher mit der Tätigkeit befaßten Mitarbeiter jedenfalls zu einem erheblichen Teil zum neuen Arbeitgeber wechseln. Nur dann hätte dieser kurzfristig über entsprechend qualifiziertes Personal verfügt und wäre auf Seiten des Landes die erhoffte Kostenentlasung im Personalsektor eingetreten.

Im zuständigen Ministerium hat man deswegen Überlegungen zu verschiedenen Modellen eines Wechsels der betreffenden Mitarbeiter angestellt (individualrechtliche Übernahme; Dienstleistungsüberlassungsvertrag; Beurlau-

bung aus dem öffentlichen Dienst; Zuweisung an einen "Nichtdienstherm" bzw. an eine Einrichtung außerhalb des räumlichen Geltungsbereiches des BAT). In diesem Zusammenhang hat das Ministerium eine Liste von Mitarbeitern der bisherigen Stelle mit Name, Vorname, Dienstbezeichnung, Geburtsdatum und Eintrittsdatum in den öffentlichen Dienst dem Personalbüro der privaten Firma zur Verfügung gestellt.

Nach Prüfung der Rechtslage, um die mich der zuständige Personalrat gebeten hatte, bin ich zu dem Ergebnis gekommen, daß die Datenübermittlung in dieser Form und in diesem Umfang unzulässig war.

Ich verkenne nicht, daß für die Beurteilung von tatsächlicher Möglichkeit und Wirtschaftlichkeit der beabsichtigten Maßnahme gleichermaßen für Dienststelle und potentiellem Übernehmer nötig ist, möglichst präzise die Einzelauswirkungen eines Wechsels auf das jeweilige Dienst- oder Arbeitsverhältnis zu kennen, und daß nur auf dieser Grundlage konkrete Gespräche der im Grundsatz hierzu bereiten Bedienstete mit dem künftigen Arbeitgeber sinnvoll sind.

Allerdings sind die bereichsspezifischen Vorschriften, die die Verarbeitung der Daten von Angestellten im öffentlichen Dienst und Beamten regeln, zu beachten.

Der für die Angestellten im öffentlichen Dienst geltende § 29 Abs. 1 Satz 3 SDSG bestimmt ausdrücklich, daß die Datenübermittlung an einen künftigen Arbeitgeber nur mit Einwilligung des Betroffenen zulässig ist.

Nach § 108d Abs. 1 Saarländisches Beamtengesetz ist die Vorlage der Personalakte oder die Erteilung von Auskünften aus der Personalakte ohne Einwilligung des Beamten nur zulässig an die oberste Dienstbehörde oder eine im Rahmen der Dienstaufsicht weisungsbefugte Behörde für Zwecke der Personalverwaltung oder Personalwirtschaft. Das Gleiche gilt für Behörden desselben Geschäftsbereichs, soweit die Vorlage zur Vorbereitung oder Durchführung einer Personalentscheidung notwendig ist, sowie für Behörden eines anderen Geschäftsbereichs desselben Dienstherrn, soweit diese an einer Personalentscheidung mitzuwirken haben (§ 108 Abs. 1 Satz 2 SBG).

An Dritte, dazu gehören private Arbeitgeber, dürfen Auskünfte grundsätzlich nur mit Einwilligung des Beamten erteilt werden (§ 108d Abs. 2 Satz 1 SBG).

Soweit die Vertragsmodelle auf ein individuelles neues Beschäftigungsverhältnis gerichtet waren, hätte deshalb vor konkreten Gesprächen die Einwilligung zur Weitergabe der Daten eingeholt werden müssen.

Soweit andere Modelle zulässig sind, die vom Fortbestand des bestehenden Dienst- bzw. Arbeitsverhältnis ausgehen, hätte es ohne Einwilligung zu diesem Zeitpunkt nicht sämtlicher übermittelten Daten bedurft, um für den Fall des Erfordernisses eines derartigen Modells die Auswirkungen zu besprechen.

Das zuständige Ministerium, dem ich meine Bewertung zugeleitet habe, hat zugesichert, daß zukünftig keine personenbezogenen Daten der Mitarbeiter des Geschäftsbereichs des Ministeriums ohne deren Einwilligung an Private weitergegeben werden.

15 Steuern

15.1 Überprüfung bei einem Finanzamt

Bei einem Finanzamt habe ich technisch-organisatorische und allgemeine Fragen der Datenverarbeitung sowie die Möglichkeiten überprüft, in welcher Weise bei steuerlichen Verfahren den einzelnen Bediensteten Verarbeitungsrechte eingeräumt werden.

Dabei wurde folgendes festgestellt:

- Der Serverraum war nicht verschließbar und somit der Zugang durch Unbefugte jederzeit möglich.
- Die Anmeldung zum Großrechner erfolgte mit einem zu kurzen Paßwort, obwohl die vorläufige Dienstanweisung für IT-gestützte Arbeitsplätze bei den Finanzämtern (DA-IT) eine Mindestlänge von 6 Zeichen vorschreibt.
- Die im Finanzamt installierten unvernetzten PC waren nicht durch eine geeignete Sicherungssoftware abgesichert.
- Der Zugang zu den im Außendienst eingesetzten Laptop war ohne Eingabe eines Paßwortes möglich und die auf dem Laptop befindlichen Daten waren entgegen der Vorschriften der DA-IT nicht verschlüsselt.
- Die Funktionstrennung zwischen Systembetreuer und Anwender war nicht gewährleistet.

Die Beseitigung dieser Mängel wurde zugesagt.

Die Rechtevergabe auf steuerliche Verfahren erfolgte in dem Amt regelmäßig auf mündliche Anweisung der Geschäftsstelle; ein Kontrollausdruck wurde nicht erstellt. Eine Überprüfung, wem wann welche Rechte durch wen zugeteilt wurden, war dadurch nicht möglich. Ich habe eine schriftliche Anweisung, in der neben den Verfahrensfragen auch der Kontrollausdruck sowie die stichprobenweise Überprüfung geregelt ist, gefordert. Ob die durch die Oberfinanzdirektion angekündigte Anweisung zwischenzeitlich erlassen wurde, entzieht sich meiner Kenntnis.

Bei der Einräumung der Zugangsrechte auf die Mitarbeiter eines Finanzamtes ist insbesondere auch von datenschutzrechtlicher Bedeutung, ob der Datenzugriff auf die Steuerbürger des Amtes begrenzt ist oder finanz-

amtsübergreifend oder gar landesweit eingerichtet ist. Eine über den Zuständigkeitsbereich hinausreichende Zugriffmöglichkeit tangiert das Steuergeheimnis; auch § 30 AO setzt für die Offenbarung von Steuerdaten Erforderlichkeit und Angemessenheit voraus. Dies erfordert die Prüfung, ob aufgrund der zu erwartenden Fallzahlen und der Eilbedürftigkeit überhaupt erforderlich ist, ein automatisiertes Abrufverfahren einzurichten. Soweit dies nicht gegeben ist, erscheint eine herkömmliche telefonische oder schriftliche Anfrage durchaus zumutbar. Der finanzamtsübergreifende Zugriff setzt darüber hinaus technische und organisatorische Vorkehrungen voraus, um die nachträgliche Feststellung zu ermöglichen, wer, welche Daten abgerufen hat (Protokollierung), sowie deren jedenfalls stichprobenweise Überprüfung.

Ohnehin fehlt für Abrufe durch nicht unmittelbar mit der jeweiligen Sachbearbeitung befaßte Bedienstete eine zureichende gesetzliche Grundlage für die mit dem Abruf verbundene Übermittlung personenbezogener Daten. Zwar enthält § 30 Abs. 6 AO eine allgemeine Befugnis für den Abruf; die zur näheren Ausgestaltung vorgesehene Rechtsverordnung insbesondere über die Art der Daten, deren Abruf zulässig ist, sowie über den Kreis der Amtsträger, die zum Abruf solcher Daten berechtigt sind, ist jedoch bisher nicht ergangen. An deren Stelle ist eine Verwaltungsvorschrift (Steuerdaten-Abruf-Verwaltungsregelung) erlassen worden. Diese kann jedoch keinen Ersatz für die fehlende Rechtsverordnung darstellen.

Unabhängig davon sieht selbst die Verwaltungsregelung zur nachträglichen Kontrolle der Rechtmäßigkeit der Abrufe umfangreiche Protokollierungen und stichprobenweise Überprüfungen vor. Auch bezüglich des Zugriffs der Aufsichtsbehörden enthält sie Bestimmungen.

Ich halte es deshalb für unverzichtbar, daß - anstelle einer Verwaltungsregelung - die noch ausstehende Rechtsverordnung erlassen wird; Entwürfe hierfür gab es schon vor mehr als 10 Jahren. Bis dahin hat die Finanzverwaltung zumindest die Regelungen der Verwaltungsvorschrift zu beachten.

15.2 Auskunft über Freistellungsaufträge

Steuern auf Zinserträge werden nicht bereits von den Kreditinstituten berechnet und abgeführt, wenn ihnen - im Rahmen der Freibeträge - entsprechende Freistellungsaufträge erteilt worden sind. Dabei verlieren die Sparer gelegentlich den Überblick über die an verschiedene Kreditinstitute erteilten Aufträge und möchten - möglichst an zentraler Stelle - hierüber Kenntnis erlangen. Der durch das Zinsabschlagsgesetz eingefügte § 45 d Einkommensteuergesetz erlaubt dem Bundesamt für Finanzen, die Daten von Freistellungsaufträgen von den Kreditinstituten zu verlangen. Dadurch können die Daten von verschiedenen Instituten beim Bundesamt zusammengeführt und einer Kontrolle z.B. auf Überschreitung des zustehenden Freibetrages unterzogen werden.

Die Betroffenen haben nach § 19 Bundesdatenschutzgesetz ein Recht auf Auskunft über die beim Bundesamt gespeicherten Daten. In einem Erlaß verweigerte das Bundesministerium der Finanzen aber die Erfüllung dieses Anspruchs. Deshalb haben der Bundesbeauftragte für Datenschutz und die Landesbeauftragten für Datenschutz in ihrer Entschließung vom 5./6.10.1998 eine Aufhebung des Erlasses gefordert, um den gesetzlich zustehenden Anspruch des Betroffenen auf Auskunft zu gewährleisten (Anlage 19.15).

15.3 Außenprüfungen in Arztpraxen

Beim selbständigen Betrieb medizinischer Berufe folgen steuerlich relevante Umstände u.a. aus den Rechtsbeziehungen zu ihren Patienten. Für die Besteuerung einer derartigen Praxis stellt sich damit die Frage nach der Reichweite des Patientengeheimnisses, denn nach § 102 Abs. 1 Nr. 3 c AO können Ärzte, Zahnärzte, Apotheker und Hebammen über das, was ihnen in dieser Eigenschaft anvertraut worden oder bekannt geworden ist, die Auskunft verweigern.

Nach Auffassung der Finanzverwaltung sollen bei berechtigten Zweifeln an der Ordnungsmäßigkeit der Aufzeichnungen eines Arztes auch personenbezogene Patientenunterlagen mit Namensangabe in die Außenprüfung einbezogen werden. Der Bundesbeauftragte für den Datenschutz und die Landesbeauftragten sowie führende Kommentatoren (z.B. Tipke/Kruse, Hübschmann/Hepp/Spitaler) vertreten demgegenüber die Ansicht, dem Auskunftsverweigerungsrecht nach § 102 Abs. 1 Nr. 3 c AO unterliegen (ebenso wie der ärztlichen Schweigepflicht nach § 203 Abs. 1 Nr. 1 StGB) alle dem Arzt in Ausübung seines Berufs bekannt gewordenen Daten, einschließlich des Patientennamens.

Gesetzlich gleich gelagert ist der Fall, in dem für die steuerliche Anerkennung beruflich bedingter Fahrten in einem Fahrtenbuch die Angabe von Namen und Anschrift der Patienten verlangt wird. Die auch hier abweichende Meinung der Finanzverwaltung führte zwischenzeitlich dazu, daß der Bundesbeauftragte für den Datenschutz die Verfahrensweise der Finanzverwaltung formell beanstandet hat.

15.4 Aufbewahrung von Prüfungsakten zu nicht bestandenen Prüfungen

Die Steuerberaterkammer des Saarlandes hat mir die Frage gestellt, ob Prüfungsakten nach bestands- bzw. rechtskräftiger Feststellung des Nichtbestehens der Prüfung weiterhin unbefristet aufzubewahren sind. Zur Begründung hierfür wurde vorgetragen, daß wirksame Vorkehrungen gegen einen (nicht zulässigen) vierten Versuch zur Ablegung der Prüfung getroffen wer-

den müssen. Diese Problematik dürfte sich auch bei anderen Prüfungsstellen ergeben.

Die nur abstrakte Möglichkeit eines (unrechtmäßigen) vierten Versuches zur Ablegung der Prüfung bietet nach meiner Überzeugung keine hinreichende Rechtfertigung für die Aufbewahrung; generell mit einem Täuschungsversuch zu rechnen, wäre unangebracht. Eine Aufbewahrung über die in den Prüfungsordnungen festgelegten Fristen hinaus, ist - im Gegensatz zu den Fällen, in denen die Prüfung noch wiederholt werden kann - zur Aufgabenerfüllung nicht mehr erforderlich. Die Akten sind nach Ablauf der vorgesehenen Aufbewahrungsfristen zu vernichten.

15.5 Veröffentlichung von Verurteilungen und Unterlassungserklärungen durch die Steuerberaterkammer

Mehrere Eingaben befaßten sich mit der Zulässigkeit von Veröffentlichungen von personenbezogenen Daten bei Verurteilungen und strafrechtlichen Unterlassungserklärungen. Jedenfalls in einzelnen Kammerbereichen in der Bundesrepublik sei üblich, in den entsprechenden Mitteilungsschriften der Steuerberaterkammern solche Hinweise zu verbreiten. Auf meine Anfrage teilte mir die Steuerberaterkammer des Saarlandes mit, daß derartige Veröffentlichungen bisher in den Kammermitteilungen nicht vorgenommen wurden. Hiervon habe ich mich bei einer Überprüfung "vor Ort" überzeugen können, die ich aufgrund weiterer Eingaben bei der Steuerberaterkammer vorgenommen habe.

16 Statistik

16.1 Europaweiter Zensus im Jahre 2001

Nach einem Vorschlag der Europäischen Union soll im Jahre 2001 eine gemeinschaftsweite Volkszählung (Zensus) durchgeführt werden. Um den Kostenaufwand, wie er etwa aus der Volkszählung 1987 bekannt ist, im Jahre 2001 geringer zu halten, haben Bund und Länder Modelle erarbeitet, nach denen die Ergebnisse überwiegend aus bereits vorhandenen Daten in Verwaltungsregistern gewonnen werden könnten.

Das Melderegister stellt in diesem Zusammenhang das wichtigste Instrument für eine zukünftige Volkszählung dar, das aber ausreichend zuverlässig sein muß. Es hat sich daher die Frage gestellt, inwiefern sich seine Qualität durch Datenübermittlungen anderer Behörden verbessern läßt und ob hierfür zusätzliche Rechtsgrundlagen im Melderecht geschaffen werden müssen oder das vorhandene Recht ausreicht.

Das Ministerium des Innern hat in einem Erlaß an die Meldebehörden Wege aufgezeigt, wie schon heute Verbesserungen in der Qualität der Melderegister erzielt werden können. Es stützt diese sowohl auf allgemeines Datenschutzrecht als auch auf Melderecht. Die dort vertretene Rechtsauffassung teile ich.

Im Erlaß wird allerdings zu Recht auch betont, daß spezialgesetzliche Bestimmungen (z.B. für Sozial- oder Jugendämter) Datenübermittlungen an Meldebehörden ausschließen können. Im Jahre 1999 sei zudem eine Evaluierung der Verbesserungsmaßnahmen vorgesehen. Danach ist m.E. auch zu entscheiden, ob zur Erreichung des Ziels der Volkszählung neue Rechtsgrundlagen zu schaffen wären, die selbstverständlich datenschutzrechtlichen Anforderungen genügen müssen.

17 Rundfunk und Medien, Telekommunikation

Die technische Weiterentwicklung von Rundfunk und Fernsehen ermöglicht individuellere Nutzungen als früher; gerade diese individuelle Nutzung erzeugt aber an verschiedenen Stellen "Spuren", die neue datenschutzrechtliche Gefahren bergen. Insbesondere dürfen Möglichkeiten. die Vermittlung und Abrechnung von Sendungen auf einzelne Kunden auszurichten, nicht ohne deren Willen dazu verwendet werden, individuelle Vorlieben und Gewohnheiten zu registrieren und damit Mediennutzungsprofile zu erstellen.

17.1 Neues Multimediarecht

Mitte 1997 haben Bund und Länder mit einer Reihe von Normen (Teledienstegesetz, Teledienstedatenschutzgesetz, Mediendienste-Staatsvertrag, Gesetz über die digitale Signatur) ein neues Multimedia-Recht in Kraft gesetzt; auf die Entstehung der Normen, die mit teilweise übereinstimmenden Schranken die Gefahren für Bürgerinnen und Bürger einzudämmen versuchen, bin ich bereits im letzten Bericht eingegangen (TZ 21.3 ff). Beispielhaft wird hierbei bereits gesetzlich betont, daß dem Grundsatz der Datenvermeidung bei der Technikentwicklung und deren Anwendung Rechnung zu tragen ist. Auch wenn das deutsche Recht im weltweiten Wettbewerb der Gerätehersteller und Anbieter sowie bei der grenzüberschreitenden Verflechtung der Netze nicht allein ausreichen mag, private und staatliche Stellen an der Ausforschung von Kommunikation und Nutzerverhaltens zu hindern, wurde doch ein Rahmen geschaffen, der international als fortschrittlich gelten darf.

Positiv zu vermerken ist, daß im Gesetzgebungsverfahren dem wiederholt vorgetragenen Wunsch letztlich nicht entsprochen wurde, Sicherheit mit einem Verbot oder einer Reglementierung von Verschlüsselung erreichen zu wollen. Schon weil das Mittel nicht geeignet ist, das angestrebte Ziel zu er-

reichen, kommt nicht in Betracht, dem Bürger geschützte Kommunikation zu verbieten, wie wir es ihm zur Sicherung der Vertraulichkeit gerade raten.

Auch blieben Vorstellungen unberücksichtigt, nach denen Anbieter von Telediensten den Strafverfolgungsbehörden, Sicherheits- und Nachrichtendiensten erheblich weitergehende Auskunftsrechte hätten einräumen müssen, als sie nach geltendem Recht für Zwecke der Gefahrenabwehr und der Strafverfolgung bereits bestehen. Daß die in den neuen - meist digitalen - Kommunikationsmedien vermehrt anfallenden und leicht nutzbaren Datenspuren besonderes Interesse der Sicherheits- und Nachrichtendienste finden, ist verständlich. Zwar haben diese Dienste zur Wahrung legitimer Sicherheitsbelange der Allgemeinheit gesetzlich zugewiesene Befugnisse und müssen in der Lage sein, ihre Aufgaben auch dann zu erfüllen, wenn sich die Bürger der neuen Kommunikationstechniken bedienen; des Zugriffs auf die sog. Bestandsdaten bedarf es hierfür aber nicht. In Abwägung mit dem Grundrecht auf informationelle Selbstbestimmung und auf Informations- und Meinungsfreiheit haben die Datenschutzbeauftragten dagegen mit Entschließung vom 17./18. April 1997 (Anlage 19.3) gemeinsam auf schon ausreichende polizeiliche und strafprozessuale Möglichkeiten verwiesen.

Die Umsetzung des neuen Regelwerks ist allerdings nicht immer einfach, weder für die Anbieter noch für die Bürger, die den erweiterten Schutz und ihre Auskunftsrechte erst erlernen und einfordern müssen. Kompliziert ist es auch für die öffentlichen Stellen: schon das Abgrenzen der einzelnen Verwaltungs- und Kontrollzuständigkeiten untereinander und mit dem Rundfunk- und Telekommunikationsrecht sowie sonstigen Rechtsgebieten erfordert akribische Abstimmung, um die sich mein Berliner Kollege dankenswerterweise bemüht hat.

17.2 Änderung des Landesrundfunkgesetzes

Am 3. Juli 1996 hatte der Landtag in das Landesrundfunkgesetz eine Regelung über "Modellversuche mit neuartigen Rundfunktechniken, Rundfunkdiensten oder rundfunkähnlichen Diensten" eingefügt; in einem vereinfachten Konzessionsverfahren konnte die Landesanstalt für das Rundfunkwesen (jetzt: Landesmedienanstalt) - befristet bis Ende 1998 - die Durchführung von Vorhaben zulassen. Bereits in meinem letzten Bericht (16. TB TZ 21.6) hatte ich darauf hingewiesen, daß weder die möglichen Inhalte der Versuche noch die Schutzvorkehrungen ausreichend im Gesetz bestimmt sind. Die vom Landtag am 14. 10. 1998 beschlossene erneute Änderung beläßt es bezüglich neuartiger Techniken bei dieser unklaren Regelung, die nunmehr sogar unbefristet gelten soll. Mit Umbenennung der "Rundfunkdienste und rundfunkähnlichen Dienste" in "Mediendienste" wird aber konkludent auf die Datenschutzregelung im Mediendienste-Staatsvertrag Bezug genommen.

Die Hoffnung, daß länderübergreifend mit dem geplanten Vierten Rundfunkänderungsstaatsvertrag auch für technikbezogene Vorhaben präziseres Recht gesetzt wird, hat sich bislang nicht erfüllt. Zwar liegt hierfür den Ministerpräsidenten ein Entwurf vor, der diesbezüglich nicht umstrittenen sein soll; der Abschluß des Vertrages scheiterte bisher am Konsens in anderen Fragen. Die Notwendigkeit (und die gegebene Möglichkeit) eines angemessenen Datenschutzes speziell im "digitalen Fernsehen" haben die Datenschutzbeauftragten von Bund und Ländern mit Entschließung vom 19./20. 3. 1998 betont (Anlage 19.10). Es wäre zu bedauern, wenn die Chance zu datenschutzgerechter Technikgestaltung vertan würde, bevor der Markt über die Einführung der Geräte entscheidet.

Im Gesetzgebungsverfahren zur Änderung des Landesrundfunkgesetzes hatte ich mich auch dafür eingesetzt, jedenfalls für den Rundfunkdatenschutz rechtzeitig - vor November 1998 - der Pflicht nachzukommen, das Landesrecht an die EG-Datenschutzrichtlinie anzupassen (vgl. TZ 2.2). Dieser ist - auch soweit er spezielle Vorschriften für den Saarländischen Rundfunk enthält - bisher teilweise im SDSG geregelt; ohnehin läge nahe, den rundfunkspezifischen Datenschutz im Fachgesetz zu normieren.

Das in § 32 Abs. 1 SDSG geregelte Medienprivileg, das von den allgemeinen Datenschutzstandards Abweichungen zuläßt, muß nunmehr enger eingegrenzt werden; Erleichterungen für die Medien sind nur zulässig, soweit "sich dies als notwendig erweist, um das Recht der Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen" (Erwägungsgrund [17] der Richtlinie). Es gibt danach keine Rechtfertigung, den Medien allein technisch-organisatorische Maßnahmen zur Gewährleistung sicherer Datenverarbeitung aufzuerlegen und sie im übrigen von Vorschriften etwa über Haftung, Sanktionen und Rechtsbehelfe freizustellen.

Auch in organisatorischer Hinsicht ist die geltende Regelung über die Datenschutzkontrolle zu überdenken, soweit sie beim Saarländischen Rundfunk insgesamt - also nicht nur für den journalistisch-redaktionellen Bereich, sondern auch für den administrativen und kaufmännischen Sektor - einer eigenständigen (internen) Instanz zugewiesen ist. Art. 28 der EG-Datenschutzrichtlinie fordert Kontrollstellen mit wirksamen Einwirkungsbefugnissen, die ihre Aufgabe "in völliger Unabhängigkeit" wahrnehmen. Auf die in verschiedenen anderen Bundesländern bereits bestehende andere Zuständigkeit und die zur Anpassung an die Richtlinie seitens des Bundesinnenministeriums für die "Deutsche Welle" vorgesehene Regelung habe ich in meiner Stellungnahme verwiesen; der Landtag ist hierauf nicht eingegangen.

17.3 Befreiung von der Rundfunkgebührenpflicht

Unter bestimmten Voraussetzungen ist nach der "Verordnung über die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht" eine Befreiung von den Rundfunkgebühren möglich. So müssen etwa Personen, deren Einkommen eine in der Verordnung festgelegte Höhe nicht überschreitet, keine Rundfunkgebühren bezahlen. Die Befreiung setzt einen Antrag an die zuständige Gemeinde voraus; die Entscheidung über die Rundfunkgebührenbefreiung trifft die Rundfunkanstalt auf Vorschlag der Gemeinde.

Der Saarländische Rundfunk hatte die Gemeinden aufgefordert, die Antragsteller nach dem Vorhandensein eines Kabelanschlusses und eines Kraftfahrzeuges zu befragen und die entsprechenden Angaben in den Befreiungsantrag aufzunehmen. Die Rechtmäßigkeit dieser Datenerhebung wurde von einer Gemeinde bezweifelt.

Der Saarländische Rundfunk begründete die Erhebung der fraglichen Daten damit, daß der Besitz eines Kabelanschlusses oder eines PKW eine Rundfunkgebührenbefreiung ausschließe. Dem lag die Überlegung zugrunde, daß derjenige, der sich einen Kabelanschluß oder ein Kraftfahrzeug leisten könne, auch in der Lage sein müßte, die demgegenüber verhältnismäßig geringen Rundfunkgebühren zu tragen.

Dieser Auffassung konnte ich mich nicht anschließen, denn die vom Saarländischen Rundfunk vorgetragenen Überlegungen haben in der Rundfunkgebührenbefreiungsverordnung keinen Niederschlag gefunden. Maßgebend ist nach dieser Verordnung allein, ob das Einkommen des Antragstellers die maßgebliche Einkommensgrenze überschreitet.

Im Ergebnis verzichtet der Saarländische Rundfunk nunmehr auf die Frage nach einem Kabelanschluß. Nach der Haltereigenschaft hinsichtlich eines PKW wird zukünftig nur gefragt, wenn sich im Einzelfall Anhaltspunkte für die Notwendigkeit dieser Frage ergeben.

17.4 Kontrolle des Jugendschutzes in Mediendiensten durch die länderübergreifende Stelle "jugendschutz.net"

Auf Beschluß der Jugendminister wurde in Mainz eine - nicht rechtsfähige - Zentralstelle eingerichtet, die Unterstützung bei der Kontrolle des Jugendschutzes nach dem Mediendienste-Staatsvertrag (MDStV) leisten soll. Nach einer - bis Ende 1999 verlängerten - Verwaltungsvereinbarung hat sie insbesondere Internet-Angebote auf jugendschutzwidrige Inhalte zu durchsuchen und Anbieter zu bewegen, diese Angebote zu entfernen. Ggf. werden die für das Sitzland zuständigen obersten Landesbehörden unterrichtet bzw. bei Straftatverdacht die zuständige Staatsanwaltschaft eingeschaltet.

Eine derartige Konzentration ist aus Kapazitätsgründen sicherlich vernünftig. Weil dabei Daten des Anbieters und Informationen über seine Abmahnung

automatisiert verarbeitet werden und Übermittlungen an andere Behörden stattfinden, stellte sich die Frage, ob die genannte Vereinbarung eine ausreichende Rechtsgrundlage darstellt und ob die Datenschutzkontrolle auch insoweit durch den LfD Rheinland-Pfalz wahrgenommen werden kann, als Anbieter aus anderen Ländern betroffen sind.

Solange die im engeren Sinn hoheitlichen Anordnungen und die Verfolgung von Ordnungswidrigkeiten unmittelbar den zuständigen Behörden verbleibt, erscheint mir vertretbar, die im wesentlichen vorbereitende Arbeit der Zentralstelle für die nach § 18 Abs. 1 MDStV allgemein für den Jugendschutz zuständigen Stellen auf der derzeitigen Basis zu akzeptieren. Eine förmliche gesetzliche - d.h. staatsvertragliche - Grundlage für die ab 2000 geplante Dauerlösung würde sämtliche Zweifel an ungenügender Legitimation der Stelle zerstreuen.

18 Schlußbemerkung

In der "Informationsgesellschaft" wird auch der Umgang mit personenbezogenen Daten zunehmen, und immer mehr werden hierbei technische Verfahren eingesetzt werden (müssen?). Umfang, Art und Wirkung der Datenverarbeitung sind für den Einzelnen kaum noch zu durchschauen; welche Risiken entstehen und ob sie eingegangen werden können, läßt sich oft nur schwer abschätzen. Bürgerinnen und Bürger dürfen hierbei nicht allein gelassen, aber auch keineswegs bevormundet werden.

Völlig zutreffend führt die Koalitionsvereinbarung zur Bildung der derzeitigen Bundesregierung aus: "Effektiver Datenschutz im öffentlichen und privaten Bereich gehört zu den unverzichtbaren Voraussetzungen für eine demokratische und verantwortbare Informationsgesellschaft."

Zum notwendigen "Service" des Staates hierfür gehört zuvörderst eine Rechtsordnung, die einen Rahmen schafft, der "modernen" Anforderungen genügt. Aus Landessicht ist - neben der Mitwirkung an der Bundesgesetzgebung - in erster Linie die Novelle des Saarländischen Datenschutzgesetzes gefragt.

Im Bereich der Exekutive müssen Ausstattung, Einrichtung der Verfahren und Ausbildung der Mitarbeiter darauf ausgerichtet sein, bei der jeweiligen Sachaufgabe zugleich die Privatsphäre der Betroffenen zu schützen. Die Annahme, dieser Gesetzesauftrag sei nur nachrangig zu erfüllen, ist falsch. Die Verantwortlichkeit der Verwaltungsleitungen und Aufsichtsbehörden sei nochmals betont. Selbstverständlich gilt dies auch bei Versuchen, die Verwaltung zu "verschlanken" oder durch "Outsourcing" den eigenen Aufwand zu verringern.

Die - notwendige - Kontrolle dieses Bemühens ist sachgerecht nur möglich, wenn die dazu erforderlichen Kapazitäten zur Verfügung stehen. Bei rasant

ansteigendem Technikeinsatz auch in der öffentlichen Verwaltung werde ich meiner Aufgabe mit dem derzeitigen Personal nicht in dem nötigen Maß nachkommen können. Der hilfreiche Kenntnis- und Erfahrungsaustausch mit den übrigen Aufsichtsstellen kann den wiederholt beklagten Mangel nicht ausgleichen.

Nach Kräften werde ich mit meinen Mitarbeiterinnen und Mitarbeitern weiterhin auf datenschutzgerechtes Verhalten der öffentlichen Stellen achten und hierbei als Anwalt der Bürger besonders deren Interessen wahrnehmen. Auf ihre Möglichkeit, sich unmittelbar an mich zu wenden, möchte ich nochmals besonders aufmerksam machen. Auch ihnen stehen die Informationen zur Verfügung, die ich in meinem Internet-Angebot (**www.lfd.saarland.de**) bereitgestellt habe oder auf die dort verwiesen wird.

Anlagen

19.1 Beratungen zum StVÄG 1996

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Entwicklung, im Gesetzgebungsverfahren zu einem Strafverfahrensänderungsgesetz 1996, die Gewährleistung der informationellen Selbstbestimmung im Strafverfahren nicht nur nicht zu verbessern, sondern vielmehr bestehende Rechte sogar noch zu beschränken. Dies gilt insbesondere für den Beschluß des Bundesrates, der gravierende datenschutzrechtliche Verschlechterungen vorsieht.

Bereits der Gesetzentwurf der Bundesregierung wird in Teilbereichen den Vorgaben des Bundesverfassungsgerichts nicht gerecht und fällt teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z.B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück.

Kritik erheben die Datenschutzbeauftragten des Bundes und der Länder insbesondere an folgenden Punkten:

- Die Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung sind nicht hinreichend bestimmt. So wird z.B. nicht angemessen zwischen Beschuldigten und Zeugen differenziert.
- Für Privatpersonen und Stellen, die nicht Verfahrensbeteiligte sind, wird als Voraussetzung zur Auskunfts- und Akteneinsicht lediglich ein vages "berechtigtes" statt eines rechtlichen Interesses gefordert.
- Die Regelungen über Inhalt, Ausmaß und Umfang von Dateien und Informationssystemen mit personenbezogenen Daten bei Staatsanwaltschaften sind unzureichend. Das hat zur Folge, daß nahezu unbeschränkt Zentraldateien oder gemeinsame Dateien eingerichtet und Daten ohne Berücksichtigung der Begehungsweise und Schwere von Straftaten gespeichert werden können. Die Zugriffsmöglichkeiten der Strafverfolgungs- und Strafjustizbehörden auf diese Daten gehen zu weit. Darüber hinaus werden Standardmaßnahmen des technischen und organisatorischen Datenschutzes (z.B. Protokollierung, interne Zugriffsbeschränkungen etc.) weitgehend abgeschwächt.

Die Bedenken und Empfehlungen der Datenschutzbeauftragten des Bundes und der Länder fanden in den ersten Beratungen des Bundesrates zum Gesetzentwurf nahezu keinen Niederschlag.

Darüber hinaus hat der Bundesrat in seiner Stellungnahme weitergehende datenschutzrechtliche Verschlechterungen beschlossen, die vor allem die Entfernung mehrerer im Gesetzentwurf noch vorhandener Beschränkungen und verfahrensrechtlicher Sicherungen zum Schutz des Persönlichkeitsrechts und des Rechtes auf informationelle Selbstbestimmung der Betroffenen zum Inhalt haben.

Beispiele hierfür sind:

- Der Richtervorbehalt für die Anordnung der Öffentlichkeitsfahndung und der längerfristigen Observation soll gestrichen werden.
- Die Verwendungsbeschränkungen bei Daten, die mit besonderen Erhebungsmethoden nach dem Polizeirecht gewonnen wurden, sollen herausgenommen werden.
- Das Auskunfts- und Akteneinsichtsrecht auch für öffentliche Stellen soll erheblich erweitert werden.
- Detaillierte Regelungen für Fälle, in denen personenbezogene Daten von Amts wegen durch Strafverfolgungs- und Strafjustizbehörden an andere Stellen übermittelt werden dürfen, die im weitesten Sinne mit der Strafrechtspflege zu tun haben, sollen gestrichen werden.
- Das Verbot soll gestrichen werden, über die Grunddaten hinausgehende weitere Angaben nach Freispruch, endgültiger Verfahrenseinstellung oder unanfechtbarer Ablehnung der Eröffnung des Hauptverfahrens Daten in Dateien zu speichern.
- Speicherungs- und Löschungsfristen für personenbezogene Daten in Dateien sollen ersatzlos gestrichen werden.
- Kontrollverfahren für automatisierte Abrufverfahren sollen aufgehoben werden und die Verwendungsbeschränkungen für Protokolldaten sollen entfallen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Deutschen Bundestag auf, bei den anstehenden weiteren Beratungen des Gesetzentwurfes die vom Bundesrat empfohlenen datenschutzrechtlichen Verschlechterungen nicht zu übernehmen und die noch bestehenden datenschutzrechtlichen Mängel zu beseitigen.

Hingegen sollten Vorschläge des Bundesrates für Regelungen für den Einsatz von Lichtbildvorlagen und für die Datenverarbeitung zur Durchführung des Täter-Opfer-Ausgleichs aufgegriffen werden.

19.2 Genetische Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997

Immer häufiger wird bei der Verfolgung von Straftaten am Tatort oder beim Opfer festgestelltes, sog. biologisches Material als Spurenmaterial durch die Polizei sichergestellt, mittels DNA-Analyse untersucht und mit anderen DNA-Materialien verglichen. Die DNA-Analyse ist zur Standardmethode geworden, um die Herkunft von Spurenmaterial von bestimmten bekannten Personen (Verdächtigen, Opfern, unbeteiligten Dritten) oder die Identität mit anderem Spurenmaterial unbekannter Personen feststellen zu können.

Der Gesetzgeber hat zwar vor kurzem im Strafverfahrensänderungsgesetz - DNA-Analyse ("Genetischer Fingerabdruck")- die Voraussetzungen und Grenzen genetischer Untersuchungen im Strafverfahren geregelt. Eine Festlegung, ob und in welchen Grenzen die Speicherung und Nutzung der durch eine DNA-Analyse gewonnenen Untersuchungsergebnisse in Datenbanken der Polizei zu erkennungsdienstlichen Zwecken zulässig ist, enthält dieses Gesetz jedoch nicht.

Bezüglich des Aussagegehalts der gespeicherten Daten der Analyseergebnisse ist ein grundsätzlich neuer Aspekt zu berücksichtigen:

Die automatisiert gespeicherten Informationen aus DNA-Merkmalen, die zum Zweck der Identitätsfeststellung erstellt worden sind, ermöglichen derzeit tatsächlich zwar keine über die Identifizierung hinausgehenden Aussagen zur jeweiligen Person oder deren Erbgut. In Einzelfällen können die analysierten nicht codierenden persönlichkeitsneutralen DNA-Merkmale jedoch mit codierenden Merkmalen korrespondieren. In Anbetracht der weltweiten intensiven Forschung im Bereich der Genom-Analyse ist es nicht ausgeschlossen, daß künftig auch auf der Basis der Untersuchung von bisher als nicht codierend angesehenen Merkmalen konkrete Aussagen über genetische Dispositionen der betroffenen Personen mit inhaltlichem Informationswert getroffen werden können. Dieses Risiko ist deshalb nicht zu vernachlässigen, weil gegenwärtig weltweit mit erheblichem Aufwand die Entschlüsselung des gesamten menschlichen Genoms vorangetrieben wird.

Dieser Gefährdung kann dadurch begegnet werden, daß bei Bekanntwerden von Überschußinformationen durch die bisherigen Untersuchungsmethoden andere Untersuchungmethoden (Analyse eines anderen Genomabschnitts) verwendet werden, die keine Informationen über die genetische Disposition liefern. Derartige Ausweichstrategien können jedoch zur Folge haben, daß die mit anderen Methoden erlangten Untersuchungsergebnisse nicht mit bereits vorliegenden vergleichbar sind. Datenspeicherungen über verformelte

Untersuchungsergebnisse könnten daher dazu führen, daß einmal verwendete Untersuchungsformen im Interesse der Vergleichbarkeit beibehalten werden, obwohl sie sich als problematisch herausgestellt haben und unproblematische Alternativen zur Verfügung stehen, z.B. durch Verschlüsselung problematischer Informationen.

In Anbetracht dieser Situation und angesichts der Tendenz, mittels der DNA-Analyse gewonnene Daten nicht nur in einem bestimmten Strafverfahren zu verwenden, sondern diese Daten in abrufbaren Datenbanken auch für andere Strafverfahren zugänglich zu machen, fordern die Datenschutzbeauftragten des Bundes und der Länder ergänzend zu §§ 81 e und f StPO für die automatisierte Speicherung und Nutzung von DNA-Identitätsdaten eine spezielle gesetzliche Regelung in der Strafprozeßordnung, um das Persönlichkeitsrecht der Betroffenen zu schützen:

1. Es muß ein grundsätzliches Verbot der Verformelung und Speicherung solcher Analyseergebnisse statuiert werden, die inhaltliche Aussagen über Erbanlagen ermöglichen.

   Im Hinblick auf die nicht auszuschließende Möglichkeit künftiger Rückschlüsse auf genetische Dispositionen ist bereits jetzt ein striktes Nutzungsverbot für persönlichkeitsrelevante Erkenntnisse zu statuieren, die aus den gespeicherten Verformelungen der DNA resultieren.

2. Wenn zum Zweck des Abgleichs mit Daten aus anderen Verfahren (also zu erkennungsdienstlichen Zwecken) DNA-Informationen automatisiert gespeichert werden sollen (DNA-Datenbank mit der Funktion, die bei Fingerabdrücken die AFIS-Datenbank des BKA besitzt), müssen darüber hinaus folgende Regelungen geschaffen werden:

   - Nicht jede DNA-Analyse, die zum Zweck der Aufklärung einer konkreten Straftat erfolgt ist, darf in diese Datei aufgenommen werden. Die Speicherung von Verformelungen der DNA-Struktur in eine Datenbank darf nur dann erfolgen, wenn tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte künftig strafrechtlich in Erscheinung treten wird und daß die Speicherung aufgrund einer Prognose unter Zugrundelegung des bisherigen Täterverhaltens die künftige Strafverfolgung fördern kann.
   - Eine Speicherung kommt insbesondere dann nicht in Betracht, wenn der Tatverdacht gegen den Beschuldigten ausgeräumt wurde. Bereits erfolgte Speicherungen sind zu löschen. Gleiches gilt für den Fall, daß die Anordnung der DNA-Untersuchung oder die Art und Weise ihrer Durchführung unzulässig war.
   - Die Aufbewahrungsdauer von Verformelungen der DNA-Struktur ist konkret festzulegen (z.B. gestaffelt nach der Schwere des Tatvorwurfs).

3. Voraussetzung für Gen-Analysen muß in jedem Fall mindestens die richterliche Anordnung sein, unabhängig davon, ob die Daten in einem anhängigen Strafverfahren zum Zweck der Straftatenaufklärung, wie in § 81 f Absatz 1 Satz 1 StPO normiert, oder ob sie zum Zweck der künftigen Strafverfolgung (also zu Zwecken des Erkennungsdienstes) benötigt werden.

4. Ein DNA-Screening von Personengruppen, deren Zusammensetzung nach abstrakt festgelegten Kriterien ohne konkreten Tatverdacht gegenüber einzelnen erfolgt, führt im Regelfall zur Erhebung von DNA-Daten zahlreicher völlig unbeteiligter und unschuldiger Bürger. Die Daten dieser Personen sind unmittelbar dann zu löschen, wenn sie für das Anlaßstrafverfahren nicht mehr erforderlich sind. Sie dürfen nicht in verfahrensübergreifenden DNA-Dateien gespeichert werden und auch nicht mit solchen Datenbeständen abgeglichen werden.

19.3 Geplante Verpflichtung von Teledienstean bietern, Kundendaten an Sicherheitsbehörden zu übermitteln

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997

Der Entwurf der Bundesregierung für ein Teledienstedatenschutzgesetz (Artikel 2 (§ 5 Absatz 3) des Informations- und Kommunikationsdienste-Gesetzes vom 20.12.1996 - BR-Drs. 966/96) sieht vor, daß die Anbieter von Telediensten (z.B. Home-Banking, Home-Shopping) dazu verpflichtet werden sollen, insbesondere der Polizei und den Nachrichtendiensten Auskunft über Daten zur Begründung, inhaltlichen Ausgestaltung oder Änderung der Vertragsverhältnisse mit ihren Kunden (sog. Bestandsdaten) zu erteilen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Aufnahme einer solchen Übermittlungsvorschrift in das Teledienstedatenschutzgesetz des Bundes. Eine Folge dieser Vorschrift wäre, daß Anbieter von elektronischen Informationsdiensten (z.B. Diskussionsforen) offenlegen müßten, welche ihrer Kunden welche Dienste z.B. mit einer bestimmten politischen Tendenz in Anspruch nehmen. Darin läge ein massiver Eingriff nicht nur in das Recht auf informationelle Selbstbestimmung, sondern auch in die Informations- und Meinungsfreiheit des Einzelnen. Das geltende Recht, insbesondere die Strafprozeßordnung und das Polizeirecht enthalten hinreichende Möglichkeiten, um strafbaren und gefährlichen Handlungen auch im Bereich der Teledienste zu begegnen. Über die bisheri-

ge Rechtslage hinaus würde bei Verabschiedung der geplanten Regelung zudem den Nachrichtendiensten ein nichtöffentlicher Datenbestand offenstehen. In keinem anderen Wirtschaftsbereich sind vergleichbare Übermittlungspflichten der Anbieter von Gütern und Dienstleistungen hinsichtlich ihrer Kunden bekannt.

Mit guten Gründen haben deshalb die Länder davon abgesehen, in den inzwischen von den Ministerpräsidenten unterzeichneten Staatsvertrag über Mediendienste eine vergleichbare Vorschrift aufzunehmen. In der Praxis werden sich aber für Bürger und Online-Dienstanbieter schwierige Fragen der Abgrenzung zwischen den Geltungsbereichen des Mediendienste-Staatsvertrags und des Teledienstedatenschutzgesetzes ergeben. Auch aus diesem Grund halten die Datenschutzbeauftragten eine Streichung der Vorschrift des § 5 Absatz 3 aus dem Entwurf für ein Teledienstedatenschutzgesetz für geboten.

19.4 Achtung der Menschenrechte in der Europäischen Union

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997

Die DSB-Konferenz ist gemeinsam der Überzeugung, daß hinsichtlich nicht Verdächtiger und hinsichtlich nicht kriminalitätsbezogener Daten die Forderung des Europäischen Parlaments vom 17.09.1996 zu den Dateien von Europol unterstützt werden soll.

Das Europäische Parlament hat in seiner Entschließung zur Achtung der Menschenrechte gefordert, "alle Informationen persönlichen Charakters, wie Angaben zur Religionszugehörigkeit, zu philosophischen oder religiösen Überzeugungen, Rasse, Gesundheit und sexuellen Gewohnheiten, von der Erfassung in Datenbanken von EUROPOL auszuschließen."

19.5 Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997

Die Datenschutzbeauftragten des Bundes und der Länder halten es für sehr problematisch, daß in Folge technischer und gesellschaftlicher Veränderungen in einer zunehmenden Anzahl von Konstellationen personenbezogene

medizinische Patientendaten außerhalb des ärztlichen Bereiches verarbeitet werden. Sie fordern, daß zunehmend die Möglichkeiten einer anonymen oder pseudonymen Datenverarbeitung mit Verschlüsselung genutzt werden. Soweit dennoch Patientendaten personenbezogen weitergegeben werden, ist ein wesentliches Problem, daß außerhalb des ärztlichen Gewahrsams der von der Strafprozeßordnung vorgesehene Schutz personenbezogener Patientendaten vor Inanspruchnahme als Beweismittel durch Zeugeneinvernahme oder Beschlagnahme nicht mehr zweifelsfrei sichergestellt ist bzw. überhaupt nicht existiert.

Die folgenden Beispiele machen dies deutlich:

1. Ärzte bzw. Krankenhäuser haben z.B. keinen Gewahrsam an den personenbezogenen Patientendaten, die der Patient auf einer (freiwilligen) Patientenchipkarte bei sich trägt/besitzt oder die von einer dritten Stelle außerhalb des ärztlichen Bereichs im Auftrag verarbeitet werden, wie z.B. bei Mailbox-Systemen, externer Archivierung oder der Vergabe von Schreibarbeiten an selbständige Schreibbüros.

   Fraglich ist auch die Aufrechterhaltung des ärztlichen Gewahrsams, wenn Hilfspersonal des Arztes oder Krankenhauses Patientendaten in der Privatwohnung bearbeitet.

2. Zunehmend werden einzelne Unternehmensfunktionen bzw. fachliche Aufgaben ausgelagert und einer externen Stelle - in der Regel einem Privatunternehmen - übertragen (sog. Outsourcing), - z.B. bei Einschaltung eines externen Inkassounternehmens, bei externem Catering für stationäre Patienten, bei externer Archivierung oder bei Vergabe von Organisationsanalysen an externe Beratergesellschaften.

3. Medizinische Daten mit Patientenbezug sollen an Forscher oder Forschungsinstitute zu Zwecken wissenschaftlicher Forschung übermittelt werden. Je umfassender und komplizierter der Einsatz automatisierter Datenverarbeitung für Forschungszwecke vorgesehen wird, desto weniger werden die personenbezogenen Patientendaten ausschließlich durch ärztliches Personal verarbeitet. Hier setzt sich vielmehr die Verarbeitung durch Informatiker und Statistiker immer mehr durch. Aber auch bei Verarbeitung durch Ärzte, die in der Forschung tätig sind, ist keineswegs sichergestellt, daß die personenbezogenen Patientendaten diesen Ärzten "in ihrer Eigenschaft als Arzt" bekannt geworden sind, wie dies durch die Strafprozeßordnung für den Beschlagnahmeschutz als Voraussetzung festgelegt ist.

Die zunehmende Verlagerung personenbezogener Patientendaten aus dem Schutzbereich des Arztgeheimnisses nach außen verstößt nach Ansicht der

Datenschutzbeauftragten massiv gegen Interessen der betroffenen Patienten, solange nicht ein gleichwertiger Schutz gewährleistet ist.

Die Datenschutzbeauftragten des Bundes und der Länder bitten daher den Bundesgesetzgeber - unabhängig von weiteren Fragen des Datenschutzes, die mit der Verarbeitung medizinischer Daten im Rahmen der Telemedizin verbunden sein können - für die sich zunehmend entwickelnden modernen Formen der Auslagerung medizinischer Patientendaten sowie für die Weitergabe medizinischer Patientendaten für Zwecke wissenschaftlicher medizinischer Forschung einen dem Arztgeheimnis entsprechenden Schutz der Patientendaten zu schaffen.

19.6 Vorschläge der Arbeitsgruppe des ASMK "Verbesserter Datenaustausch bei Sozialleistungen"

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 20. Oktober 1997

Mit dem von der ASMK-Arbeitsgruppe vorgeschlagenen erweiterten Datenaustausch bei Sozialleistungen wird die Bekämpfung von Leistungsmißbräuchen angestrebt. Soweit dieses Ziel der Arbeitsgruppe mit einer Veränderung der Strukturen der Verarbeitung personenbezogener Daten im Sozialleistungsbereich – insbesondere mit veränderten Verfahren der Datenerhebung – erreicht werden soll, muß der verfassungsrechtlich gewährleistete Grundsatz der Verhältnismäßigkeit beachtet werden.

Die gegenwärtigen Regelungen der Datenerhebung im Sozialleistungsbereich sehen unterschiedliche Verfahren der Datenerhebung vor, vor allem

- Datenerhebungen beim Betroffenen selbst
- Datenerhebungen bei Dritten mit Mitwirkung des Betroffenen
- Datenerhebungen bei Dritten ohne Mitwirkung des Betroffenen aus konkretem Anlaß
- Datenerhebungen bei Dritten ohne Mitwirkung des Betroffenen ohne konkreten Anlaß (Stichproben / Datenabgleich).

Diese Verfahren der Datenerhebung sind mit jeweils unterschiedlich schwerwiegenden Eingriffen in das Persönlichkeitsrecht der Betroffenen verbunden. So weiß z.B. bei einer Datenerhebung beim Betroffenen dieser, wer wann welche Daten zu welchem Zweck über ihn erhebt, und Dritte erhalten keine Kenntnis von diesen Datenerhebungen. Im Gegensatz dazu wird bei einer Datenerhebung bei Dritten ohne Mitwirkung des Betroffenen dieser darüber im Unklaren gelassen, wer wann welche Daten zu welchem Zweck über ihn

erhebt, und Dritten werden Daten über den Betroffenen zur Kenntnis gegeben (z.B. der Bank die Tatsache, daß der Betroffene Sozialhilfeempfänger ist).

Dieses System der Differenzierung des Verfahrens der Datenerhebung entspricht dem Grundsatz der Verhältnismäßigkeit. Ferner ist zu differenzieren, ob Daten aus dem Bereich der Sozialleistungsträger oder Daten außerhalb dieses Bereichs erhoben werden.

In dem Bericht der Arbeitsgruppe wird dieses System zum Teil aufgegeben. Es werden Verfahren zur Datenerhebung vorgesehen, die schwerwiegend in die Rechte der Betroffenen eingreifen, ohne daß hinreichend geprüft und dargelegt wird, ob minder schwere Eingriffe in das Persönlichkeitsrecht zum Erfolg führen können. Die Datenschutzbeauftragten wenden sich nicht um jeden Preis gegen Erweiterungen des Datenaustauschs, gehen aber davon aus, daß pauschale und undifferenzierte Änderungen des gegenwärtigen Systems unterbleiben.

Datenabgleichsverfahren sollen nur in Frage kommen bei Anhaltspunkten für Mißbrauchsfälle in nennenswertem Umfang. Deshalb müssen etwaige neue Datenabgleichsverfahren hinsichtlich ihrer Wirkungen bewertet werden. Daher ist parallel zu ihrer Einführung die Implementierung einer Erfolgskontrolle für das jeweilige Abgleichsverfahren vorzusehen, die auch präventive Wirkungen erfaßt. Dies ermöglicht, Aufwand und Nutzen zueinander in das verfassungsmäßig gebotene Verhältnis zu setzen.

Soweit unter Beachtung dieser Prinzipien neue Kontrollinstrumente gegen den Leistungsmißbrauch tatsächlich erforderlich sind, muß für den Bürger die Transparenz der Datenflüsse sichergestellt werden. Diese Transparenz soll gewährleisten. daß der Bürger nicht zum bloßen Objekt von Datenerhebungen wird.

Bezug nehmend auf die bisherigen Äußerungen des BfD und von LfD bestehen gegen folgende Vorschläge im Bericht gravierende Bedenken:

1. Mitwirkung bei der Ahndung des Mißbrauchs (für alle Leistungsträger) und Verbesserungen für die Leistungsempfänger (zu D.II.10.1 und B.I) (S. 30 u. S. 2)

Die vorgeschlagenen Möglichkeiten von anlaßunabhängigen Mißbrauchskontrollen beinhalten keine Klarstellung der gegebenen Rechtslage, sondern stellen erhebliche Änderungen des bisherigen abgestuften Systems der Datenerhebung dar.

Die mit der Datenerhebung verbundene Offenlegung des Kontaktes bzw. einer Leistungsbeziehung zu einem Sozialleistungsträger stellt einen erheblichen Eingriff für den Betroffenen dar, u.a. da sie geeignet ist, seine Stellung in der Öffentlichkeit, z.B. seine Kreditwürdigkeit, wesentlich zu beeinträchtigen. Anfragen bei Dritten ohne Kenntnis des Betroffenen lassen diesen im Unklaren, welche Daten wann an wen übermittelt wurden.

Derartige Datenerhebungen werden vom geltenden Recht deshalb mit Rücksicht auf das verfassungsrechtliche Verhältnismäßigkeitsprinzip nur in begrenzten und konkretisierten Ausnahmefällen zugelassen. Von dieser verfassungsrechtlich gebotenen Systematik würde die vorgeschlagene Neuregelung grundlegend abweichen. Die Datenschutzbeauftragten betonen bei dieser Gelegenheit den allgemeinen Grundsatz, daß Datenerhebungen, die sowohl pauschal und undifferenziert sind, als auch ohne Anlaß erfolgen, abzulehnen sind.

Die Datenschutzbeauftragten weisen schließlich darauf hin, daß gegen eine Ausnutzung der technischen Datenverarbeitungsmöglichkeiten zugunsten des Betroffenen (B.I des Berichts) nichts spricht, solange die Betroffenen davon informiert sind und soweit sie dem Verfahren zugestimmt haben.

2. Nachfrage beim Wohnsitzfinanzamt des Hilfesuchenden und Schenkungen und Erbschaften (zu D.I.1.1) (S. 6)

Die Datenschutzbeauftragten teilen nicht die Auffassung, daß Stichproben nach der geltenden Rechtslage zu § 21 Abs. 4 SGB X möglich sind. § 21 Abs. 4 SGB X ist eine Auskunftsvorschrift für die Finanzbehörden, die über die Datenerhebungsbefugnis der Sozialleistungsträger nichts aussagt. Die Leistungsträger dürfen diese Auskünfte bei den Finanzbehörden als Dritten nur nach Maßgabe des § 67 a SGB X einholen, soweit das erforderlich ist: Diese Erforderlichkeit setzt Anhaltspunkte für Leistungsmißbrauch im Einzelfall voraus.

3. Auskunftspflicht der Banken und Lebensversicherungen (zu D.II.1.6) (S.13)

Die Datenerhebung im Sozialbereich ist von einer möglichst weitgehenden Einbeziehung des Betroffenen gekennzeichnet. Der Vorschlag zur Einführung einer Auskunftspflicht geht auf dieses differenzierte System der Datenerhebungen im Sozialbereich überhaupt nicht ein.

Die Annahme in der Begründung des Vorschlags, ohne eine derartige Auskunftspflicht bestünden keine sachgerechten Ermittlungsmöglichkeiten, trifft nicht zu. Der Betroffene ist verpflichtet, Nachweise zu erbringen; dazu können auch Bankauskünfte gehören. Allerdings ist dem Betroffenen vorrangig Gelegenheit zu geben, solche Auskünfte selbst und ohne Angabe ihres Verwendungszwecks beizubringen. Nur soweit dennoch erforderlich, ist der Betroffene im Rahmen seiner Mitwirkungspflicht gehalten, sein Einverständnis in die Erteilung von Bankauskünften zu geben. Die vorgeschlagene pauschale Auskunftsverpflichtung birgt deshalb die Gefahr in sich, daß dann generell ohne Mitwirkung des Betroffenen und ohne sein Einverständnis sofort an die Bank/Lebensversicherung herangetreten wird mit der Wirkung, daß der Betroffene desavouiert wird.

Die Datenschutzbeauftragten halten deshalb eine Klarstellung für dringend erforderlich, daß derartige unmittelbare Anfragen und Auskünfte erst in Betracht kommen, wenn die Ermittlungen unter Mitwirkung des Betroffenen zu keinem ausreichenden Ergebnis führen und Anhaltspunkte dafür bestehen, daß bei der fraglichen Bank/Lebensversicherung nicht angegebenes Vermögen vorhanden ist.

4.Akzeptanz des Datenaustausches (zu E.IV) (S. 36)

Datenabgleiche beinhalten eine Verarbeitung personenbezogener Daten, die nicht beliebig durchgeführt werden darf und anerkanntermaßen einer gesetzlichen Grundlage bedarf. Die im Papier der Arbeitsgruppe unter E.IV vertretene These, daß anlaßunabhängige Datenabgleiche keiner speziellen gesetzlichen Grundlage bedürften, trifft deshalb nicht zu.

Die Datenschutzbeauftragten wenden sich nicht gegen einzelne Veränderungen der Datenverarbeitung im Sozialleistungsbereich, soweit sie tatsächlich erforderlich und verhältnismäßig sind und die zuvor aufgezeigten Grundsätze beachtet werden. Die Datenschutzbeauftragten sind dazu gesprächsbereit.

19.7 Novellierung des Bundesdatenschutzgesetzes und Modernisierung des Datenschutzrechts

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997

Die fristgerechte Harmonisierung des Datenschutzes entsprechend den Vorgaben der europäischen Datenschutzrichtlinie vom 24. Oktober 1995 droht zu scheitern. Die von dieser Richtlinie gesetzte Dreijahresfrist wird heute in einem Jahr ablaufen. Eine gründliche Beratung im Deutschen Bundestag wird durch den baldigen Ablauf der Legislaturperiode in Frage gestellt.

Noch immer gibt es keinen Kabinettsbeschluß; die Bundesregierung hat bisher noch nicht einmal einen abgestimmten Referentenentwurf vorgelegt. Sie gefährdet dadurch die rechtzeitige Umsetzung der Richtlinie und riskiert ein Vertragsverletzungsverfahren vor dem Europäischen Gerichtshof.

Für die Entwicklung des Datenschutzes ist diese Lage höchst nachteilig:

- Verbesserungen des Datenschutzes der Bürger, z.B. durch genauere Information über die Verarbeitung ihrer Daten, verzögern sich;
- dem Datenschutzrecht droht Zersplitterung, weil den Ländern eine Orientierung für die Anpassung der Landesdatenschutzgesetze fehlt.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an die Bundesregierung, für eine fristgerechte Umsetzung der Richtlinie Sorge zu tragen.

Zur Harmonisierung des europäischen Datenschutzrechts empfehlen die Datenschutzbeauftragten der Bundesregierung und dem Gesetzgeber folgende Grundsatzentscheidungen:

- weitgehende Gleichbehandlung des öffentlichen und des privaten Bereichs bei gleichzeitiger Verbesserung der Datenschutzkontrolle, insbesondere durch generell anlaßunabhängige Kontrolle und durch die ausdrückliche Festlegung der völligen Unabhängigkeit der Aufsichtsbehörden und die Erweiterung ihrer Eingriffsbefugnisse;
- Bestellung weisungsfreier Datenschutzbeauftragter auch bei öffentlichen Stellen mit dem Recht, sich jederzeit an den Bundes- oder Landesbeauftragten für den Datenschutz zu wenden;
- Bürgerfreundlichkeit durch einfache und verständliche Formulierung des BDSG, z.B. durch einen einheitlichen Begriff der Verarbeitung personenbezogener Daten entsprechend der Richtlinie;
- Gewährleistung eines einheitlichen, hohen Datenschutzniveaus durch Beibehaltung der Funktion des BDSG und der Landesdatenschutzgesetze als Querschnittsgesetze sowie durch Vermeidung eines Gefälles zwischen den Bereichen, die der EG-Datenschutzrichtlinie unterfallen, und den übrigen Gebieten, deren Datenschutzregelungen nicht verschlechtert werden dürfen
- Sonderregelungen für Presse und Rundfunk nur, soweit zur Sicherung der Meinungsfreiheit notwendig.

Als ebenso vordringlich betrachten die Datenschutzbeauftragten eine Anpassung der noch von der Großrechnertechnologie der siebziger Jahre bestimmten gesetzlichen Regelungen an die heutige Informationstechnologie und an die Verhältnisse der modernen Informationsgesellschaft. Dazu gehören insbesondere folgende Punkte:

- Verbindliche Grundsätze für die datenschutzfreundliche Gestaltung von Informationssystemen und -techniken, so zur Datensparsamkeit, zur Anonymisierung und Pseudonymisierung, zur Verschlüsselung und zur Risikoanalyse;
- mehr Transparenz für die Verbraucher und mehr Eigenständigkeit für die Anbieter durch Einführung eines Datenschutzaudits;
- Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen, Regelung der Video-Überwachung;

- Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren;
- Einführung einer Vorabkontrolle für besonders risikoreiche Datenverarbeitung, namentlich bei Verarbeitung sensitiver Daten;
- Regelungen für Chipkarten-Anwendungen;
- Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing, unter anderem auch mindestens durch die Festlegung von Hinweispflichten hinsichtlich der Möglichkeit des Widerspruchs; vorzuziehen ist in jedem Fall eine Einwilligungsregelung;
- Verstärkung des Schutzes gegenüber der Einholung von Selbstauskünften vor Abschluß von Miet-, Arbeits- und ähnlich existenzwichtigen Verträgen;
- Datenexport nach Inlandsgrundsätzen nur bei angemessenem Schutzniveau im Empfängerstaat; Festlegung, unter welchen Voraussetzungen ein Mitgliedstaat Daten, die er im Anwendungsbereich der Richtlinie (also nach Inlandsgrundsätzen) erhalten hat, außerhalb ihres Anwendungsbereichs verwenden darf;
- möglichst weitgehende Ersetzung der Anmeldung von Dateien bei der Aufsichtsbehörde durch Bestellung weisungsfreier Datenschutzbeauftragter; Beibehaltung des internen Datenschutzbeauftragten auch bei Sicherheitsbehörden;
- Stärkung der Kontrollrechte des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz durch uneingeschränkte Kontrollbefugnis bei der Verarbeitung personenbezogener Daten in Akten einschließlich solcher über Sicherheitsüberprüfungen.

Die Konferenz weist ferner auf die Rechtspflicht der Länder hin, ihr Datenschutzrecht ebenfalls der EG-Richtlinie fristgerecht anzupassen.

19.8 Informationelle Selbstbestimmung und Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997

Überlegungen des Gesetzgebers und eine beginnende öffentliche Diskussion, moderne Dokumentationstechnik der Wahrheitsfindung und dem Zeugenschutz in gerichtlichen Verfahren nutzbar zu machen, liegen auch im Interesse des Datenschutzes. Dabei ist allerdings zu beachten, daß Bild-Ton-

Aufzeichnungen von Vernehmungen im Strafverfahren einen erheblichen Eingriff in das Persönlichkeitsrecht darstellen. Sie spiegeln die unmittelbare Betroffenheit der Beschuldigten oder Zeugen in Mimik und Gestik umfassend wider. Zweck und Erforderlichkeit dieses Eingriffs bedürfen einer sorgfältigen Begründung durch den Gesetzgeber. Sie bildet den Maßstab, der über Möglichkeiten, Grenzen und Verfahren der Videotechnologie im Strafprozeß entscheidet. Erkennbar und nachvollziehbar sollte sein, daß der Gesetzgeber die Risiken des Einsatzes dieser Technologie, insbesondere die Verfügbarkeit der Aufzeichnungen nach den allgemeinen Vorschriften über die Beweisaufnahme bedacht und bewertet hat. Ferner sollte erkennbar und nachvollziehbar sein, daß Alternativen zur Videotechnologie, namentlich die Verwendung von Tonaufzeichnungen, in die Erwägungen des Gesetzgebers aufgenommen wurden.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sollten die vorliegenden Gesetzentwürfe des Bundesrates (BT-Drs. 13/4983 vom 19.06.1996) sowie der Fraktionen der CDU/CSU und F.D.P. (BT-Drs. 13/7165 vom 11.03.1997) in einem umfassenderen Bedeutungs- und Funktionszusammenhang diskutiert werden. Zunehmend tritt das Anliegen der Praxis hervor, Bild-Ton-Aufzeichnungen auch mit anderer Zielsetzung zu verwerten:

Bild-Ton-Aufzeichnungen ermöglichen eine vollständige und authentische Dokumentation nicht nur des Inhalts, sondern auch der Entstehung und Begleitumstände einer Aussage. Die Beurteilung ihres Beweiswerts wird dadurch deutlich verbessert. Zugleich dient eine nur einmalige Vernehmung, die möglichst zeitnah zum Tatgeschehen durchgeführt und aufgezeichnet wird, der Wahrheitsfindung und erhöht die Qualität der gerichtsverwertbaren Daten ("Vermeidung kognitiver Dissonanzen"). Ausgehend von diesen Überlegungen, hat der Gesetzgeber unter Einbeziehung von Erkenntnissen der Vernehmungspsychologie zu prüfen, ob und inwieweit eine wortgetreue Abfassung von Vernehmungsniederschriften ausreicht und eine Aufzeichnung der Aussage nur im Wort auf Tonband für die Zwecke des Strafverfahrens in ihrer Beweisqualität der Videotechnologie sogar überlegen ist.

Für Videoaufzeichnungen des Betroffenen, die zu seinem Schutz gefertigt werden sollen, ist dessen Einwilligung unverzichtbare Voraussetzung für die Zulässigkeit einer Bild-Ton-Aufzeichnung im Strafverfahren. Sofern der Betroffene nicht in der Lage ist, die Bedeutung und Tragweite einer Bild-Ton-Aufzeichnung und ihrer Verwendungsmöglichkeiten hinreichend zu beurteilen, hat der Gesetzgeber festzulegen, wer anstelle des Betroffenen die Einwilligung erteilen darf. Vor Abgabe der Einwilligungserklärung ist der Betroffene umfassend aufzuklären, insbesondere auch über alle zulässigen Arten der weiteren Verwertung und über die Möglichkeit des Widerrufs der Einwilligung für die Zukunft. Die Aufklärung ist zuverlässig zu dokumentieren. Entsprechendes gilt für die Herausgabe von Videoaufzeichnungen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern wirksame Vorkehrungen zum Schutz des Persönlichkeitsrechts bei Verwendung von Bild-Ton-Aufzeichnungen im Strafverfahren. Unabhängig von der Frage, welche Zielsetzung mit Bild-Ton-Aufzeichnungen im Strafverfahren verfolgt werden soll, sind hierbei insbesondere folgende Gesichtspunkte von Bedeutung:

1. Es ist sicherzustellen, daß der Eindruck des Aussagegeschehens z.B. durch Zeitlupe, Zeitraffer, Einzelbildabfolge, Standbild und Zoom nicht gezielt verfremdet oder verzerrt wird.

2. Einsatz und Verwertung von Bild-Ton-Aufzeichnungen sind so zu regeln, daß gesetzliche Zeugnisverweigerungsrechte gewahrt bleiben. Insbesondere ist eine weitere Nutzung der Aufnahme, auch zum Zwecke des Vorhalts, ausgeschlossen, wenn sich ein Zeuge auf sein Zeugnisverweigerungsrecht beruft.

3. Vorbehaltlich des o.g. Einwilligungserfordernisses darf eine Übermittlung von Videoaufzeichnungen an Stellen außerhalb der Justiz, wenn überhaupt, nur in Ausnahmefällen erlaubt sein, da nur so ein wirksamer Schutz vor Mißbrauch, etwa durch kommerzielle Verwertung, gewährleistet werden kann. Soweit der Gesetzgeber aus Gründen eines fairen, rechtsstaatlichen Strafverfahrens die Weitergabe von Videokopien an Verfahrensbeteiligte zuläßt, müssen jedenfalls wirksame Vorkehrungen gegen Mißbrauch gewährleistet sein, z.B. sichtbare Signierung und strafbewehrte Regelungen über Zweckbindungen und Löschungsfristen.

4. Eine Verwertung der Aufzeichnungen im Rahmen eines anderen Strafverfahrens ist nur zulässig, soweit sie auch für die Zwecke dieses anderen Verfahrens hätten angefertigt werden dürfen.

5. Soweit eine Verwertung in einem anderen gerichtlichen Verfahren - etwa zur Vermeidung erneuter Anhörung kindlicher Zeugen vor dem Familien- oder Vormundschaftsgericht - zugelassen werden sollte, sind in entsprechenden Ausnahmeregelungen präzise Voraussetzungen hierfür abschließend zu bestimmen und enge Verwendungsregelungen zu treffen.

6. Spätestens mit dem rechtskräftigen Abschluß des Strafverfahrens sind grundsätzlich die Aufzeichnungen unter Aufsicht der Staatsanwaltschaft zu vernichten. Der Betroffene ist davon zu benachrichtigen. Soweit der Gesetzgeber ausnahmsweise zur Wahrung vorrangiger Rechtsgüter eine längere Aufbewahrung der Aufzeichnungen zuläßt, müssen Voraussetzungen, Umfang und Fristen der weiteren Aufbewahrung klar und eng geregelt werden.

19.9 Erforderlichkeit datenschutzfreundlicher Technologien

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997

Moderne Informations- und Telekommunikationstechnik (IuK-Technik) gewinnt in allen Lebensbereichen zunehmende Bedeutung. Die Nutzer wenden diese Technik z. B. in Computernetzen, Chipkartensystemen oder elektronischen Medien in vielfältiger Weise an und hinterlassen dabei zumeist umfangreiche elektronische Spuren. Dabei fällt in der Regel eine Fülle von Einzeldaten an, die geeignet sind, persönliche Verhaltensprofile zu bilden.

Den Erfordernissen des Datenschutzes wird nicht in ausreichendem Maße Rechnung getragen, wenn sich der Schutz der Privatheit des einzelnen lediglich auf eine Beschränkung des Zugangs zu bereits erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten reduziert. Daher ist es erforderlich, bereits vor der Erhebung und Speicherung die zu speichernde Datenmenge wesentlich zu reduzieren.

Datensparsamkeit bis hin zur Datenvermeidung, z. B. durch Nutzung von Anonymisierung und Pseudonymisierung personenbezogener Daten, spielen in den unterschiedlichen Anwendungsbereichen der IuK-Technik, wie elektronischen Zahlungsverfahren, Gesundheits- oder Verkehrswesen, bisher noch eine untergeordnete Rolle. Eine datenschutzfreundliche Technologie läßt sich aber nur dann wirksam realisieren, wenn das Bemühen um Datensparsamkeit die Entwicklung und den Betrieb von IuK-Systemen ebenso stark beeinflußt wie die Forderung nach Datensicherheit.

Die Datenschutzbeauftragten des Bundes und der Länder wollen in Zusammenarbeit mit Herstellern und Anbietern auf datenschutzgerechte Lösungen hinarbeiten. Die dafür erforderlichen Techniken stehen weitgehend schon zur Verfügung. Moderne kryptographische Verfahren zur Verschlüsselung und Signatur ermöglichen die Anonymisierung oder Pseudonymisierung in vielen Fällen, ohne daß die Verbindlichkeit und Ordnungsmäßigkeit der Datenverarbeitung beeinträchtigt werden. Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff "Privacy enhancing technology (PET)" eine Philosophie der Datensparsamkeit beschreibt und ein ganzes System technischer Maßnahmen umfaßt, sollten genutzt werden.

Vom Gesetzgeber erwarten die Datenschutzbeauftragten des Bundes und der Länder, daß er die Verwendung datenschutzfreundlicher Technologien durch Schaffung rechtlicher Rahmenbedingungen forciert. Sie begrüßen, daß sowohl der Mediendienste-Staatsvertrag der Länder als auch das Teledienstedatenschutzgesetz des Bundes bereits den Grundsatz der Datenvermeidung normieren. Der in den Datenschutzgesetzen des Bundes und der Länder festgeschriebene Grundsatz der Erforderlichkeit läßt sich in Zukunft ins-

besondere durch Berücksichtigung des Prinzips der Datensparsamkeit und der Verpflichtung zur Bereitstellung anonymer Nutzungsformen verwirklichen. Die Datenschutzbeauftragten des Bundes und der Länder bitten darüber hinaus die Bundesregierung, sich im europäischen Bereich dafür einzusetzen, daß die Förderung datenschutzfreundlicher Technologien entsprechend dem Vorschlag der Kommission in das 5. Rahmenprogramm "Forschung und Entwicklung" aufgenommen wird.

Neben Anbietern von Tele- und Mediendiensten sollten auch die Hersteller und Anbieter von IuK-Technik bei der Ausgestaltung und Auswahl technischer Einrichtungen dafür gewonnen werden, sich am Grundsatz der Datenvermeidung zu orientieren und auf eine konsequente Minimierung gespeicherter personenbezogener Daten achten.

19.10 Datenschutz beim digitalen Fernsehen

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998

Die Datenschutzbeauftragten des Bundes und der Länder machen darauf aufmerksam, daß bei elektronischen Diensten immer umfangreichere Datenspuren über das Verhalten der Einzelnen entstehen. Mit der Digitalisierung der Fernseh- und Hörfunkübertragung entsteht die technische Infrastruktur dafür, daß erstmals auch das individuelle Mediennutzungsverhalten registriert werden kann. Sie bekräftigen deshalb ihre Forderung, daß auch bei der Vermittlung und Abrechnung digitaler Fernsehsendungen eine flächendeckende Registrierung des individuellen Fernsehkonsums vermieden wird. Im digitalen Fernsehen ("Free TV" und "Pay TV") muß die unbeobachtete Nutzung des Mediums ohne Nachteile möglich bleiben.

Die Datenschutzbeauftragten begrüßen es deshalb, daß die Staats- und Senatskanzleien Vorschläge für die Änderung des Rundfunkstaatsvertrags vorgelegt haben, mit denen Belangen des Datenschutzes Rechnung getragen werden soll. Besonders hervorzuheben sind folgende Punkte:

- Die Gestaltung technischer Einrichtungen muß sich an dem Ziel ausrichten, daß so wenige personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden;
- die Rundfunkveranstalter müssen die Nutzung und Bezahlung von Rundfunkangeboten anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist;

- personenbezogene Daten über die Inanspruchnahme einzelner Sendungen dürfen für Abrechnungszwecke nur gespeichert werden, wenn ein Einzelnachweis verlangt wird;
- wie bereits im Mediendienstestaatsvertrag enthält auch der Entwurf des Rundfunkstaatsvertrags eine Vorschrift zum Datenschutzaudit, d.h. Veranstalter können ihr Datenschutzkonzept und ihre technischen Einrichtungen von unabhängigen Gutachtern prüfen und das Prüfungsergebnis veröffentlichen lassen.

Die Datenschutzbeauftragten halten diese Grundsätze für geeignet, eine datenschutzgerechte Nutzung digitaler Fernsehangebote zu ermöglichen. Die technischen Möglichkeiten, diesen datenschutzrechtlichen Vorgaben zu entsprechen. sind gegeben. Die Datenschutzbeauftragten konnten sich bereits 1996 hiervon praktisch überzeugen. Die Systementscheidung von Veranstaltern für einen Decodertyp, der möglicherweise weniger geeignet ist, die Datenschutzanforderungen zu erfüllen, kann kein Maßstab für die Angemessenheit dieser Anforderungen sein, wenn zugleich andere Geräte ihnen ohne Probleme genügen.

Der Forderung von Inhabern von Verwertungsrechten, einen Nachweis über die Inanspruchnahme von pay-per-view-Angeboten vorzulegen, kann ohne Personenbezug - etwa durch zertifizierte Zähleinrichtungen oder den Einsatz von Pseudonymen - entsprochen werden.

Die Datenschutzbeauftragten bitten deshalb die Ministerpräsidentin und die Ministerpräsidenten der Länder, an den datenschutzrechtlichen Regelungen des Entwurfs festzuhalten. Damit würden das bisherige Datenschutzniveau für die Fernsehnutzung im digitalen Zeitalter abgesichert und zugleich die Vorschriften für den Bereich des Rundfunks und der Mediendienste harmonisiert.

Die Datenschutzbeauftragten fordern die Rundfunkveranstalter und Hersteller auf, den Datenschutz bei der Gestaltung von digitalen Angeboten schon jetzt zu berücksichtigen.

19.11 Datenschutzprobleme der Geldkarte

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt ihre Forderung aus ihrer Entschließung vom 13.10.1995 nach einem anonymen elektronischen Zahlungsverfahren bei elektronischen Geld-

börsen. Dies gilt insbesondere für die Geldkarte des deutschen Kreditwesens, bei der in kartenbezogenen "Schattenkonten" der Evidenzzentralen nicht nur der Kaufbetrag und ein identifizierbarer Händlerschlüssel, sondern auch der Kaufzeitpunkt gespeichert werden. Mit diesen Daten können sämtliche mit der Geldkarte getätigten Kaufvorgänge jahrelang nachvollzogen werden, wenn die Daten mit den persönlichen Kundendaten zusammengeführt werden. Diese Geldkarte erfüllt nicht die Forderungen der Datenschutzbeauftragten.

Außerdem werden die Kundinnen und Kunden über diese "Schattenkonten" noch nicht einmal informiert. Die Herausgeber solcher Karten bzw. die Kreditinstitute haben aber die Pflicht, ihre Kundinnen und Kunden über Art und Umfang der im Hintergrund laufenden Verarbeitungsvorgänge zu informieren.

Unabhängig davon müssen bei der Geldkarte des deutschen Kreditwesens sämtliche Umsatzdaten in den Evidenzzentralen und auch bei den Händlern nach Abschluß der Verrechnung (Clearing) gelöscht oder zumindest anonymisiert werden.

Die Datenschutzbeauftragten fordern die Kartenherausgeber und die Kreditwirtschaft erneut dazu auf, vorzugsweise kartengestützte Zahlungssysteme ohne personenbezogene Daten - sog. White Cards - anzubieten. Die Anwendung ist so zu gestalten, daß ein karten- und damit personenbezogenes Clearing nicht erfolgt.

Der Gesetzgeber bleibt aufgerufen sicherzustellen, daß auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher bei Bargeldzahlung anonym zu bleiben.

19.12 Fehlende bereichsspezifische Regelungen bei der Justiz

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998

Derzeit werden in allen Bereichen der Justiz – bei Staatsanwaltschaften, Gerichten und Gerichtsvollziehern – im Zuge von Modernisierungsvorhaben umfassende Systeme der automatisierten Datenverarbeitung eingeführt mit der Folge, daß sensible personenbezogene Daten auch hier in viel stärkerem Maße verfügbar werden als bisher. Sogar die Beauftragung Privater mit der Verarbeitung sensibler Justizdaten wird erwogen. Gerade vor dem Hintergrund dieser vollkommen neuen Qualität der Datenverarbeitung in der Justiz wird deutlich, daß die Rechtsprechung des Bundesverfassungsgerichts zum sogenannten Übergangsbonus hier keine tragfähige Grundlage für Eingriffe in die informationelle Selbstbestimmung mehr darstellen kann. Vielmehr

müssen die Entscheidungen des Gesetzgebers den Maßstab für die weitere technische Ausgestaltung der Datenverarbeitung innerhalb der Justiz bilden und nicht umgekehrt. Dabei ist nicht nur für formell ausreichende Rechtsgrundlagen Sorge zu tragen. Auch Fragen der Datensicherheit und der Ordnungsmäßigkeit der Datenverarbeitung bedürfen der Regelung.

Seit dem Volkszählungsurteil des Bundesverfassungsgerichts sind 15 Jahre vergangen. Dennoch werden ausgerechnet im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen deshalb im Anschluß an ihren Beschluß der 48. Konferenz vom 26./27.09.1994 in Potsdam ihre wiederholten Forderungen zu bereichsspezifischen Regelungen bei der Justiz.

Zwar hat der Gesetzgeber in der abgelaufenen Legislaturperiode zumindest Regelungen über Datenerhebung, -verarbeitung und –nutzung im Strafvollzug sowie über die Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentlichen Stellen geschaffen.

Trotzdem sind in wichtigen Bereichen gesetzliche Regelungen weiterhin überfällig. Ausreichende gesetzliche Regelungen fehlen vor allem für

- weite Bereiche der Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien

namentlich die

  - Übermittlung von Strafverfahrensdaten an nicht am Strafverfahren beteiligte dritte Stellen;
  - Rechte der Betroffenen (nicht nur der Beschuldigten, sondern auch von Zeugen und sonstigen Personen, deren Daten gespeichert werden) in Bezug auf Daten, die im Zusammenhang mit einem Strafverfahren gespeichert werden.

- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien;
- Datenübermittlung zu wissenschaftlichen Zwecken;
- Datenverarbeitung in der Zwangsvollstreckung;
- Datenverarbeitung im Jugendstrafvollzug;
- Datenverarbeitung im Vollzug der Untersuchungshaft.

Der Gesetzgeber sollte daher in der kommenden Legislaturperiode zügig die notwendigen Novellierungen, für die zum Teil ja schon erhebliche Vorarbei-

ten geleistet worden sind, aufgreifen. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und –verarbeitung in welchem Umfang erforderlich ist. Ferner hat der Gesetzgeber jeweils bereichsspezifisch zu prüfen, inwieweit Aufgaben der Justiz und damit verbundene Datenverarbeitungen Privaten übertragen werden dürfen.

Der Entwurf für ein "StVÄG 1996" erfüllt diese Voraussetzungen nicht, im Gegenteil fällt er teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z.B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück. Zu kritisieren sind vor allem:

- Mangelnde Bestimmtheit der Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung
- Unangemessen weite Auskunfts- und Akteneinsichtsmöglichkeiten für nicht Verfahrensbeteiligte
- Unzureichende Regelungen über Inhalt, Ausmaß und Umfang von staatsanwaltlichen Dateien und Informationssystemen

Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe unverzüglich in der neuen Legislaturperiode bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes der Bürgerinnen und Bürger entgegenwirken.

19.13Weitergabe von Meldedaten an Adressbuchverlage und Parteien

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998

Bei den Datenschutzbeauftragten des Bundes und der Länder gehen viele Beschwerden ein, in denen deutlicher Unmut über veröffentlichte Daten in Adressbüchern und unverlangt erhaltene Werbesendungen geäußert wird. Vor Wahlen nehmen die Beschwerden noch zu. Überrascht stellten Betroffene fest, daß sie persönlich adressierte Wahlwerbung der Parteien bekommmen. Ihnen ist unerklärlich, wie Adressbuchverlage und Parteien an ihre Adressen gekommen sind. Sie erhalten auf Anforderung Daten aus den kommunalen Melderegistern. Damit sind die Adressbuchverlage und Parteien gegenüber anderen gesellschaftlichen Gruppen privilegiert.

Dieser Umgang mit Meldedaten ist weder transparent noch angemessen. Die Konferenz tritt dafür ein, die Rechte der Bürgerinnen und Bürger zu verbessern. Die Information über die Widerspruchsmöglichkeit erreicht die Menschen häufig nicht. Vorzuziehen ist deshalb eine Einwilligungslösung. Sie würde das Grundrecht auf informationelle Selbstbestimmung konsequent umsetzen - erst fragen, dann handeln. Nach der Einwilligungslösung ist eine Erklärung informierter Bürgerinnen und Bürger gegenüber dem Meldeamt nötig, ob sie mit den Datenweitergaben an die genannten Empfänger einverstanden sind oder nicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt den gesetzgebenden Körperschaften, künftig die Einwilligungslösung vorzusehen.

19.14 Dringlichkeit der Datenschutzmodernisierung

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt und unterstützt grundsätzlich die vom 62. Deutschen Juristentag (DJT) im September 1998 in Bremen gefaßten Beschlüsse zum Umgang mit Informationen einschließlich personenbezogener Daten. Von den gesetzgebenden Körperschaften erhofft sich die Konferenz die Berücksichtigung dieser Beschlüsse bei der nunmehr dringend erforderlichen Umsetzung der EG-Datenschutzrichtlinie in Bundes- und Landesrecht.

Insbesondere betont die Konferenz folgende Punkte:

- Die materiellen Anforderungen des Datenschutzrechts sind angesichts der wachsenden Datenmacht in privater Hand auf hohem Niveau grundsätzlich einheitlich für den öffentlichen wie für den privaten Bereich zu gestalten.
- Die anlaßfreie Aufsicht für die Einhaltung des Datenschutzes im privaten Bereich muß in gleicher Weise unabhängig und weisungsfrei ausgestaltet werden wie die Datenschutzkontrolle bei öffentlichen Stellen.
- Die Rechte der Bürgerinnen und Bürger sind zu stärken; als Voraussetzung für die Ausübung des Rechts auf informationelle Selbstbestimmung der Betroffenen sind die Verpflichtungen zu ihrer Information, Aufklärung und ihren Wahlmöglichkeiten ohne faktische Zwänge auszuweiten.

- Ein modernisiertes Datenschutzrecht hat die Grundsätze der Datenvermeidung, des Datenschutzes durch Technik, der Zweckbindung der Daten und ihres Verwendungszusammenhangs in den Mittelpunkt zu stellen.
- Zur Sicherstellung vertraulicher und unverfälschter elektronischer Kommunikation ist die staatliche Förderung von Verschlüsselungsverfahren geboten, nicht eine Reglementierung der Kryptographie.

19.15 Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über ihre Freistellungsaufträge

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998

Die Datenschutzbeauftragten des Bundes und der Länder betonen das Recht der Bürgerinnen und Bürger auf Auskunft über ihre Daten auch gegenüber der Finanzverwaltung (§ 19 BDSG). Die Betroffenen haben Anspruch, von dem Bundesamt für Finanzen Auskunft über die Freistellungsaufträge zu erhalten, die sie ihrer Bank im Zusammenhang mit dem steuerlichen Abzug von Zinsen erteilt haben.

Der Bundesbeauftragte für den Datenschutz hat die Verweigerung der Auskünfte gegenüber dem Bundesministerium der Finanzen beanstandet und dieses aufgefordert, den entsprechenden Erlaß an das Bundesamt aufzuheben. Bisher hat das Ministerium in der Sache allerdings nicht eingelenkt.

Für die Betroffenen ergibt sich hierdurch ein unhaltbarer Zustand. Ihnen wird die Auskunft zu Unrecht vorenthalten.

Die Datenschutzbeauftragten der Länder unterstützen mit Nachdruck die Forderung des Bundesbeauftragten für den Datenschutz gegenüber dem Bundesministerium der Finanzen, seinen Erlaß an das Bundesamt für Finanzen aufzuheben und dieses anzuweisen, dem Auskunftsanspruch der Auftraggeber von Freistellungsaufträgen nachzukommen.

19.16 Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998

Die Datenschutzbeauftragten des Bundes und der Länder stellen fest, daß in der Praxis die Abgrenzung ihrer Zuständigkeiten bei den Gerichten immer wieder Anlaß von Unsicherheiten ist. Sie weisen daher darauf hin, daß die Beschränkung der Prüfkompetenz bei den Gerichten einzig und allein den Zweck hat, den grundgesetzlich besonders geschützten Bereich der richterlichen Unabhängigkeit von Kontrollen freizuhalten.

Deshalb erstreckt sich die Kontrolle der Datenschutzbeauftragten bei den Gerichten u.a. auch darauf, ob die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung getroffen und eingehalten werden, insbesondere bei automatisierter Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder halten eine gesetzliche Klarstellung für hilfreich, daß Gerichte der Kontrolle des Bundesbeauftragten bzw. der Landesbeauftragten für den Datenschutz unterliegen, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

19.17 Entwicklungen im Sicherheitsbereich

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, daß die Sicherheitsbehörden in den vergangenen Jahren umfangreiche zusätzliche Eingriffsbefugnisse erhalten haben. Demgegenüber fehlen in weiten Teilen Erkenntnisse über die Wirksamkeit und Grundrechtsverträglichkeit der Anwendung dieser Instrumente, wie z.B. bei der Schleppnetzfahndung und der Ausweitung der Telefonüberwachung.

Die Datenschutzbeauftragten des Bundes und der Länder erwarten vom Bundesgesetzgeber und der Bundesregierung, daß die Erforderlichkeit und die Wirksamkeit aller Eingriffsbefugnisse anhand objektiver Kriterien überprüft werden (Evaluierung).

Index

Abkürzungsverzeichnis

AO	Abgabenordnung
BAT	Bundesangestelltentarifvertrag
BDSG	Bundesdatenschutzgesetz
BIOS	Basis-Betriebssystem eines PC als Voraussetzung für den technischen Zugriff auf die einzelnen Komponenten (braucht nicht installiert zu werden, da es zur Grundausstattung gehört)
BSHG	Bundessozialhilfegesetz
Bus/Ethernet	Vernetzung mit standardisierter Datenübertragung, bei der alle Rechner an verschiedenen Stellen auf einer einzigen Leitung angebunden sind
BVB	Besondere Vertragsbedingungen zur Regelung der Beziehungen der öffentlichen Hand mit privaten Auftragnehmern (z.B. Miete, Kauf, Wartung, Pflege usw.)
BverfG	Bundesverfassungsgericht
BverwG	Bundesverwaltungsgericht
BZRG	Bundeszentralregistergesetz
debis	Daimler-Benz-Informations-System GmbH
DIPOL	Automatisiertes Informationssystem der Polizei
DNA	Desoxyribonukleinsäure-Analyse (Molekular genetische Untersuchung)
dSS	debis-Systemhaus-Saar: Gemeinschaftsunternehmen zwischen debis und dem Saarland zur Erbringung von EDV-Dienstleistungen
DV	Datenverarbeitung
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
EGStPO	Einführungsgesetz zur Strafprozeßordnung
eMail	elektronische versandte Post
EU	Europäische Union
EUROPOL	Europäisches Polizeiamt

Firewall	rechnergestützte Datenfilterung beim Übergang zwischen zwei Netzen; in der Regel in Verbindung mit dem Internet
FISCUS	in Entwicklung befindliches bundeseinheitliches Steuerverfahren
GEMA	Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte
GG	Grundgesetz
GMBl	Gemeinsames Ministerialblatt des Saarlandes
Homepage	Informationsangebot im Internet mit Darstellung des Anbieters
Hub	technische Komponente eines Netzwerks zur Verbindung von Leitungen
Intranet	Internes Datenkommunikationssystem auf Basis der Internet-Technologie ohne Anbindung an das Internet
IT	Informationstechnik
IT-GSHB	IT-Grundschutzhandbuch des BSI (Bundesamt für die Sicherheit in der Informationstechnik) mit Maßnahmeempfehlungen für den mittleren Schutzbedarf
KSVG	Kommunalselbstverwaltungsgesetz
LBO	Landesbauordnung
LfD	Landesbeauftragter für Datenschutz
Link	Adreßverweis im Internet
LVA	Landesversicherungsanstalt
MBKW	Ministerium für Bildung, Kultur und Wissenschaft
MdI	Ministerium des Innern
MdJ	Ministerium der Justiz
MDK	Medizinischer Dienst der Krankenversicherung
MDStV	Mediendienste-Staatsvertrag
MeldDÜV	Meldedaten-Übermittlungsverordnung
MFAGS	Ministerium für Frauen, Arbeit, Gesundheit und Soziales
MG	Meldegesetz
MiStra	Anordnung über Mitteilungen in Strafsachen
MUEV	Ministerium für Umwelt, Energie und Verkehr
MWF	Ministerium für Wirtschaft und Finanzen
NJW	Neue Juristische Wochenschrift
OrgKG	Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität
PGP	Pretty good privacy: international bekanntes Verschlüsselungsverfahren, das mit öffentlichen und privaten Schlüsseln arbeitet
Pkw	Personenkraftwagen

RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
SBG	Saarländisches Beamtengesetz
SDSG	Saarländisches Datenschutzgesetz
SGB	Sozialgesetzbuch
SKHG	Saarländisches Krankenhausgesetz
SL	Saarland
SPersVG	Saarländisches Personalvertretungsgesetz
SSL	Secure Socket Layer: gesichertes Übertragungsverfahren im Internet
Stern/Ethernet	Vernetzung mit standardisierter Datenübertragung, bei der mehrere Leitungen über ein Hub als Verbindungsglied so gekoppelt werden, daß logisch praktisch ein einziger Bus (aus mehreren Teilleitungen) entsteht.
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
TAN	Transaktionsnummer; nur einmal verwendbare Zahlengruppen zur Authentifizierung von kritischen Aktivitäten über ein Datennetz
TB	Tätigkeitsbericht
TDSV	Telekommunikationsdiensteunternehmen-Datenschutzverordnung
TÜ	Überwachung der Telekommunikation
TZ	Textziffer
VIPA	Informationssystem als "virtuelles" Prüfungsamt
X400	Austauschsystem für elektronische Post auf Basis der Norm X400
ZDV/ZDV-Saar	Zentrale Datenverarbeitung Saar; Betrieb des Landes zur Erbringung von EDV-Dienstleistungen im Geschäftsbereich des Ministeriums für Wirtschaft und Finanzen
ZPO	Zivilprozeßordnung