LANDTAG DES SAARLANDES
11. Wahlperiode

Drucksache 11/1103

SECHZEHNTER BERICHT

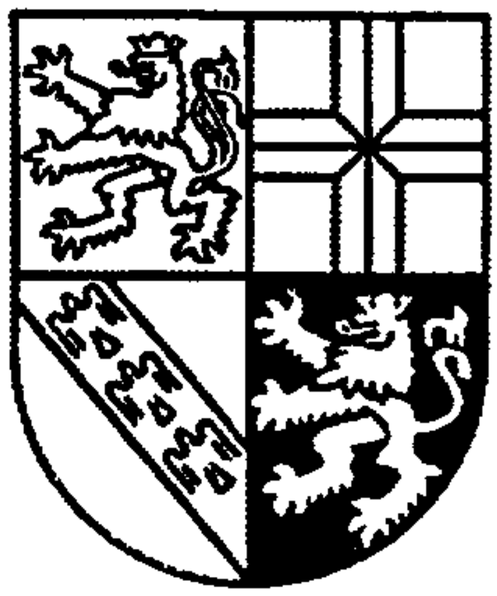
über die

Tätigkeit des Landesbeauftragten für Datenschutz gemäß § 27 des Saarländischen Gesetzes zum Schutz personenbezogener Daten
(Berichtszeitraum: 1995/1996)

Ausgegeben: 11.03.97

SAARLAND

DER LANDESBEAUFTRAGTE FÜR DATENSCHUTZ



16. Tätigkeitsbericht

1995/1996

Der vorliegende Bericht gibt Aufschluß über die Tätigkeit des Landesbeauftragten für Datenschutz in den Jahren 1995 und 1996.

Er wird gemäß § 27 des Saarländischen Datenschutzgesetzes dem Landtag und der Landesregierung zugeleitet und als Drucksache 11/1103 veröffentlicht.

Der Bericht kann selbstverständlich kein umfassendes Bild der Arbeit meiner kleinen Dienststelle zeichnen. Die aufgezeigten Einzelfälle geben vielmehr nur beispielhaft das Bemühen wieder, bei den öffentlichen Stellen im Saarland mit Hilfen und Kontrollen darauf zu dringen, daß die Persönlichkeitsrechte der Bürger gewahrt sind. Weiter werden Anregungen für normative und organisatorisch - technische Maßnahmen genannt.

Trotz erheblicher Fortschritte ist das Grundrecht auf informationelle Selbstbestimmung nicht hinreichend gesichert. Neue Entwicklungen gerade in der automatisierten Datenverarbeitung erfordern Aufmerksamkeit und neuen Schutz.

Wichtig ist auch, daß die Bürger selbst die Risiken erkennen und sich über die vorhandenen Sicherungen informieren können. Hierzu soll die Veröffentlichung dieses Berichtes beitragen.

Saarbrücken, im Februar 1997

(Bernd Dannemann)

Herausgeber:
SAARLAND Der Landesbeauftragte für Datenschutz
Fritz-Dobisch-Straße 12, 66111 Saarbrücken Postfach 102631, 66026 Saarbrücken
Tel.: (0681) 503 415 Fax.: (0681) 498 629 eMail: lfd-saar@t-online.de
Internet-Angebot unter: http://www.saarland.de/dschutz/LfD.html

Inhaltsverzeichnis

1 Vorbemerkung

Der vorliegende Bericht wird erstmals nicht mehr von Dr. Gerhard Schneider verantwortet, der am 3. 10. 1978 zum ersten Datenschutzbeauftragten des Saarlandes ernannt worden war und dieses Amt über lange Jahre wahrgenommen hat.

Als damals zuständiger Referent hatte Herr Dr. Schneider bereits maßgeblichen Anteil an Vorbereitung und Umsetzung des Saarländischen Datenschutzgesetzes vom 17. Mai 1978. Seine unbestrittene Fachkompetenz auf diesem noch jungen Rechtsgebiet ließ damals naheliegend erscheinen, ihm auch die Kontrolle über die Beachtung des Datenschutzes bei öffentlichen Stellen zu übertragen. In drei Amtsperioden wurde er von der seinerzeit zuständigen Landesregierung bestellt; die jeweils einhellige Zustimmung des Landtages stärkte seine unabhängige Stellung gegenüber der Exekutive. Das Innenministerium betraute ihn auch mit der Wahrnehmung von Aufgaben der Aufsichtsbehörde im nicht-öffentlichen Bereich. Als 1993 das Datenschutzgesetz geändert und der Landesbeauftragte dem Landtag zugeordnet wurde, war aufgrund Sachkunde, Erfahrung und Persönlichkeit des bisherigen Amtsinhabers selbstverständlich, daß es keinen Wechsel gab.

Gleichzeitig mit der Kontrollaufgabe hatte er zunächst dafür zu sorgen, die Funktion durch Aufbau der kleinen Dienststelle arbeitsfähig zu machen. Trotz einiger Schwierigkeiten, die er in seinen Tätigkeitsberichten beklagen mußte, gelang dies weitgehend, auch dank der Unterstützung durch motivierte Mitarbeiter. Die für die Aufgabe eigentlich gebotene personelle Ausstattung, die immer noch aussteht, hat er nicht erreichen können.

Herr Dr. Schneider hat sich mit großem Engagement für die Fortentwicklung des Datenschutzes im Saarland eingesetzt. Seine Vorschläge, Hilfen, aber auch seine Kritik an bestehenden und geplanten Verfahren und Normen haben viel zur Verwirklichung des Grundrechtes beigetragen und die Verwaltungskultur mitgeprägt. Nicht alle seine Initiativen fanden in der praktischen Arbeit von Parlament und Verwaltung tatsächlichen Niederschlag. Zu grundlegender Entmutigung hat dies gleichwohl nicht geführt. Den öffentlichen Stellen gegenüber blieb er stets ein hilfreich - kritischer,

gelegentlich auch streitbarer Kontrolleur, den Bürgern gegenüber ein aufgeschlossener Ombudsmann bei Wahrnehmung ihrer Rechte. Bei den Kollegen der übrigen Länder und des Bundes hat er sich in der Mitarbeit an übergreifenden Problemen große Anerkennung erworben.

Nachdem Herr Dr. Schneider im Frühjahr 1995 in den verdienten Ruhestand getreten war, hat für eine längere Zwischenzeit Frau Ministerialrätin Metscher als Vertreterin neben ihren sonstigen Aufgaben die Dienststelle geführt und hierbei viel Geschick bewiesen. Ihr sei an dieser Stelle herzlich dafür gedankt.

Am 8. November 1995 hat mich der Landtag des Saarlandes mit breiter Mehrheit als neuen Landesbeauftragten gewählt. Der Wahl lag, wie gesetzlich vorgeschrieben, ein Vorschlag der Landesregierung zugrunde, die hierbei meine bisherige Tätigkeit innerhalb der Staatskanzlei und verschiedener Ministerien einbeziehen konnte.

Im Zusammenhang mit der Wahl wurde Kritik an dieser gesetzlichen Regelung geäußert. Stimmenthaltungen, die auf die Bindung an einen Vorschlag der Landesregierung bezogen waren, werte ich als Bemühen, im Interesse eines möglichst effektiven Schutzes für die Rechte der Bürgerinnen und Bürger die unabhängige Stellung des Landesbeauftragten zu stärken. Denn die Kontrolltätigkeit bei öffentlichen Stellen, für deren Handeln die Landesregierung unmittelbar oder über ihre Aufsichtsbefugnisse Mitverantwortung trägt, führt notwendigerweise zu unterschiedlicher, oft kritischer Bewertung. Der Landesbeauftragte kann sie um so unbefangener wahrnehmen, je mehr er sich des Vertrauens des Parlaments gewiß sein kann und je geringer die auch nur theoretische Gefahr unsachlicher Einflußnahme ist.

In Konsequenz der Kritik hat eine Landtagsfraktion 1996 eine Änderung des SDSG mit dem Ziel vorgeschlagen, die Wahl künftig auf Vorschlag der Fraktionen und mit qualifizierter Mehrheit vorzunehmen; weiter sollten Unabhängigkeit und Vertrauen bei der Bevölkerung in die sachliche Amtsführung dadurch gestärkt werden, daß ihm keine andere Amts-, Berufs- oder Mandatstätigkeit erlaubt wird. Dieser Vorschlag fand indes nicht die Mehrheit des Landtags.

Ich will betonen, daß es in meiner bisherigen Tätigkeit zu keinem Versuch einer unsachlichen Einflußnahme gekommen ist. Gleichwohl hätte ich für die Zukunft die Umsetzung dieses Änderungsvorschlags begrüßt, weil er auch institutionell die vorausgesetzte Freiheit bestärkt hätte.

Selbstverständlich werde ich, wie es mir aufgetragen ist, auch nach geltendem Recht mein Amt unabhängig, unparteiisch und ohne jede Rücksichtnahme auf etwaige „Erwartungen" wahrnehmen. Erwarten können aber die Bürger, deren Persönlichkeitsrechte meiner Aufmerksamkeit anvertraut sind, daß ich für ihre Interessen Partei ergreifen und mich um einen angemessenen Umgang der Verwaltungen mit ihren Daten bemühen werde.

Entsprechend müssen die Verwaltungen erwarten, daß ich ihr Handeln kritisch beobachten werde. Das Ziel meiner Tätigkeit sehe ich aber vornehmlich nicht darin, mit ihnen die Konfrontation zu suchen. Primär gilt es, ihre Überzeugung zu stärken, daß Grundrechtsschutz für die Bürger auch ihre Aufgabe ist, den sie mit Blick allein auf eine effektive Bewältigung der Sachaufgaben nicht vernachlässigen dürfen. Soweit möglich, möchte ich mit Hilfen für angemessene Maßnahmen hierzu beitragen. Gelingt dies nicht, muß selbstverständlich der Mangel deutlich bezeichnet und an politisch verantwortlicher Stelle Abhilfe eingefordert werden.

Der festgelegte Zweijahreszeitraum für den Bericht bringt mit sich, daß nur ein Teil der aufgeführten Ereignisse und Tätigkeiten in die Amtszeit des neugewählten Landesbeauftragten fällt. Dies ist objektiv kein Problem, weil es ja um die Funktion des LfD und nicht den Amtsinhaber geht. Ich sehe aber auch für mich persönlich keine Schwierigkeiten, die von meinem Amtsvorgänger eingenommene Haltung aufzunehmen und meist in gleicher Weise fortzuführen. Dem entspricht, wenn ich im Schriftverkehr und auch im Bericht sprachlich regelmäßig nicht danach differenziere, ob Herr Dr. Schneider, in der Zwischenzeit Frau Metscher oder ich selbst verantwortlich waren.

2 Erörterungen im Ausschuß für Datenschutz

Gemäß § 27 SDSG legt der Landesbeauftragte seine Tätigkeitsberichte dem Landtag und der Landesregierung vor. Im Ausschuß für Datenschutz

werden Einzelaspekte mit den Vertretern der Ressorts und ggf. der Behörden diskutiert, nachdem die Landesregierung schriftlich zum Tätigkeitsbericht Stellung genommen hat. Zur Sprache kommen hierbei vornehmlich solche Themen, die zwischen LfD und Landesregierung fortdauernd unterschiedlich bewertet werden, auch wenn dies selbstverständlich kein zutreffendes Bild vom „Alltag" der Datenschutzkontrolle zuläßt.

Eine abschließende Sachentscheidung in dem Sinn, daß bestimmte Auffassungen für verbindlich erklärt werden, ist dabei entsprechend dem grundsätzlichen Charakter eines Ausschusses weder den Ressorts gegenüber noch dem LfD wegen dessen Unabhängigkeit möglich. In den nicht seltenen Fragen etwa, in denen es um die rechtliche Bewertung einer bestimmten Datenverarbeitung durch öffentliche Stellen geht, könnte einem Parlamentsausschuß auch schwerlich eine „Streitentscheidung" zukommen. Selbst mit „Billigung" des Ausschusses bliebe eine unzulässige Datenverarbeitung dem Bürger gegenüber eine Grundrechtsverletzung.

Die Erörterung im Ausschuß kann und soll aber dazu führen, den Abgeordneten Ansätze und Hilfen für eigenes parlamentarisches Handeln zu geben. Einerseits kann die Notwendigkeit deutlich werden, eine gesetzliche Regelung abweichend oder neu zu treffen; andererseits kann der Hinweis auf fehlerhafte Verwaltungstätigkeit Anlaß geben, mit den parlamentarischen Kontrollrechten auf die Exekutive einzuwirken. In der Regel werden die Vertreter der Ressorts entsprechende Signale der „ersten Gewalt" auch den Ausschußsitzungen selbst entnehmen können. Deshalb halte ich es für sinnvoll, wenn der Ausschuß unter Würdigung der vorgetragenen Standpunkte in geeigneten Fällen ausdrückliche Bitten an die Vertreter der Landesregierung formuliert.

Überdies wäre aber sicher - auch zur breiteren Information und zur weiteren Verankerung des Datenschutzes in der Bevölkerung - hilfreich, wenn auch das Plenum des Landtages selbst sich mit der Praxis der Datenverarbeitung bei den öffentlichen Stellen befaßte, etwa in Form eines regelmäßig vom Ausschuß gegebenen Berichtes, wie ihn auch der Ausschuß für Eingaben erstattet.

Im Berichtszeitraum behandelte der Ausschuß in fünf Sitzungen die beiden Tätigkeitsberichte über die Jahre 1992 bis 1994 (14. und 15. TB) und griff auf meine Anregung auch Einzelthemen aus den vorher noch nicht erörterten Berichten über die Jahre 1990 und 1991 auf (12. und 13. TB). Daneben bestand Gelegenheit, im Ausschuß Schwerpunkte des präventiven Datenschutzes vornehmlich im technisch - organisatorischen Bereich vorzustellen.

Die ausdrücklich erklärte Bereitschaft des Ausschusses, sich auch außerhalb der Behandlung von Tätigkeitsberichten mit Fragen des Datenschutzes zu befassen, begrüße ich sehr. Ich vertraue darauf, die Mitglieder stets als aktive Streiter für die Persönlichkeitsrechte der Bürgerinnen und Bürger auf deren Seite zu wissen.

3 Ausgangslage und Perspektiven

Um Schwerpunkte der künftigen Arbeit zu entwickeln, war es für mich als neuen Datenschutzbeauftragten zunächst wichtig, sich ein Bild über die Ausgangslage zu machen.

3.1 Stand des Datenschutzes

18 Jahre nach Erlaß des ersten Datenschutzgesetzes im Saarland ist dieses Rechtsgebiet „volljährig" geworden. Die allgemeinen Grundnormen liegen - zusammen mit dem etwa gleichaltrigen Bundesdatenschutzgesetz - vor; die Landesverfassung selbst nennt jedenfalls in einer Grundnorm ausdrücklich den Anspruch des einzelnen auf Schutz seiner personenbezogenen Daten und verpflichtet damit unmittelbar alle Staatsgewalten. Für viele Rechtsgebiete gibt es in den Fachgesetzen inzwischen die gebotene fachspezifische Datenschutzordnung, wo eine präzisere oder von den allgemeinen Normen abweichende Regelung erforderlich erscheint, und der Aspekt Datenschutz wird bei anstehenden Novellen normalerweise mitbeachtet. Allerdings gibt es nach wie vor Bereiche, für die eine gesetzesförmliche Abwägung zwischen Einzel- und Gemeinschaftsinteressen noch gänzlich fehlt oder unzureichend ist.

Den Kinderschuhen entwachsen ist auch der Umgang der Verwaltungen mit diesem Grundrecht und den Vorschriften, die es konkretisieren und schützen sollen. Verwaltungsleitungen und Mitarbeiter kennen seine Bedeutung oder erkennen sie jedenfalls bei einem Hinweis. Großenteils gibt es auch organisatorische und technische Maßnahmen zu seinem Schutz. Daß die Verantwortlichen die Regeln völlig mißachten, ist ebenso selten wie der absichtliche Verstoß. Wohl aber fehlt es, wie wir bei Kontrollen und Eingaben Betroffener erfahren, vielfach an nötiger Sorgfalt und an Vorkehrungen gegen Nachlässigkeit.

Damit spiegeln Tätigkeit des Gesetzgebers und Verwaltungshandeln der öffentlichen Stellen wider, daß auch in der Bevölkerung das informationelle Selbstbestimmungsrecht zwar zunehmend selbstverständlicher verankert erscheint, gleichwohl aber von anderen Prioritäten oft deutlich überlagert wird und dann im Bewußtsein nicht präsent ist.

Die erstaunliche Feststellung einer seriösen Umfrage, daß die Furcht der Bundesbürger vor einem Datenmißbrauch durch Adreßverlage stärker empfunden werde als Bedrohungen durch Kriminalität, Straßenverkehr und Umweltverschmutzung, macht zwar die Sensibilität der Bevölkerung für Fragen des Datenschutzes deutlich; sie steht jedoch in deutlichem Gegensatz dazu, daß viele Bürger selbst oft höchst leichtfertig mit ihren eigenen Daten umgehen. Deren nachlässige Verfahrensweise rührt oft daher, daß mögliche Gefahren auf Anhieb nicht zu erkennen sind. Ungenügende Anstrengungen der öffentliche Stellen kann sie indes keinesfalls rechtfertigen. Für diese gilt vielmehr der Anspruch aller Bürger, darauf vertrauen zu dürfen, daß ihre Grundrechte durch korrekten Umgang mit ihren Daten gewahrt bleiben.

Fortbestehende und teilweise gravierend zunehmende Gefährdungen dieses Rechts sehe ich insbesondere in folgenden Entwicklungen:

- Nicht allein quantitativ nimmt der Gebrauch solcher Techniken im privaten Bereich wie bei den öffentlichen Stellen zu, die mehr als konventionelle Bearbeitung zulassen, Einzeldaten zu umfassenden Bildern über den Menschen zusammenzufügen. Moderne Speicher- und Übertragungstechnologie erlaubt Anwendungen mit gegenüber früher ungleich höherer Leistungsfähigkeit. Damit lassen sich vielfach neuartige, in ihren Auswirkungen häufig nicht vollständig bekannte oder jedenfalls für

den Anwender nicht überschaubare Auswertungsmöglichkeiten nutzen, die auch der Gefahr unvorhersehbarer Angriffe und Manipulationen ausgesetzt sind. Umfassende Vernetzung droht die „informationelle Gewaltenteilung" aufzuheben, die der sichtbaren Organisation entspricht und dem einzelnen Bürger annähernd den Informationsfluß transparent werden läßt. Erst recht ist damit die Möglichkeit ernsthaft gefährdet, grundsätzlich selbst über die Verwendung seiner Daten zu bestimmen, mindestens aber die vom Gesetzgeber getroffene Abwägungsentscheidung nachvollziehen zu können.

- Kommunikationsbeziehungen werden weiträumiger, vielfach sogar international. Längst ist nicht mehr allein derjenige, der dem Bürger unmittelbar gegenübertritt, auch derjenige, in dessen Obhut seine Daten stehen oder der sie nutzt. Wo - wie bei Nutzung des weltweiten, nicht hierarchisch gegliederten Internet - gar nicht mehr festgestellt werden kann, an welchen Orten bestimmte Schritte in der Datenverarbeitung stattfinden und welche Verantwortungen hierfür bestehen, reicht der Schutz durch Rechtsvorschriften nicht aus, schon gar nicht auf allein nationaler Ebene.

- Den Verwaltungen werden immer mehr Leistungen abverlangt, die sie mit geringeren Kosten bewerkstelligen sollen. Der Zwang zu höherer Effizienz („schlanke Verwaltung") kann nicht allein durch personell-organisatorische Maßnahmen oder dadurch aufgefangen werden, daß menschliche Arbeitskraft durch Technik ersetzt wird. Notwendig wird vielmehr auch, Kosten in und bei der Leistungserfüllung zu vermeiden. „Abbau von Standards" heißt das Schlagwort; betroffen hiervon sind besonders natürlich Rahmenbedingungen, die außer Betracht bleiben, wenn nur die Effizienz der „eigentlichen" Aufgabenerfüllung betrachtet wird. Leider gerät dann der Datenschutz in Gefahr, als Luxusziel betrachtet zu werden, das wir uns in wirtschaftlich guten Zeiten leisten konnten, nicht aber in angespannter Haushaltslage.

- Vornehmlich der Wirtschaftlichkeitsdruck läßt die öffentlichen Stellen zudem nach Chancen suchen, Kosten- oder sonstige Vorteile durch andere rechtliche Gestaltungsformen, durch Auslagerung von Aufgaben oder in Zusammenarbeit mit anderen öffentlichen oder privaten Einrichtungen zu erzielen. „Outsourcing", das Verlagern von bisher in der öffentlichen Stelle selbst vorgenommenen Verarbeitungsschritten

an andere Stellen oder die Wahrnehmung in formal anderer Rechtsform berührt auch die besonderen Bindungen, die gerade den öffentlichen Stellen auferlegt sind. Mag auch bei Wahl der Gestaltungsform der Aspekt des Datenschutzes meist nicht im Vordergrund stehen, muß doch vermieden werden, daß Grundrechtsschutz für die Bürger sich mit geringeren materiellen Anforderungen oder niedrigerer Kontrolldichte vermindert.

3.2 Folgerungen

In dieser Situation muß auch „der Datenschutz" sich daraufhin überprüfen lassen, ob die Ziele und ob Regelungsmechanismen und Kontrollinstrumente, wie sie vor allem in den letzten 20 Jahren entwickelt worden sind, einer Anpassung bedürfen.

– Das Recht auf Privatheit, bezogen auf Datenverarbeitung ausgeprägt als „informationelle Selbstbestimmung", wie es das Bundesverfassungsgericht formuliert hat, ist altes und auch künftig unverzichtbares Menschenrecht. Freiräume privater Existenz sind lebenswichtig. Sie müssen zur Bindung des sonst übermächtigen Staates nicht nur diesem gegenüber gesichert werden; weil zunehmend umfassende Kenntnisse über höchst sensible Daten in privater Hand zusammenlaufen, muß der Staat zugleich zum Garanten für die Freiheitsrechte seiner Bürger werden.

  Diese Verpflichtungen haben höchsten Rang und gelten nicht nur bei „schönem Wetter"; sie sind nicht beliebig anderen - natürlich ebenfalls legitimen und wichtigen - Zielen in der Prioritätenfolge nachzuordnen. Die Aussage, wir könnten uns Datenschutz nicht mehr leisten, ist hierbei ebenso falsch wie der Verweis auf die Bereitschaft vieler Bürger, umfassende Kontrollbefugnisse hinnehmen zu wollen, wenn es um die Sicherheit oder die gerechte Verteilung von Ressourcen geht. Abstriche am Ziel kann es also nicht geben.

– Instrumentarium für den gebotenen Grundrechtsschutz ist selbstverständlich weiterhin in erster Linie das Gesetz. Individualrechte gegen andere Rechte und Ziele generell abzuwägen, ist dem Parlament vorbehalten. Für dieses ist Normsetzung die klassische Handlungsmög-

lichkeit. Rechtsnormen setzen staatlicher und privater Übermacht Grenzen, schaffen für alle die gebotene Transparenz und wirken damit unmittelbar und mittelbar auf das Verhalten ein. Soweit Gefahren von außen drohen oder Verarbeitung außerhalb des eigenen Einwirkungsbereichs stattfindet, sind über den nationalen Rahmen hinausreichende Normen oder die Vereinbarung gleichwertiger Schutzstandards nötig.

Gerade im Bereich öffentlicher Stellen bleibt unverzichtbar, von vornherein strikte und eindeutige Regelungen vorzugeben, die parlamentarisch verantwortet sind. Die Verwaltungen dürfen sich nicht beliebig Befugnisse zur Datenverarbeitung, die ihnen der Gesetzgeber nicht zugesteht, über die Einwilligung der Betroffenen einräumen lassen, erst recht dann nicht, wenn sie damit Ziele verfolgen wollen, die für die umrissenen Aufgaben der Stellen im strengen Sinn nicht erforderlich sind. Tendenzen hierzu sind aber erkennbar. Zwar verwirklicht die eigene Entscheidung des Bürgers seine informationelle Selbstbestimmung; im Verhältnis zu öffentlichen Stellen geschieht dies aber häufig unter faktischem Zwang, der echte Freiwilligkeit ausschließt.

- Die bloße Existenz von Vorschriften, die die rechtliche Zulässigkeit von Datenverarbeitung bestimmen, reicht indes nicht aus. Normen entfalten sich nur, wenn die Mitarbeiter in den datenverarbeitenden Stellen sie kennen und mit Überzeugung anwenden. Das SDSG schreibt bewußt anstelle einer nur formelhaften Verpflichtung der Mitarbeiter vor, daß das Personal zu „unterrichten" ist. Hierzu bedarf es einer ausreichenden Schulung und Fortbildung, die von den anwendenden Stellen und ihren Fortbildungseinrichtungen zu gewährleisten ist. Der Landesbeauftragte kann hier lediglich erste Hinweise geben und erinnern.

- Das Verantwortungsbewußtsein der datenverarbeitenden Stellen, denen ja der Grundrechtsschutz obliegt, kann weiter mit geeigneten organisatorischen Vorgaben gestärkt werden. Für den nicht-öffentlichen Bereich schreibt das Bundesdatenschutzgesetz die Bestellung betrieblicher Datenschutzbeauftragter vor; im öffentlichen Bereich muß eine solche Eigenkontrolle nur eingeschränkt, beispielsweise bei den Sozialversicherungsträgern, eingerichtet werden. Zunehmend gehen allerdings auch im Saarland öffentliche Stellen aufgrund untergesetzlicher Anordnung oder eigener Entscheidung dazu über, behördliche Datenschutzbeauftragte zu bestellen. Mir erscheint sinnvoll, die Einrichtung

einer solchen Stelle künftig verbindlich zu machen; zu erwägen wäre, dort auch das Dateienregister zu führen, das an zentraler Stelle beim LfD vom Bürger kaum als Informationsquelle genutzt wird.

– Schließlich ist für die Art der Datenschutzkontrolle zu fragen, ob die Schwerpunkte der Datenschutzkontrolle nicht verschoben werden sollten. Auch im Hinblick auf die nur begrenzten Kapazitäten halte ich für zweckmäßig, meine eigene Kontrolltätigkeit zeitlich vorzuverlagern, sie also mehr als Beratungs- und Hilfsinstrument zu verstehen als in der Funktion, Fehler aufzuspüren und aufzugreifen. Das SDSG sieht eine Vorab-Beteiligung ja vor, soweit es bei den öffentlichen Stellen um Verwaltungsvorschriften und um die Freigabe automatisierter Verfahren zur Verarbeitung personenbezogener Daten geht (§ 8 Abs. 1 und 2).

In geeigneten Fällen ist aber zweckmäßig, nicht erst auf eine konkrete Beteiligung zu warten, sondern unsere Kenntnisse und Erfahrungen bereits unabhängig hiervon den Anwendern in Form von Mustertexten oder Arbeits- und Orientierungshilfen zur Verfügung zu stellen. Für die einzelnen Stellen, die oft nicht regelmäßig mit solchen Verfahren befaßt sind, helfen auch Checklisten und standardisierte Abläufe, ihre Aufgaben zu erfüllen. Für Maßnahmen im technisch-organisatorischen Datenschutz habe ich verstärkt solche Hilfen verfügbar gemacht und hierfür bei den Stellen positive Resonanz gefunden. Mit gleicher Zielsetzung, durch möglichst frühzeitiges Einwirken auf die Ausgestaltung automatisierter Verfahren zu gewährleisten, daß die im Saarland geltenden Datenschutzvorschriften eingehalten werden, kommt in Einzelfällen auch Kontakt mit externen Programmentwicklern in Betracht, die häufig für mehrere Stellen Anwendungen erstellen.

Weil auf diesem Weg ein breiterer Kreis erreicht und damit letztlich „mehr" Datenschutz verwirklicht werden kann, als mit bloßen (nachträglichen) Kontrollen, halte ich trotz unserer geringen Ressourcen einen solchen Schwerpunkt für sinnvoll und beteilige mich auch aktiv an solchen Aktivitäten in der Landesverwaltung und vergleichbaren Bestrebungen der Kollegen.

– Selbstverständlich muß es aber auch künftig bei Kontrollen „herkömmlicher" Art verbleiben, für die ein konkreter Anlaß nicht bestehen muß. Auch bei diesen ist allerdings mein Bemühen, vor allem den

Schutz der Persönlichkeitsrechte in der zukünftigen Arbeit der Stelle im Auge zu haben und bei festgestellten Schwachstellen nach Möglichkeit konkrete Hilfen zu geben.

– Immer mehr aber erweist sich, daß Rechtsnorm und Kontrolle nicht mehr ausreichen, die mit neuartigen Techniken neu und gesteigert auftretenden Risiken für das informationelle Selbstbestimmungsrecht zu bändigen. Diese Risiken zeigen sich beispielsweise in breiten Datenspuren, die Bürger hinterlassen, wenn sie neue Kommunikationstechniken und Chipkarten einsetzen. Private wie öffentliche Stellen sind in Versuchung, einmal verfügbare Daten unabhängig von der ursprünglichen Zweckbestimmung zu nutzen.

Hier gilt es zu vermeiden, daß überhaupt derartige Spuren zwingend gelegt und bewahrt werden. Alternativen müssen aufgezeigt und ggf. entwickelt werden für die Bürger, die nicht - trotz Kenntnis der Gefahren - die Risiken bewußt eingehen wollen. Datenvermeidung und Datensparsamkeit muß Grundsatz auch bei den Techniken und Verfahren selbst sein. Hierbei zeigt sich, daß Technik nicht allein zusätzliche Gefahren schafft, sondern sich einsetzen läßt, um eben diese auszuschließen oder herabzusetzen. Die Chancen, etwa mit Sicherheitsprodukten, Verschlüsselung, digitaler Signatur, anonymen Verfahren, intelligenten Chipkarten für die Bürger gerade ein „Mehr" an Schutz der informationellen Selbstbestimmung zu erreichen, sollten gefördert und auch unter staatlichen Sicherheitsinteressen nicht unangemessen behindert werden. Die Datenschutzbeauftragten können hier aus ihren Erfahrungen anregend tätig werden.

– Wird für die einzelnen Bürger die Alternative deutlich, könnte sogar die Technik mit größerem Datenschutzstandard bei ihnen höhere Akzeptanz erhalten; Anwendungen, die den höheren Standard gewährleisten, könnten damit Wettbewerbsvorteile erzielen. Vorentwürfe für einen Rechtsrahmen bei Multimediaanwendungen sahen beispielsweise eine Zertifizierung ähnlich dem Öko-Audit vor. Auch wenn es hierzu nicht kommt: die Überlegung ist deswegen interessant, weil sie das Augenmerk wieder darauf lenkt, daß Schutz des informationellen Selbstbestimmungsrechts am Betroffenen auszurichten ist. Zu Recht hebt die EU-Datenschutzrichtlinie hervor: „Die Informationssysteme stehen im Dienst des Menschen". Deshalb bleibt wichtig, daß die Bürger selbst

die hohe Qualität des Grundrechtes wahrnehmen und nicht allein darauf vertrauen, daß Kontrollbehörden sich um den Schutz sorgen.

4 Nutzung neuer Technik

Wegen der rasant voranschreitenden technischen Entwicklung erscheint es notwendig, auch in der Datenschutzkontrolle einen deutlichen Schwerpunkt auf diesen Aspekt zu richten. Dabei geht es sowohl darum, gesetzlich bestehende Regelungen und allgemein formulierte Ziele für den Technikeinsatz zu interpretieren, als auch darum, den anwendenden Stellen Risiken deutlich zu machen und mögliche Gegenmaßnahmen aufzuzeigen.

Ich finde mich hierbei in Übereinstimmung mit Kollegen, die diese Konsequenz für ihre Arbeit ebenso herausstellen. Deshalb beteiligt sich meine Dienststelle auch intensiv daran, in Abstimmung mit den übrigen Datenschutzbeauftragten entsprechende Hilfen auszuarbeiten. Für meine Tätigkeit kommt - wie dargestellt - meine Hoffnung hinzu, gerade mit frühzeitiger präventiver Beratung und Beteiligung im Ergebnis mehr an effektivem Datenschutz erreichen zu können als mit nachträglicher Kontrolle.

Auf einige Aktivitäten, die - teilweise aus der gemeinsamen Arbeit - den Schwerpunkt technikbezogener Ausrichtung deutlich machen, sei nachfolgend hingewiesen:

4.1 Datenschutz durch Technik

Auf die Thematik „Datensparsamkeit durch moderne Informationstechnik - Datenvermeidung, Anonymisierung und Pseudonymisierung" haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer 52. Konferenz am 22./23. Oktober 1996 in Hamburg mit einem Kurzbericht in genereller Form auch die Öffentlichkeit hingewiesen (Anlage 1).

Betont wird, daß die zunehmende Verbreitung, Nutzung und Verknüpfbarkeit von Informations- und Kommunikationstechnik mit sich bringt, daß jeder Benutzer immer mehr elektronische Spuren hinterläßt. Das wird da-

zu führen, daß er über Art, Umfang, Speicherort, Speicherdauer und Verwendungszweck der vielen über ihn gespeicherten Daten keine Kontrolle mehr hat, so daß die Gefahr des Mißbrauchs und der Zusammenführung zu komplexen Persönlichkeitsprofilen ständig zunimmt.

Dieser Gefahr kann dann begegnet werden, wenn in Zukunft die Frage nach der Erforderlichkeit personenbezogener Daten im Vordergrund steht, wobei Datensparsamkeit bis hin zur Datenvermeidung angestrebt werden muß. Durch die Nutzung neuer Möglichkeiten der modernen Informations- und Kommunikationstechnik (IuK-Technik) ist es in vielen Anwendungsfällen möglich, den Umgang mit personenbezogenen Daten zu reduzieren bis hin zur vollständigen Vermeidung. Auf diese Weise kann das Prinzip "Datenschutz durch Technik" umgesetzt werden. Datensparsamkeit und Datenvermeidung werden sich dabei auch zunehmend als Wettbewerbsvorteil erweisen.

Ausgehend von einer Untersuchung des niederländischen Datenschutzbeauftragten und des Datenschutzbeauftragten von Ontario/Kanada zum sogenannten Identity Protector beschäftigen sich derzeit die Datenschutzbeauftragten des Bundes und der Länder intensiv mit der Formulierung von Anforderungen zur datenschutzfreundlichen Ausgestaltung von IuK-Technik. Einige datenvermeidende Technologien wie die anonyme, vorausbezahlte Telefonkarte sind bereits seit längerer Zeit allgemein akzeptiert. Auf erste Ansätze der Datenvermeidung auf gesetzgeberischer Ebene im damaligen Entwurf zum Teledienstegesetz und zum Mediendienstestaatsvertrag wird verwiesen.

Die Datenschutzbeauftragten haben ihren Arbeitskreis "Technische und organisatorische Datenschutzfragen" beauftragt, einen Bericht mit Vorschlägen und Empfehlungen vorzulegen, wie unter Nutzung der modernen Datenschutztechnik das Prinzip der Datenvermeidung umgesetzt werden kann. Neben der Entwicklung entsprechender Hard- und Software werden Anonymisierung und Pseudonymisierung eine zentrale Rolle spielen. Bei der Erarbeitung dieses Berichtes werden Experten aus Wissenschaft und Forschung hinzugezogen, um die technische Entwicklung berücksichtigen zu können. Auch Vertreter der Wirtschaft als Entwickler und Anwender werden einbezogen, damit die Umsetzung der Vorschläge der Datenschutzbeauftragten als zukünftiger Wettbewerbsvorteil erkannt wird.

4.2 Chipkarten

Chipkarten, meist in der genormten Größe einer Eurocheque- oder Kreditkarte, finden im täglichen Leben der Bürger zunehmend Verbreitung und gewinnen weiter an Bedeutung. Aus der Sicht des Datenschutzes bedürfen sie zur Wahrung des informationellen Selbstbestimmungsrechts und der informationstechnischen Sicherheit größter Aufmerksamkeit.

Es handelt sich um miniaturisierte Computer, die über bloße Identifikation hinaus eigene Rechenleistungen bereitstellen. Die derzeit bekannteste Chipkarten-Anwendung ist die Telefonkarte. Ebenfalls allgemein bekannt ist die Krankenversicherungskarte (KVK), die zur Identifizierung des Patienten sowie zur Abrechnung ärztlicher Leistungen verwendet wird. Weitere neue Anwendungsbereiche von Chipkarten wie z. B. ein Einsatz im bargeldlosen Zahlungsverkehr oder als Gesundheits- bzw. Patientenchipkarten sind derzeit in der Diskussion bzw. in der Erprobung.

Aus technischer Sicht sind reine Speicherchipkarten zur Aufnahme von Daten von solchen Karten zu unterscheiden, in die Mikroprozessoren und speichernde Bauteile integriert sind. Die Nutzung solcher Chipkarten setzt die Verfügbarkeit von Kartenterminals voraus, die die Funktionalität der jeweiligen Chipkarte ausnutzen, indem sie Daten von der Karte abrufen oder dort ablegen. Dabei werden Chipkarten als Speichermedium für Daten (z. B. Kontodaten, medizinische Individualdaten), als Mittel zur Authentifizierung ihres Trägers für die Gewährung des Zugriffs auf sicherheitsrelevante Daten und Funktionen (Kontoverfügungen, Änderung medizinischer Individualdaten) und als Mittel zur Signatur von Dokumenten (Verträge, Willenserklärungen, Befunde etc.) genutzt.

Schwachpunkt bei der Chipkartennutzung ist die Identifizierung des Trägers, die derzeit vor allem durch einen Zahlencode, der PIN, abgesichert wird. Wird lediglich eine PIN verlangt und notieren Anwender, weil sie sich den Code nicht merken können, diesen irgendwo (vielleicht sogar auch der Chipkarte) auf, können von Unbefugten leicht Daten in Erfahrung gebracht oder Unterschriften unbemerkt gefälscht werden. Ob biometrische Sicherungsverfahren, z. B. eine Fingerabdruckerkennung, in absehbarer Zeit eingesetzt werden können, bleibt fraglich.

Für den datenschutzgerechten Einsatz von Chipkarten ist eine konsequente und überzeugende Sicherungstechnologie erforderlich. Um einem Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit entgegenzuwirken, müssen Datensicherungsmaßnahmen in ihrer Gesamtheit einen hinreichenden Schutz der Daten vor Mißbrauch gewährleisten. Vor der Entscheidung über den Einsatz von Chipkarten sollte eine Risikoanalyse durchgeführt werden, aus der ein Sicherheitskonzept abzuleiten ist.

Die Problematik des Chipkarteneinsatzes und Mindestanforderungen an den Chipkarteneinsatz aus datenschutzrechtlicher Sicht wurden in einer Orientierungshilfe des Arbeitskreises „Technik" der Datenschutzbeauftragten des Bundes und der Länder dargestellt, die in meinem Internetangebot (TZ 22.2) zur Verfügung steht.

4.3 Elektronische Geldbörse

Das elektronische Bezahlen mit Chip-, Magnetstreifen oder sonstigen Karten bringt Datenschutzrisiken neuer Qualität mit sich. Während man beim Bezahlen mit Bargeld anonym bleiben kann, hinterläßt man beim Bezahlen mit „elektronischen Geldbörsen" auch elektronische Spuren und setzt sich damit der Gefahr aus, daß Zahlungsdaten detailliert ausgewertet werden können.

Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung zum Datenschutz bei elektronischen Geldbörsen und anderen kartengestützten Zahlungssystemen ihre Forderungen zusammengefaßt (siehe Anlage 2). Anlaß dafür ist, daß über Modellversuche hinaus immer mehr angestrebt wird, mit Hilfe elektronischer Geldbörsen Bargeld zu ersetzen. So können bei der Deutschen Bahn AG Fahrscheine bereits heute bargeldlos erworben werden. Auch in saarländischen Kreditinstituten wird derzeit die Ausgabe von Chipkarten zur Nutzung als elektronische Geldbörse vorbereitet bzw. ist schon angelaufen.

Daten über die Nutzung von elektronischen Geldbörsen können zu Kundenprofilen verdichtet werden; die Speicherung von Ort, Zeitpunkt, Anlaß und Betrag der Kartenbenutzung läßt die Erstellung von Bewegungsprofilen und die Auswertung von Kaufgewohnheiten zu. Daß solche Daten jedenfalls für die werbende Wirtschaft von Interesse sind, liegt auf der

Hand; sie könnten auch auf das Interesse von Polizei und Staatsanwaltschaft, von Finanzämtern und Arbeitgebern stoßen. Dadurch besteht die Gefahr, daß der datenfreie Raum, in dem sich der Bürger unbeobachtet verhalten und bewegen kann, immer kleiner wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern in ihrer Entschließung zum Datenschutz bei elektronischen Geldbörsen und anderen kartengestützten Zahlungssystemen die Kartenherausgeber und die Kreditwirtschaft auf, möglichst datenschutzfreundliche Guthabenkarten einzusetzen. Bei der Verrechnung der Geldwerte sollte weder eine individuelle Kartennummer noch ein anderer Bezug zum Karteninhaber benutzt werden. Der Gesetzgeber sollte sicherstellen, daß auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher anonym zu bleiben.

4.4 Sichere Übermittlung durch Verschlüsselung, elektronische Unterschrift

Angaben über persönliche Verhältnisse, die privaten oder öffentlichen Institutionen gegenüber gegeben werden, bleiben in den seltensten Fällen nur bei diesen allein, weil die Stellen ihrerseits auf den Kontakt mit anderen angewiesen sind. Datenübertragungen nehmen im täglichen Leben permanent zu: Ärzte geben ihre Leistungsdaten an kassenärztliche Vereinigungen und Verrechnungsstellen, Steuerberater die Steuererklärungen an zentrale Rechenzentren oder an das Finanzamt, Zulassungsämter ihre Daten in das Kfz-Steuerverfahren. Solche Daten sind zwar beim jeweiligen Anwender bzw. deren Mitarbeitern durch Arztgeheimnis, Bankgeheimnis, Steuergeheimnis und sonstige Berufsgeheimnisse geschützt. Während der Übertragung oder anderer Formen des Transports ist der Schutz personenbezogener Daten dagegen nicht immer gewährleistet.

Will man eine Nachricht seinem Partner so zukommen lassen, daß möglichst kein anderer sie lesen oder fälschen kann, kennzeichnet man sie konventionell mit einer charakteristischen Unterschrift, verschließt sie in Umschlägen und transportiert sie durch zuverlässige Kuriere. Elektronisch gespeicherte personenbezogene Daten können sowohl auf leitungsgebundenen oder drahtlosen Übertragungswegen als auch auf maschinell

lesbaren Datenträgern weitergegeben werden, deren Eigenschaften meist weder vom Absender noch vom Empfänger beeinflußbar sind. Aber auch hierbei müssen Vertraulichkeit, Integrität (Unversehrtheit) und Zurechenbarkeit (Authentizität) der Daten sichergestellt sein.

Auf diese Problematik haben die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 9. 5. 1996 (Anlage 3) hingewiesen und hierfür zugleich eine Möglichkeit aufgezeigt, sie zu lösen: sie fördern, beim Transport elektronisch gespeicherter personenbezogener Daten unter Berücksichtigung ihrer Schutzwürdigkeit geeignete, sichere kryptographische Verfahren anzuwenden.

Was die Zurechenbarkeit der Daten betrifft, ist auch aus anderen rechtlichen Gesichtspunkten ein wichtiges Anliegen, hierfür klare gesetzliche Bedingungen zu setzen. Die Bundesregierung legte Ende 1996 den Entwurf zu einem Informations- und Kommunikationsdienstegesetz vor, innerhalb dessen auch Fragen der elektronischen Unterschrift (aber nicht der Verschlüsselung) behandelt werden (Gesetz zur digitalen Signatur). Es wird erwartet, daß auf der Basis dieses Entwurfs schon im Laufe des Jahres 1997 ein Gesetz verabschiedet werden kann.

Zur eigentlichen Verschlüsselung gibt es - nicht nur für den Bereich der Bundesrepublik - einen Grundsatzstreit (sogenannte Kryptokontroverse). Gegen die Forderung nach Sicherungsmöglichkeiten, die nicht allein wegen des Persönlichkeitsschutzes, sondern auch aus wirtschaftlichen Gründen (Sicherheit beim „electronic commerce") erhoben wird, werden nämlich vor allem Sicherheitsbedenken geltend gemacht: so könnten mit solchen Mitteln zugleich etwa kriminelle Aktivitäten versteckt werden. Gegenüber herkömmlichen Kommunikationsmedien, bei denen ja aus übergeordneten Sicherheitsinteressen und unter gesetzlich bestimmten Voraussetzungen eine Kontrolle stattfinden könne, dürfe kein Sicherheitsloch entstehen; deshalb sei Verschlüsselung generell zu verbieten oder jedenfalls auf bestimmte Verfahren (bei denen z. B. die Schlüssel für die Behörden rekonstruierbar sind) zu begrenzen. Das Verschlüsselungsverfahren müsse deswegen gesetzlich reglementiert werden; frei zugängliche und beispielsweise im Internet derzeit verbreitete Programme dürften so nicht (weiter) genutzt werden.

Die Datenschutzbeauftragten halten ein generelles Verbot jeglicher Verschlüsselung nicht für verfassungsmäßig, weil es das Interesse an möglichst sicherer und unbeobachteter Kommunikation übermäßig einschränkt.

Bei Abwägung zwischen den guten Gründen, die es für die freie Zulassung möglichst leistungsfähiger Verschlüsselungsverfahren gibt, und den Interessen der Sicherheits- und Strafverfolgungsbehörden muß der Gesetzgeber selbstverständlich beachten, daß Schranken grundrechtlicher Freiheiten nur dann zulässig sind, wenn die vorgesehenen Maßnahmen geeignet sind, das Regelungsziel zu erreichen. In verschiedenen Publikationen wird aber darauf hingewiesen, daß eine Kontrolle eventueller Restriktionen nicht möglich ist: durch Überverschlüsselung mit einem zulässigen Verfahren lassen sich z. B. eigene Verschlüsselungen tarnen, durch Verstecken (Steganographie) von Nutzinformationen in unverdächtiger Verpackungsinformation (z. B: Veränderung von festgelegten Bits in Bilddateien, Ausnutzung des Rauschens bei Sprachübertragung) kann eine Kontrolle ins Leere laufen.

Auch Zweifel an der Eignung veranlaßten dazu, daß sich die Datenschutzbeauftragten dagegen ausgesprochen haben, eine Verschlüsselung per Gesetz zu verbieten. Bei Redaktionsschluß des Berichtes war innerhalb der Bundesregierung noch keine Entscheidung getroffen.

4.5 Datenschutz und Telefax

Nach dem Telefon ist inzwischen das Telefax zum wichtigsten Kommunikationsverfahren geworden; auch im Verkehr der öffentlichen Stellen findet es zunehmend Verwendung. Bereits mit dem 14. Tätigkeitsbericht (TZ 11.5) hatte ich auf die Risiken dieser Übertragungsart hingewiesen und Vorkehrungen in einer Dienstanweisung empfohlen, wie sie beispielhaft gemeinsam mit einem Ministerium erarbeitet worden war.

Die Weiterentwicklung auch dieser Technik - etwa durch Fernwartungsmöglichkeiten, die unbemerkte Zugriffe der Hersteller zulassen, oder durch Integration von Telefaxlösungen in Bürokommunikationssysteme - gab Anlaß, in einer zusammen mit den übrigen Datenschutzbeauftragten

überarbeiteten Empfehlung erneut entsprechende Hinweise zu geben (Anlage 4).

4.6 Protokollierung

In § 11 SDSG ist unter anderem geregelt, daß

- im Rahmen der Übermittlungskontrolle nachträglich überprüf- und feststellbar sein muß, welche Daten zu welcher Zeit an wen durch Einrichtungen zur Datenübertragung übermittelt worden sind

- im Rahmen der Eingabekontrolle nachträglich überprüf- und feststellbar sein muß, welche Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind.

Diesen Anforderungen und weiteren Anforderungen der Organisationskontrolle kann in der Regel nur entsprochen werden, wenn eine ausreichende Protokollierung durchgeführt wird. Weil auch Protokolldaten zusätzlich erzeugte, sensible personenbezogene Daten enthalten, müssen sie gesondert geschützt werden. Ihr Schutz wird durch eine enge Zweckbindung gewährleistet; sie sind nach § 19 SDSG zu sperren, d. h. besonders zu sichern, so daß nur befugte Kontrollinstanzen wie z. B. die IT-Revision oder die Datenschutzkontrolle darauf zugreifen können. Um den Umfang der Protokolldaten beschränken und eine effektive Kontrolle durchführen zu können, sind diese Kontrollen zeitnah und mit geeigneten Auswerteprogrammen durchzuführen.

Der Arbeitskreis „Technik" der Datenschutzbeauftragten hat zu dieser Problematik in einer Orientierungshilfe im einzelnen die rechtlichen, organisatorischen und technischen Aspekte dargestellt und Hilfen formuliert. Ich habe sie den saarländischen Fachverwaltungen zur Verfügung gestellt; sie ist ebenfalls in meinem Internet-Angebot (TZ 22.2) enthalten.

4.7 Internet-Nutzung

Seit einiger Zeit wächst in öffentlichen Stellen des Saarlandes der Wunsch nach einem Zugang zu globalen Datennetzen. In der Öffentlichkeit wird die Öffnung der Verwaltung auch für Möglichkeiten der elektronischen Kommunikation gefordert oder vorausgesetzt. Insbesondere das Internet ist durch seine weltweite Nutzung und die Kommunikationsmöglichkeiten unterschiedlichster Benutzer und Bereiche, die auch unter den Begriffen "Datenautobahn" und "globales Dorf" propagiert werden, sehr attraktiv. Durch Anbindung von Einzelplatz-PC oder Verwaltungsnetzen an das Internet können dort verfügbare Informationen gewonnen, eigene Informationen für andere zum Abruf bereitgestellt oder das Netz zum Transport von Verwaltungsdaten genutzt werden.

Mit dem Zugang zum Internet sind jedoch Risiken verbunden, die größtenteils daraus resultieren, daß dieses Datennetz nicht unter Sicherheitsaspekten entwickelt wurde und historisch gewachsen ist. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Übertragungswegen und Rechnersystemen. So gibt es beispielsweise keine sicheren Mechanismen zur Identifikation und Authentisierung im Netz. Ohne besondere Schutzmaßnahmen kann sich ein Angreifer oft mit wenig Aufwand unter Ausnutzung der Sicherheitslükken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen oder sogar manipulieren oder zerstören. Abgerufene Programme und Dokumente können bekannte und unbekannte Viren enthalten. Programme, Dokumente und Bilder können verfälscht sein. Dies ist besonders gravierend, weil aufgrund der riesigen Zahl von Internet-Teilnehmern auch die Zahl potentieller Angreifer, die diese Sicherheitslücken ausnützen und somit die am Internet angeschlossenen Verwaltungsrechner und -netze bedrohen können, sehr groß ist.

Daß hierbei Gefahren für die informationelle Selbstbestimmung entstehen, verdeutlicht auch ein Blick auf die private Nutzung: Für die im Internet angebotenen Dienstleistungen und die dabei entstehenden Kosten gibt es derzeit noch keine sicheren Verrechnungsmöglichkeiten. In den USA wird auch im Internet in der Regel durch Angabe der Kreditkartennummer bezahlt. Doch gewarnt durch entsprechende Hackeraktivitäten, bei denen Kreditkartennummern im Netz abgefangen und mißbräuchlich

verwendet wurden, geht die Bereitschaft, die Kartennummer offen weiterzugeben, immer mehr zurück. Ihre Dienstleistungen können die Anbieter deshalb oft nur über - genau auf Zielgruppen ausgerichtete - Werbung finanzieren, die ungefragt in die Angebote eingestreut wird. Der Nutzer wird dabei vielleicht verwundert feststellen, daß Suchmaschinen und Dienstleistungsrechner sein Kundenverhalten registrieren, um gerade seinem Interesse entsprechende Werbung zuzuleiten; er wird es aber nicht hinnehmen wollen, daß Daten über sein Kundenverhalten, seine Kundenzufriedenheit oder die in Anspruch genommenen Dienstleistungen und natürlich seine E-Mail-Adresse an interessierte andere Unternehmen verkauft werden. Da über 80% des Internet-Verkehrs von amerikanischen Rechnern abgewickelt werden, gelten in aller Regel die dortigen Gesetze; falls sie zu streng sein sollten, wird einfach der Sitz der Firma in die Karibik verlegt. Kein Bundesdatenschutzgesetz kann den deutschen Nutzer schützen und keine Robinsonliste kann verhindern, daß ungefragte Werbung im E-Mail-Postfach landet.

Dem kann man derzeit nur begrenzt durch bewußt anonymen Zugang entgehen; hierzu wird verschiedentlich dazu aufgefordert, sich im E-Mail-Verkehr sogenannter Remailer zu bedienen. Dies sind Internet-Dienstleister, die die Identität der Kunden verwalten und die Mail über eine Pseudokennung weitergeben, die nur sie selbst wieder dem Kunden zuordnen können. Der - kostenlose - Dienst eines finnischen Rechnerbetreibers wurde, weil er wegen angeblichen Mißbrauchs scharf kontrolliert wurde, stillgelegt; es wird schwierig, einen anderen Dienstleister zu finden, der diese Funktion kostenlos ausübt und zugleich hierfür für vertrauenswürdig gehalten wird. (Der Meldung einer amerikanischen Zeitschrift zufolge sollen Deckfirmen des CIA mindestens zwölf dieser Remailer betreiben. Nutzt ein Internet-Surfer dieses Angebot in der Annahme, er sei gegenüber Zielrechnern anonym, liefert er so nebenbei dem Geheimdienst seine Identität mitsamt seiner Post frei Haus.) Die Betreiber der Onlinedienste sind aufgefordert, solche Dienstleistungen netzintern anzubieten und zu sichern.

Mehr noch als beim privaten Surfer droht die Gefahr bei öffentlichen Stellen, wenn über das Netz Daten der Bürger verfügbar werden. Um den für den Betrieb von Netzen der öffentlichen Verwaltung Verantwortlichen deutlich zu machen, mit welchen Risiken bei einem Anschluß an das Internet zu rechnen ist und wie diese Risiken begrenzt werden können, ha-

be ich eine Orientierungshilfe herausgegeben, die in Zusammenarbeit mit den übrigen Datenschutzbeauftragten entstanden ist. Die Orientierungshilfe wurde an die Obersten Landesbehörden und den kommunalen Bereich verschickt. Inzwischen sind meine Empfehlungen auch in verschiedenen Publikationen und bei konkreten Einsatzfällen (siehe TZ 5.9) aufgegriffen worden. Die Nutzer bleiben aufgefordert, die Entwicklung permanent zu verfolgen, da immer neue Lösungen angeboten werden, aber auch wieder neue Risiken auftreten können, an die vorher niemand gedàcht hat.

4.8 Optische Datenspeicherung

Das Ministerium für Finanzen beabsichtigte im Rahmen eines Projekts, die Kfz-Steuerdaten auf optischen Datenspeichern zu verwalten und damit deren enorme Speichermöglichkeiten auf relativ kleinen Trägern zu nutzen. Die in der Landesverwaltung zum ersten Mal verwandte neue Speicherungstechnik warf aus datenschutzrechtlicher Sicht neue Probleme auf. So erlauben die dabei genutzten WORM-Platten, d. h. Datenträger, die nur einmal beschrieben, aber mehrfach gelesen werden können, keine gezielte Löschung einzelner Daten, sondern lediglich das Löschen der zu den Daten gehörigen Verweisdaten in den Verwaltungsdatenbanken, während die Nutzdaten auf den optischen Datenträgern weiter lesbar bleiben. Aus Sicht des Saarländischen Datenschutzgesetzes ist eine solche Form nicht ausreichend, weil bei einem Löschungsanspruch die Daten vollständig vernichtet werden müssen.

In Zusammenarbeit mit dem Arbeitskreis „Technik" der Datenschutzbeauftragten wurde daraufhin eine Orientierungshilfe erarbeitet, in der die technischen und datenschutzrechtlichen Aspekte eines Einsatzes optischer Datenspeicher dargestellt und Empfehlungen zu ihrem Einsatz ausgesprochen werden. Im konkreten Fall hat die Fachverwaltung der Problematik inzwischen dadurch Rechnung getragen, daß bei gegebenem Löschungsanspruch eines Bürgers auf einem neuen Datenträger eine komplette Kopie des Datenträgers ohne die zu löschenden Daten erzeugt und der alte Datenträger datenschutzgerecht vernichtet wird.

4.9 IT-Sicherheitsrichtlinie, Risikoanalysen, Sicherheitskonzepte und Schutzstufenkonzept

Hoher Aufwand bei Erfüllung der gesetzlichen Anforderungen

Nach dem saarländischen Datenschutzgesetz sind die Obersten Landesbehörden, die Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen für die Sicherstellung des Datenschutzes verantwortlich. Wenn personenbezogene Daten automatisiert verarbeitet werden, sind geeignete Maßnahmen zu treffen, um eine Zugangs-, Datenträger-, Speicher-, Benutzer-, Zugriffs-, Übermittlungs-, Eingabe-, Auftrags-, Transport- und Organisationskontrolle zu gewährleisten. Welche Maßnahmen konkret zu treffen sind, schreibt das Gesetz nicht vor.

Die öffentlichen Stellen sind daran interessiert, mit möglichst geringem Aufwand für den jeweiligen Schutzbedarf geeignete, sichere und datenschutzgerechte Maßnahmen auswählen und damit die gesetzlichen Anforderungen erfüllen zu können; eine Standardisierung tut not. Andererseits ist auch für den Landesbeauftragten für Datenschutz, der vor Einsatz automatisierter Verfahren zu hören ist, eine individuelle, datenschutzrechtliche Prüfung eines jeden Verfahrens mit den derzeit verfügbaren Kapazitäten nicht zu leisten.

IT-Grundschutzhandbuch des BSI als Mindeststandard

In vielen Handbüchern und Gesetzeskommentaren sind entsprechende Maßnahmenkataloge enthalten, die mehr oder weniger umfangreich und spezifiziert sind. Einen solchen Katalog enthält auch der Leitfaden für die Erstellung von Dienstanweisungen für den PC-Einsatz, GMBl Saarland 1992, S. 462.

Das Bundesamt für die Sicherheit in der Informationstechnik hat neuerdings mit dem IT-Grundschutzhandbuch (IT-GSHB) einen zwar umfangreichen, aber für den Anwender leicht handhabbaren Katalog von technischen und organisatorischen Maßnahmen herausgegeben. Auch wenn diese sich an der Datensicherheit als Ziel ausrichten, sind sie weitestge-

hend auch geeignete und notwendige Vorkehrungen für den Datenschutz. Damit steht eine gute Grundlage zur Verfügung, um eine fundierte Risikoanalyse und ein angemessenes Sicherheitskonzept für den mittleren Schutzbedarf zu entwickeln. Es bietet sich aus meiner Sicht an, dieses Handbuch als einheitlichen Standard für die Verwaltungen zu nutzen.

Da im Grunde auf allen IT-Systemen in der Landesverwaltung in irgendeiner Form personenbezogene Daten verarbeitet werden (dies gilt auch auf PC, die nur für Textverarbeitung eingesetzt werden), ist es sinnvoll, für alle diese IT-Systeme mindestens Maßnahmen für den mittleren Schutzbedarf zu treffen. Nach Einschätzung des BSI ist damit der Schutzbedarf von ca. 80 % aller Anwendungen abgedeckt, so daß nur noch für die restlichen 20 % mit höherem Schutzbedarf eine (aufwendige) individuelle Risikoanalyse und ein (aufwendiges) individuelles Sicherheitskonzept zu erstellen sind. Jede neu hinzukommende Anwendung auf einem so gesicherten IT-System wird dann auch in einem ausreichend hohen Sicherheitslevel betrieben, so daß in der Mehrzahl der Fälle keine zusätzlichen Maßnahmen zu treffen sind, bzw. gegebenenfalls nur wenige zusätzliche Maßnahmen entsprechend dem Schutzbedarf erforderlich sind.

IT-Sicherheitsrichtlinie

Um die Handhabung des IT-GSHB in der Landesverwaltung zu erleichtern, wurde vom interministeriellen Ausschuß für Informationstechnologie und Kommunikation eine IT-Sicherheitsrichtlinie erarbeitet. Ziel dieser Richtlinie ist es, mit Hilfe eines umfassenden IT-Sicherheitsmanagements die Datensicherheit zur Sicherstellung einer ordnungsgemäßen Informationsverarbeitung (vorwiegend im Interesse der datenverarbeitenden Stellen) und den Datenschutz bei der Verarbeitung personenbezogener Daten (vorwiegend im Interesse der Betroffenen) zu gewährleisten. Dabei soll auch die Erstellung von Risikoanalysen und Sicherheitskonzepten durch Anwendung des IT-GSHB als Maßnahmenempfehlung für den mittleren Schutzbedarf und als Mindeststandard für Verfahren der Informationstechnik und Kommunikation unterstützt werden. Diese „IT-Sicherheitsrichtlinie“ soll im Gemeinsamen Ministerialblatt des Saarlandes 1997 veröffentlicht werden.

Schutzbedarfsfeststellung und Schutzstufenkonzept

Das IT-GSHB des BSI richtet den Schutzbedarf eines IT-Systems am Schutzbedarf seiner kritischsten Anwendung aus. Der Schutzbedarf einer Anwendung orientiert sich an Fragen zu Schadenskategorien und daraus abgeleiteten Schäden und Folgen; letztendlich führt dies zu groben Einschätzungen wie: Schutzbedarf ist „niedrig" bis „mittel", wenn Schadensauswirkungen „begrenzt und überschaubar" sind, oder Schutzbedarf ist „hoch" bzw. „sehr hoch", wenn Schadensauswirkungen „beträchtlich sein oder sogar ein existentiell bedrohliches, katastrophales Ausmaß erreichen" können.

Wegen dieses relativ vagen Maßstabes ist es schwierig, den Schutzbedarf einer Anwendung nach den Kategorien des IT-GSHB unstrittig zu beurteilen, insbesondere, wenn das informationelle Selbstbestimmungsrecht bei der Verarbeitung personenbezogener Daten gewährleistet sein soll. Zur Lösung dieses Problems erscheint es vielmehr sinnvoll, die Sensibilität der in den jeweiligen Anwendungen zu verarbeitenden, personenbezogenen Daten möglichst nach einem Schutzstufenkonzept zu bewerten und dann diesem Schema zugeordnete technische und organisatorische Maßnahmen zu fordern. Solche Stufenkonzepte werden auch in anderen Vorschriften genutzt wie z. B. Verschlußsachenanweisung, IT-SEC = Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik.

Das von mir vertretene Schutzstufenkonzept wurde aus den in vielen Ländern und auch beim Bundesbeauftragten für Datenschutz genutzten Schemata abgleitet und dabei an die Zweistufigkeit des IT-GSHB (bis mittlerer Schutzbedarf, mehr als mittlerer Schutzbedarf) angepaßt. Für die große Mehrzahl der Anwendungen wird damit unter Datenschutzaspekten der Gefährdungs- und Maßnahmekatalog des Grundschutzhandbuchs anwendbar gemacht.

Das Schutzstufenkonzept darf allerdings nicht starr angewandt werden. Es dient lediglich als Einschätzung für den Mindestschutzbedarf; ergänzend dazu ist noch der jeweilige Verwendungszusammenhang zu beachten, der eventuell einen höheren Schutzbedarf ergeben kann und dann zusätzliche Maßnahmen erforderlich macht. Ergibt die Grobanalyse einen über den mittleren Schutzbedarf hinausgehenden, hohen oder sehr hohen

Schutzbedarf, sind eine weitergehende, individuelle Risikoanalyse und die Erstellung eines individuellen Sicherheitskonzeptes durchzuführen. Dabei kann auf die Verfahrensweise nach dem IT-Sicherheitshandbuch des BSI zurückgegriffen werden. Grundsätzlich sind aber mindestens alle Maßnahmen nach dem IT-GSHB zu treffen, wobei dem Schutzbedarf entsprechend weitergehende, zusätzliche Maßnahmen erforderlich sind. Dazu könnte z. B. gehören, daß alle optionalen Maßnahmen des IT-GSHB verpflichtend eingeführt werden, daß Daten zu verschlüsseln sind, daß Systemverwalterpaßworte nach dem 4-Augen-Prinzip aufzuspalten sind.

Erfahrungen mit der Anwendung des IT-GSHB bei bisherigen Projekten der Landesverwaltung

Die beschriebene Vorgehensweise wurde inzwischen bei mehreren Obersten Landesbehörden und nachgeordneten Dienststellen angewandt. Besonders zu erwähnen sind dabei die Unikliniken Homburg (TZ 5.10), das Ministerium des Innern (Verfahren Einbürgerung (TZ 5.5) und Rettungsleitstelle/noch nicht abgeschlossen), die Oberfinanzdirektion/ZBS (TZ 5.4) und die ZDV-Saar (Verfahren zur Kostenrechnung/TZ 6.3). Allgemein kann wohl festgestellt werden, daß die Anwender froh sind, eine direkt anwendbare Hilfestellung zur Gewährleistung von Datenschutz und Datensicherheit zu erhalten, die die bisherige Projektarbeit diesbezüglich formal und inhaltlich sicherer gestalten hilft. Zusätzlich erleichtert die Richtlinie die generelle Einrichtung eines ständigen IT-Sicherheitsmanagements bei den Dienststellen. Beim ersten Projekt ist zwar der Aufwand, vor allem für die Umsetzung der Richtlinie, höher als bisher zu veranschlagen. Bei jedem weiteren Projekt stellt sich der Aufwand allerdings auch wesentlich geringer dar, da die Vorgehensweise standardisiert und damit leichter umsetzbar ist; Struktur und eventuell ganze Teile der Schutzbedarfsfeststellung, der Risikoanalyse und des Sicherheitskonzepts können direkt übernommen werden, da neue Verfahren auf schon betrachteten IT-Systemen zum Einsatz kommen.

Auch der Landesbeauftragte für Datenschutz und weitere Kontrollinstanzen wie Rechnungshof, interne Revision und interne Datenschutzkontrolle profitieren von diesem Konzept, da durch standardisierte, allgemeingültige Maßnahmen ihre Prüftätigkeit wesentlich erleichtert wird.

4.10 Datenschutz im IT-Grundschutzhandbuch

Wie im vorigen Abschnitt dargestellt, ist der umfangreiche, aber leicht handhabbare Maßnahmenkatalog des IT-GSHB in der bisherigen Form vorrangig darauf ausgelegt, Datensicherheit zu gewährleisten. Zur Sicherstellung des Datenschutzes muß die Darstellung der einschlägigen Gefährdungen und der zu ihrer Begegnung zu treffenden Maßnahmen noch ergänzt werden. Dabei bietet sich an, für die Beurteilung des Schutzbedarfs personenbezogener Daten in das Handbuch auch ein Schutzstufenkonzept zu übernehmen.

In Zusammenarbeit mit den Datenschutzbeauftragten des Bundes und der Länder arbeitet das BSI derzeit daran, das IT-GSHB in seiner neuen Version für 1997 so zu ergänzen, daß auch der Datenschutz ausreichend berücksichtigt ist. Danach dürfte auch aus Sicht des Datenschutzes das Handbuch als einheitlicher Standard für alle Bundes- und Landesverwaltungen zu empfehlen sein.

4.11 Muster-Dienstanweisungen

Mit dem Leitfaden für die Erstellung von Dienstanweisungen für den PC-Einsatz, GMBl Saarland 1992, S. 462, wurde die Grundlage geschaffen, um in allen Dienststellen der Landesverwaltung geeignete Dienstanweisungen in Kraft setzen und damit eine wesentliche datenschutzrechtliche Forderung nach Organisationskontrolle erfüllen zu können. Der Umfang dieses Leitfadens und seine Struktur haben aber offensichtlich viele Anwender abgeschreckt, die die einfache Handhabung durch die im Text enthaltenen Mustertexte übersehen haben.

Um die Anwendung des Leitfadens und die Erstellung von IT-Dienstanweisungen zu erleichtern, habe ich in enger Zusammenarbeit mit ausgewählten Dienststellen für unterschiedliche Bereiche darauf hingewirkt, Dienstanweisungen so auszugestalten, daß sie als Muster-Dienstanweisungen für andere Dienststellen in diesem Bereich herangezogen werden können. Im Bereich der Obersten Landesbehörden war dies das Ministerium für Wirtschaft und Finanzen, im Schulbereich das Kaufmännische Berufsbildungszentrum Merzig, für die Landkreise der Saarpfalz-Kreis, Homburg, und für die Städte und Gemeinden die Ge-

meinde Tholey. Für die Kooperationsbereitschaft der genannten Dienststellen möchte ich mich an dieser Stelle noch einmal bei den Ansprechpartnern und den Verantwortlichen ausdrücklich bedanken.

Die Muster-Dienstanweisungen habe ich an die in Frage kommenden Dienststellen auf Diskette mit der Bitte versandt, sie für die Erstellung eigener Dienstanweisungen weiterzubearbeiten; sie sind auch in meinem Internet-Angebot enthalten (TZ 22.2).

4.12 Checklisten für Novell-Netze und TK-Anlagen

Im Rahmen des gegenseitigen Informationsaustausches erhielt ich vom Landesbeauftragten in Niedersachsen eine ausgefeilte und sehr informative Checkliste für die Prüfung datenschutzrechtlicher Aspekte beim Einsatz des Netzwerkbetriebssystems Novell. Nach Anpassung des darin enthaltenen Schutzstufenkonzepts an die saarländische Fassung ist die überarbeitete Checkliste für den Systemverwalter und das Projektmanagement eine hervorragende Grundlage, um Schwachstellen erkennen und ausreichende Sicherheit beim Netzbetrieb herstellen zu können. Bei verschiedenen Dienststellen und Projekten habe ich die Checkliste zur Hilfe bei der Einrichtung und zur Eigenkontrolle überreicht. Es liegt mir nicht daran, das darin enthaltene Expertenwissen dazu zu nutzen, den Anwender bei Kontrollen bloßzustellen, sondern ihm im Vorfeld Hilfen zu bieten, so daß eine eventuelle Kontrolle ohne Beanstandung bleiben kann und vor allem sofort der Datenschutz sichergestellt ist.

Unter Berücksichtigung der Empfehlungen des IT-GSHB habe ich weiter eine Checkliste für den Einsatz von TK-Anlagen erstellt, die auch die Herstellung und Überprüfung der bei den Unteranlagen zu treffenden Maßnahmen erlaubt. Mit Hilfe dieser Checkliste habe ich die Realisierung des TK-Anlagenverbundes der Landesverwaltung begleitet und damit dazu beigetragen, auch bei diesem komplexen Projekt den datenschutzrechtlichen Anforderungen zu genügen (siehe auch TZ 5.6).

4.13 Office-Software; EDV bei kleinen Dienststellen

Auf weitere Datenschutzgefahren, denen mit technisch-organisatorischen Maßnahmen begegnet werden muß, sei in allgemeiner Form hingewiesen:

Viele öffentliche Stellen nutzen die vielfältigen und bequemen Möglichkeiten kombinierter Standard-Programme, die auch im geschäftlichen und privaten Bereich weit verbreitet sind. In moderner Office-Software werden unterschiedliche Dienstprogramme wie Textverarbeitung, Tabellenkalkulation, Datenbank usw. nicht nur zu Paketen zusammengefaßt, sondern zusätzlich noch die Möglichkeit geschaffen, mit Hilfe sogenannter OLE-Techniken Ergebnisse eines Programms in ein anderes Programm mit Mausklick zu übernehmen bzw. einschließlich des jeweiligen Programmstarts zu integrieren. Office-Software ist inzwischen so leistungsfähig, daß auch programmierunkundige Anwender schon nach kurzer Einarbeitungszeit in der Lage sind, aufwendige Tabellenkalkulationsanwendungen und Datenbankauswertungen zu entwickeln.

So hilfreich derartige Pakete für die Anwender sind, die sie anstelle aufwendiger Spezialprogramme oder zu deren Ergänzung einsetzen, so problematisch kann die breite Verwendung für die Gewährleistung des Datenschutzes sein. Denn gerade wegen der allgemein leichten Handhabbarkeit sind Entwicklung von Anwendungen und deren mögliche Auswertungen nicht mehr mit der klassischen Vorgehensweise der Auftragsvergabe, Programmierung, Test und Freigabe zu kontrollieren. Auch integrierte Schutzmaßnahmen bleiben oft wirkungslos; so kann eine Sperrung bestimmter Funktionen in einem Programm (auch mit Paßworten) dadurch umgangen werden kann, daß über die Zwischenablage Daten-Teilbereiche in einen anderen Officeteil transferiert werden und dann dort frei zur Verfügung stehen.

Die verantwortlichen Stellen sind aufgefordert, durch Ausnutzung aller Beschränkungsmöglichkeiten in der Office-Software und durch Verwendung von sogenannten Runtime-Modulen, die gegenüber dem Vollprodukt nur eine eingeschränkte Leistungsfähigkeit (z. B. keine freie Programmierbarkeit) aufweisen, einem möglichen Wildwuchs entgegenzuwirken. Zusätzlich muß einer unkontrollierten Entwicklung durch organisatorische Maßnahmen, insbesondere durch eine IT-Dienstanweisung, entgegen-

gewirkt werden, in der das Verfahren zur Beauftragung, Erstellung und Freigabe für jeden verbindlich geregelt wird.

Dies ist auch nötig, um Datenschutzgefahren zu bannen, wie sie gerade in kleinen Dienststellen immer wieder festzustellen sind:

Immer mehr Stellen nutzen den PC-Einsatz, um ihre Arbeit zu verbessern. Dabei sind oft begeisterte Mitarbeiter Initiator und Motor dieser Entwicklung. Sie beschaffen Software oder programmieren sogar selbst und setzten die Software dann vielfach auch an ihrem Arbeitsplatz ein. Oft wird dabei nicht kritisch genug geprüft, ob der Umfang der Daten erforderlich und die Verarbeitung zulässig ist. Zusätzlich fehlt es vielfach an ausreichenden Maßnahmen, so daß die im Datenschutzgesetz vorgegebenen Kontrollziele nicht erreicht werden. Insbesondere mangelt es in aller Regel an der üblichen Funktionstrennung, die zum Ziel hat, durch Wahrnehmung der Funktionen Programmierung, Systembetreuung, Anwendung, IT-Revision und interne Datenschutzkontrolle, Wartung und Reparatur durch unterschiedliche Personen dem möglichen Mißbrauch von Daten zu begegnen. Es geht nicht an, daß Verfahren zur Verarbeitung personenbezogener Daten aus Geld- oder Personalmangel unter Gefährdung des Datenschutzes betrieben werden. Die Funktionstrennung und eine Realisierung aus datenschutzrechtlicher Sicht ausreichender technischer und organisatorischer Maßnahmen muß weiterhin sichergestellt werden.

4.14 Datenschutz im kommunalen Bereich

Im Rahmen datenschutzrechtlicher Prüfungen bei einzelnen Gemeinden wurden z. T. erhebliche Mängel aufgedeckt. Vielfach werden schon elementare Forderungen des technischen und organisatorischen Datenschutzes und verfahrensrechtliche Pflichten nicht genügend beachtet: Vorhandene Sicherungseinrichtungen (z. B. Paßworte, Schlüssel) werden nicht genutzt; geltende Regelungen (z. B. Abschließen von Zimmertüren bei leerem Zimmer, Mindestlängen von Paßworten) werden nicht eingehalten. Eine geeignete IT-Revision oder eine interne Datenschutzkontrolle zur Durchsetzung notwendiger oder Überprüfung getroffener Maßnahmen ist nicht vorhanden. Eine Dienstanweisung für den Einsatz der Informationstechnik, die als eine geeignete organisatorische Maßnahme für alle

verbindlich die geltenden Regelungen beschreibt, fehlt oft gänzlich. Die gesetzlich vorgeschriebene Beteiligung des Landesbeauftragten für Datenschutz vor der Einführung neuer oder wesentlich geänderter Verfahren ist bei vielen Gemeinden ebenso unterblieben wie die Meldung der Verfahren zum Dateienregister bzw. deren Aktualisierung. Insgesamt erscheint notwendig, das Datenschutzbewußtsein bei vielen Mitarbeitern bis hin zum Bürgermeister noch wesentlich zu verbessern.

Da ohnehin viele Kreise, Städte und Gemeinden gegenwärtig damit befaßt sind, ihre nun veraltete Datenverarbeitung durch moderne Systeme und Programme zu ersetzen, erschien es sinnvoll, der Problematik in genereller Weise präventiv zu begegnen und die Kommunen nicht erst bei einer Kontrolle auf die Notwendigkeit des Datenschutzes hinweisen zu müssen. Ich habe deshalb in mehreren Schreiben und bei einer kommunalen Messe in Lebach auf diese Aspekte hingewiesen und zusätzlich den Kreisen, Städten und Gemeinden Materialien zugeleitet, die diese als Arbeitshilfen für ihre Aufgaben nutzen können. Die zugesandte Diskette enthielt unter anderem ein elektronisches Formular zur Meldung zum Dateienregister und eine Muster-IT-Dienstanweisung (siehe TZ 4.11).

Bei völlig neuartigen Verfahren habe ich mich zudem bereit erklärt, datenschutzrechtliche Fragen genereller Art bereits mit den Lieferanten vorzuklären, so daß die Gemeinde vom Anbieter geeignete Muster erhält, die nur noch mit gemeindespezifischen Ergänzungen versehen werden müssen. Einige Firmen und Gemeinden haben dieses Angebot aufgegriffen und sich diesbezüglich an mich gewandt.

5 Technisch - organisatorische Fragen des Datenschutzes

Auf einige Fälle meiner Beteiligung an neuen Verfahren und Prüfungen mit Betonung gerade des technisch-organisatorischen Schwerpunkts sei besonders hingewiesen.

Insbesondere bei Einführung neuer Verfahren läßt sich - teilweise auch innerhalb verschiedener Abteilungen in einer Dienststelle - generell ein sehr unterschiedliches Datenschutzbewußtsein feststellen. Einige Anwender bemühen sich, bei neuen Projekten die datenschutzrechtlichen Anforderungen unter Berücksichtigung der ADV-Projektrichtlinien zu erfül-

len; dabei werden auch umfangreiche und ausgefeilte Risikoanalysen und Sicherheitskonzepte erstellt. Andererseits gibt es weiterhin Stellen, die glauben, mit der Einladung zum Abschlußtest oder der Übersendung eines Benutzerhandbuchs sei der gesetzlichen Pflicht zur Beteiligung des Landesbeauftragten für Datenschutz (§ 8 Abs. 2 SDSG) Genüge getan. Nicht hinzunehmen ist, wenn im kommunalen Bereich mit Blick auf die kommunale Selbstverantwortung eine Beteiligung ganz unterbleibt und dann der Datenschutz „auf der Strecke bleibt".

Im Rahmen meiner personellen und zeitlichen Kapazitäten bin ich gerne bereit, die Anwender bei der Umsetzung zu unterstützen. Notwendig ist aber eine frühzeitige Beteiligung, um noch so rechtzeitig Vorschläge machen zu können, daß sie auch noch in die Verfahrensentwicklung einbezogen werden können.

5.1 Verfahren Sijus-StA bei der Staatsanwaltschaft

Bei Prüfung des automatisierten Verfahrens Sijus-Straf-STA bei der Staatsanwaltschaft Saarbrücken zeigten sich datenschutzrechtliche Mängel.

So wurde die gebotene Löschung von Altfällen bisher noch nicht durchgeführt. Im Datenbestand waren noch alle Fälle vom Beginn der Automation im Jahre 1987 an enthalten. Bezüglich der IT-Unterstützung enthält das Verfahren systembedingt Mängel, die aus Sicherheitsgründen abzustellen sind:

- jede Kennung, insbesondere die Kennung des Systemverwalters, ist an jedem Arbeitsplatz mit Anschluß an das UNIX-System nutzbar; es gibt keine Zuordnungsmöglichkeit von Benutzerkennungen zu festen Stationen

- es kann eine beliebige Zahl von Fehlversuchen vorgenommen werden, ohne daß das System Alarm gibt oder den Bildschirm deaktiviert

- ein mindestens 6-stelliges Paßwort kann nicht erzwungen werden

- es gibt keine automatische Dunkelschaltung bei längerem Nichtbetrieb

- die Vergabe der Benutzerrechte durch den Systemverwalter wird nicht protokolliert

- es gibt keine IT-Revision, die eine Auswertung der Protokolldatei vornehmen kann; diese wird zyklisch mit neuen Daten überschrieben.

Soweit Anwender hierzu auf fehlende Funktionalitäten der zugrundeliegenden Betriebssystemsoftware verweisen, kann dies die Mängel nicht rechtfertigen.

Bei der Überprüfung des PC-Anschlusses bei einem Staatsanwalt, der Zugriff auf das Netz hat, wurde eine völlig unzureichende Sicherung festgestellt: Beim Einschalten des Gerätes wurde ohne Sicherungsvorkehrung das Betriebssystem geladen, und dieses startete danach selbst die Textverarbeitung Word. Die vorhandenen Sicherungsmaßnahmen wie Schlüsselschalter am Gehäuse und BIOS-Paßwort beim Systemstart waren nicht genutzt. Jeder beliebige Besucher konnte den PC starten und zumindest die lokal vorhandenen Daten, insbesondere die Word-Dokumente, lesen und verändern. Die Emulationssoftware enthielt einen ungeschützten Menüpunkt „Sitzung protokollieren", der es erlaubt, den gesamten Datenverkehr mitzuprotokollieren, so daß diese Daten nach Abschluß der Bildschirmarbeit mit Standardsoftware ausgewertet werden könnten. Das Diskettenlaufwerk war ebenfalls nicht gesichert, so daß ein Kopieren dieser Daten bzw. der lokalen Datenbestände und eine Weitergabe an Dritte möglich gewesen wäre.

Die Oberste Landesbehörde wurde aufgefordert, mit Hilfe ihrer Benutzerbetreuung und der Systemverwaltung die genannten Mängel abzustellen bzw. beim Softwarelieferanten eine Anpassung der Software zu fordern.

Da in Zukunft eine Ablösung der Bildschirme durch PC mit Terminalemulation vorgesehen ist, sind diese besonders zu sichern. Dazu ist eine Nutzung aller am PC standardmäßig vorhandenen Sicherungsmöglichkeiten (Gehäuseschlüssel, BIOS-Paßwort) geboten. Darüber hinaus müssen zusätzliche Maßnahmen ergriffen werden, wie sicheres Menüsystem mit Paßwortschutz, Verschlüsselung lokaler Datenbestände, Sperren der Diskettenlaufwerke, Entfernen der Protokollierungsmöglichkeiten bei der Emulation und eine IT-Revision und interne Datenschutzkontrolle, um

Mißbräuche aufdecken und die Durchsetzung geltender Regeln überwachen zu können.

Obwohl inzwischen mehr als ein halbes Jahr seit der Prüfung vergangen ist, steht eine Stellungnahme des Ministeriums der Justiz noch aus.

5.2 Verfahren BASIS für die Justizvollzugsanstalt

Da bei diesem Verfahren das gleiche Betriebssystem wie beim unter TZ 5.1 genannten Verfahren genutzt wird, bestehen die dort genannten systembedingten Probleme und Mängel hier ebenfalls. Ansonsten waren ausreichende technische und organisatorische Maßnahmen für den Einsatz getroffen.

Die Fachverwaltung war nicht in der Lage, mir die Verträge zur Wartung und Reparatur vorzulegen, bei denen Auftragsdatenverarbeitung stattfindet. Ich konnte dadurch nicht prüfen, ob diese unter Beachtung des § 5 SDSG abgeschlossen wurden.

5.3 Verfahren PROFISKAL für die Kostenrechnung bei der ZDV-Saar

Im Zuge der Umstrukturierung der ZDV-Saar zu einem Landesbetrieb wurde das Verfahren PROFISKAL zur Unterstützung der Kostenrechnung eingeführt. Dabei wurde zum ersten Mal eine Risikoanalyse und ein Sicherheitskonzept auf der Grundlage des IT-Grundschutzhandbuchs modellhaft durchgeführt (siehe TZ 4.9) und das Verfahren unter Beachtung personalrechtlicher Anforderungen freigegeben. Die erstellten Unterlagen dienten weiteren Projekten anderer Ressorts als Vorlage für die Erstellung eigener Konzepte.

5.4 Personalabrechnungsverfahren DAISY

Beim Verfahren DAISY (dialogisiertes Abrechnungs- und Informationssystem für die Berechnung, Festsetzung und Zahlbarmachung der Bezüge)

handelt es sich um ein Verfahren, das vom Landesamt für Besoldung und Versorgung des Landes Baden-Württemberg entwickelt und dort schon seit längerer Zeit im Einsatz ist; es wurde von der ZDV-Saar an die saarländischen Gegebenheiten angepaßt. Durch die Einführung von DAISY entfällt die Datenerfassung für Besoldung und Versorgung bei der ZDV-Saar und damit auch die Problematik von Übermittlung und Sicherung der Belege.

Das Verfahren wird auf dem Großrechner der ZDV-Saar betrieben. Die Sachbearbeiter greifen mit Hilfe ihres Arbeitsplatz-PC (9750-Terminalemulation) über ein Netzwerk der OFD/ZBS auf den Großrechner zu. Das Netzwerk soll auch zur Bürokommunikation (vorrangig Textverarbeitung, aber auch Tabellenkalkulation, Präsentation und eMail) genutzt werden.

Die vom MWF zur Einführung eingerichtete Projektgruppe erarbeitete aufgrund meiner Anforderungen ergänzend zum Hauptuntersuchungsbericht und zur Detailorganisation nach den ADV-Projektrichtlinien eine Risikoanalyse und das daraus abgeleitete Sicherheitskonzept. Bei der Vernetzung wurden die aus dem IT-Grundschutzhandbuch des BSI entnommenen Anforderungen an den Serverbetrieb, soweit unter den gegebenen Umständen noch erforderlich, realisiert. Eine IT-Revision kontrolliert die Einhaltung der Maßnahmen.

Eine Prüfung der vorgelegten Unterlagen und des laufenden Verfahrens beim Abschlußtest ergab keine grundsätzlichen datenschutzrechtlichen Bedenken zur Einführung des Verfahrens DAISY. Es waren lediglich kleinere Ergänzungen vorzunehmen und Unterlagen entsprechend dem Verfahrensgang vorzulegen (Meldung zum Dateienregister, Dienstanweisung).

5.5 Einbürgerungsverfahren

Das Ministerium des Innern beabsichtigte die Einführung eines Verfahrens zur Erfassung und Bearbeitung von Einbürgerungsanträgen. Dabei wurde eine fertige Software am Markt erworben und durch Textverarbeitungsmakros ergänzt.

Nachdem das Ministerium zunächst lediglich ein Anwenderhandbuch und eine Systembeschreibung übersandt hatte, mußte ich es für die datenschutzrechtliche Bewertung gemäß § 8 SDSG zur Vervollständigung der Unterlagen gemäß den ADV-Projektrichtlinien und zur Vorlage eines Sicherheitskonzepts auffordern. Danach gelang es dem Ministerium aber in überraschend kurzer Zeit, ein umfangreiches und abgerundetes Sicherheitskonzept vorzulegen. Da eine allgemein für das Ministerium gültige Dienstanweisung noch nicht in Kraft war, wurde eine verfahrensspezifische Dienstanweisung erlassen, in der die organisatorischen Maßnahmen zusammengefaßt waren. Der Verfahrensfreigabe stand danach nichts mehr im Wege.

5.6 TK-Anlagenverbund

Die TK-Anlagen der meisten Obersten Landesbehörden einschließlich einiger nachgeordneter Bereiche sind inzwischen unter einer Nummer zu einem TK-Anlagenverbund zusammengefaßt. Die Vermittlung erfolgt nur noch an einer einzigen Stelle. Für diese Maßnahme, die die angeschlossenen Landesdienststellen leichter erreichbar macht, sprechen auch Gründe der Wirtschaftlichkeit.

Auf meine Beteiligung und den Beginn meiner Prüfung wurde bereits im letzten Bericht eingegangen (TZ 15.3.6). Zu Beginn meiner Datenschutzprüfung bestand noch ein gesplittetes Zuständigkeitsverhältnis, demzufolge die Installation und der Betrieb des technischen Teils im Zuständigkeitsbereich des Ministeriums für Finanzen und die Administration der TK-Anlage und der Einsatz der Vermittlungskräfte im Zuständigkeitsbereich des Ministeriums für Umwelt lag.

Die Kontrolle des TK-Anlageneinsatzes unter Berücksichtigung einer Checkliste (siehe TZ 4.12) brachte folgende Mängel an den Tag:

- die Konfiguration der TK-Anlagenparameter wurde durch den Lieferanten vorgenommen, ohne daß eine Kontrolle durch den Auftraggeber möglich war,

- die systemtechnische Betreuung der TK-Anlage als EDV-System wurde durch den Lieferanten vorgenommen, ohne daß eine Kontrolle durch den Auftraggeber möglich war,

- eine Revision und eine interne Datenschutzkontrolle waren nicht eingerichtet,

- Wartung und Reparatur erfolgten durch den Lieferanten zu den ihm genehmen Zeitpunkten; er besaß einen eigenen Schlüssel, den er auch dazu nutzte, potentielle Kunden zu einer Anlagenbesichtigung einzuladen, ohne daß der Auftraggeber dies überwachen konnte,

- die zentrale Anlage war in einem Raum quasi in Erdgeschoßhöhe untergebracht, so daß Einbrüche oder Sabotage leicht möglich waren; zusätzlich waren alle Konsolen und der Computer für die Gebührenauswertung im gleichen Raum installiert und damit für jeden zugänglich, der Zugang zur Anlage hatte,

- die Dokumentation der Anlagenparameter wurde durch den Lieferanten vorgenommen, der auch die Datensicherung durchführte und die Datenbänder außer Haus brachte und in seinen Firmenräumlichkeiten aufbewahrte,

- die Betreuung der Apparatevergabe und die Zuordnung von Berechtigungen mußte von einer Kraft nebenbei erledigt werden; eine Vertretung war nur formal bestellt; die Betreuungskräfte waren mangels Unterrichtung nicht in der Lage, die Arbeiten des Lieferanten zu überwachen,

- eine schriftliche Regelung (Erlaß oder Dienstanweisung) über zusätzliche Leistungsmerkmale, Datensicherungsmaßnahmen, Zuständigkeiten, Freigabeverfahren, Meldung zum Dateienregister usw. war nicht vorhanden,

- Unterlagen und Zugangsschlüssel zur gemeinsamen TK-Anlage und zu den Unteranlagen für Notfälle waren nicht verfügbar,

- die Anlage befand sich ohne ausreichende datenschutzrechtliche Beteiligung schon im Echtbetrieb; eine Freigabe war noch nicht erteilt worden.

- zusätzlich kam aus Gründen der Kostenersparnis noch die Absicht hinzu, dem Lieferanten eine Fernwartung mit der Möglichkeit des Online-Zugriffs auf prinzipiell alle Programme, Parameter und Daten der TK-Anlage zu erlauben.

In mehreren Abstimmungen mit dem Ministerium für Wirtschaft und Finanzen und der Hochbauverwaltung, bei denen wegen der ressortübergreifenden Zuständigkeiten zuletzt sogar die Staatskanzlei eingeschaltet wurde, ist es inzwischen gelungen, den Einsatz des TK-Anlagenverbundes datenschutzgerecht zu gestalten und die oben genannten Mängel abzustellen. Insbesondere wurden die Zuständigkeiten in einer Hand im Bereich des Ministeriums für Wirtschaft und Finanzen zusammengefaßt, die TK-Anlage sicher untergebracht, eine ausreichende personelle Betreuung sichergestellt und eine IT-Revision und interne Datenschutzkontrolle eingerichtet. Aufgrund der vorgebrachten datenschutzrechtlichen Bedenken verzichtete das Ministerium auf eine Fernwartung und gab sich mit einer Fernsignalisierung im Störungsfall zufrieden; der dann überwachte Einsatz des Wartungstechnikers vor Ort erscheint datenschutzrechtlich unbedenklich. Die letztlich noch ausstehende Dienstanweisung, in der die organisatorischen Regelungen beschrieben sind, soll in Kürze nachgereicht werden.

5.7 Verrechnung von privaten Telefongebühren über Bezügeverfahren

Das Ministerium für Wirtschaft und Finanzen hatte sich zum Ziel gesetzt, das bisherige Großrechnerverfahren zur Abrechnung privater Telefondaten, bei dem zur Beitreibung der Gebühren zusätzlicher manueller und personeller Aufwand erforderlich war, durch eine kostengünstigere PC-Anwendung abzulösen, bei der zusätzlich die Abrechnungsdaten in das Bezügeverfahren automatisch per Diskettentransport übernommen werden können. Später ist eine Übertragung der Daten per Datenfernübertragung beabsichtigt. Das Verfahren wurde erst einmal für den Bereich des

Ministeriums vorläufig freigegeben, um für eine Ausweitung auf alle Ressorts Erfahrungen damit zu sammeln.

Eine weitere mögliche Kenntnisnahme personenbezogener Daten im Rahmen der Gebührenerhebung entfällt. Ich habe aber darauf hingewiesen, daß bei der Übermittlung der Gebührendaten per Diskette oder später über Datenleitungen zur Sicherung der Datenübertragung eine Verschlüsselung eingesetzt werden muß.

5.8 Automatisiertes Informationssystem der Polizei „DIPOL"

Über das Vorhaben des Ministeriums des Innern, mit dem Verfahren „DIPOL" ein automationsgestütztes Kommunikations- und Informationssystem der Polizeidienststellen einzurichten, wurde bereits wiederholt berichtet (11.TB TZ 3.2; 12. TB TZ 3.1; 14. TB TZ 2.6; 15. TB TZ 2.1). Ich begleite es aus datenschutzrechtlicher Sicht von Anfang an mit großem Interesse, da ich es für sehr wichtig halte, daß der Datenschutz bei diesem umfangreichen Projekt in allen Phasen und bei allen Aktivitäten gewahrt sein muß. Um sich noch tiefere Einblicke in die Verarbeitungsvorgänge verschaffen zu können, haben auch zwei Mitarbeiter meiner Dienststelle an einer Schulung zur Nutzung des Systems durch Polizeibeamte teilgenommen.

Eine abschließende Beurteilung des zunächst verfolgten Konzepts war allerdings bis zum Piloteinsatz 1995 nicht möglich. Insbesondere waren zum damaligen Zeitpunkt noch eine datenschutzrechtliche Beurteilung der Benutzerrechtematrix und der zu speichernden Protokollierungsdaten und die Sicherstellung einer polizeiinternen Revision und Datenschutzkontrolle offengeblieben.

Aufgrund der Probleme, die im Rahmen des Piloteinsatzes der DIPOL-Lösung in der Polizeidirektion Ost sichtbar wurden, hat das Ministerium Ende 1995 die bis dahin erarbeitete technische Lösung aufgegeben. Inzwischen wurde mir ein neues technisches Grobkonzept zur Prüfung vorgelegt, bei dem die bisher angestrebte Bildschirmlösung durch PC-Unterstützung ersetzt und die Individualsoftware DIPOL zu einer Client-Server-Lösung weiterentwickelt werden soll. Das Innenministerium, das sich an einer kooperativen Begleitung des neuen Versuchs durch den

Landesbeauftragten für Datenschutz sehr interessiert zeigt, will in einem späteren, zusätzlichen Differenzpapier die Auswirkungen der geänderten Rahmenbedingungen auf datenschutzrechtliche Aspekte näher herausstellen; zur besseren Übersicht habe ich weiter um eine neue Risikoanalyse und ein darauf aufbauendes Sicherheitskonzept gebeten.

Inzwischen wurden die ersten 250 Arbeitsplätze mit PC ausgestattet und in Abstimmung mit meiner Dienststelle eine Basislösung zur Textverarbeitung und eine allgemeine und für den Einsatzbereich ergänzte IT-Dienstanweisung freigegeben. Allerdings waren bei Redaktionsschluß dieses Berichtes die Strukturen der Datenbanken für das System noch nicht so präzise bestimmt, daß einem Echteinsatz zugestimmt werden konnte.

5.9 Firewall bei Unikliniken und ZDV-Saar

Für die medizinische Forschung und die Krankenversorgung in den Universitätskliniken wurde es zunehmend erforderlich, vom Klinikum in Homburg auf solche Informationen zuzugreifen, die in globalen Datennetzen wie dem Internet oder dem Deutschen Wissenschaftsnetz (WiN) verfügbar sind. Diese Zugriffe sollten von den zugelassen Arbeitsplätzen aus über das Kommunikationsnetz IMMUN ermöglicht werden. Um den dabei auftretenden datenschutzrechtlichen Risiken zu begegnen, hat das Rechenzentrum der Unikliniken unter Berücksichtigung der in meiner Orientierungshilfe zum Internet (siehe TZ 4.7) dargestellten Empfehlungen eine sogenannte Firewall als Filter- und Schutzfunktion eingerichtet, um das Netz und die daran angeschlossenen Rechner mit ihren Daten vor unberechtigtem Zugriff zu schützen. Eine eigene IT-Dienstanweisung für den Internetzugang befindet sich in der Abstimmung.

Auch verschiedene Ressorts der Landesverwaltung streben einen Internetzugang an. Nachdem die Landesregierung durch die ZDV-Saar ein eigenes Informationsangebot auf einem abgesetzten Internet-Server realisiert hatte, laufen derzeit die Arbeiten, um auch Netzanbindungen der Ressorts zu ermöglichen. Zur Absicherung dieser Anschlüsse hat die ZDV-Saar ebenfalls eine Firewall eingerichtet. Das weitere Vorgehen soll auch hier gemäß meinen Vorschlägen betrieben werden.

5.10 Modernisierung bei den Unikliniken Homburg mit SAP R/3

Aus Wirtschaftlichkeitsgründen haben die Uniklinken Ende 1994 damit begonnen, die vorhandenen Datenverarbeitungsverfahren mit Hilfe eines weit verbreiteten, aber nicht spezifisch auf die Belange eines Krankenhauses zugeschnittenen Standard-Softwarepaketes (Systems SAP R/3) abzulösen; nur so war die Verpflichtung des Gesundheitsstrukturgesetzes zu erfüllen, zum 1.1.96 kostenrechnende Verfahren einzuführen. Die unter hohem Zeitdruck stehende Einführung der verschiedenen Module des Systems (Personalwirtschaft, Patientenadministration und -abrechnung, Dokumentation) werden von einer Projektgruppe begleitet.

Meine Dienststelle wurde beteiligt. Ich konnte hierbei erreichen, daß nach anfänglicher Konzentration auf wirtschaftliche und damit verbundene sicherheitstechnische Aspekte verstärkt auch der Datenschutz einbezogen wurde. Unter Berücksichtigung meiner Vorschläge (siehe TZ 4.9) ist die Arbeitsgruppe derzeit damit befaßt, insgesamt und für einzelne Module eine umfangreiche und ausgefeilte Risikoanalyse mit Sicherheitskonzept zu erarbeiten. Die bisher vorgelegten Entwürfe sind schon sehr ausgereift. Zusätzlich wurde eine Dienstvereinbarung zwischen der Verwaltung und dem Personalrat der Universitätskliniken abgeschlossen, in der personal- und datenschutzrechtliche Fragen geregelt werden.

Zur datenschutzrechtlichen Beurteilung des Programms selbst enthielten die zunächst übergebenen Unterlagen des Softwareanbieters leider nur sehr wenige Informationen und Hinweise auf entsprechende Maßnahmen; ein Prüfkonzept ist für 1997 angekündigt.

Ich habe das Verfahren vor Ort überprüft und dabei einige Schwachstellen festgestellt, über deren Beseitigung ich mich derzeit mit den Universitätskliniken in der Diskussion befinde:

- In den Bildschirmmasken erscheinen eine Vielzahl von Datenfeldern, die in den Universitätskliniken nicht ausgefüllt werden. Damit es hier nicht zu unzulässigen Eintragungen kommt, sind die entsprechenden Felder für eine Eingabe zu sperren.

– Das Datum „Hausarzt", das von jedem Patienten bei der Aufnahme erfragt wird, sollte als freiwillig gekennzeichnete Angabe in den Aufnahme-Vertrag aufgenommen werden.

– Die in dem Programm vorgesehenen Bemerkungsfelder sind ersatzlos zu streichen, weil hier die datenschutzrechtliche Gefahr besteht, daß nicht erforderliche Daten in diese Felder eingetragen werden.

– Das Programm erlaubt über eine *-Funktion eine umfassende Suchmöglichkeit. Ich habe vorgeschlagen, daß nur der Nachname in Verbindung mit dem Geburtsdatum als Eingangs-Suchfunktion akzeptiert wird.

– Der Umfang der Daten, die die Krankenhäuser zulässigerweise an die Krankenkassen übermitteln dürfen, ist gesetzlich festgelegt (§ 301 Abs. 1 SGB V). Bei einigen Daten aus der mir vorgelegten Dateibeschreibung habe ich Zweifel, ob ihre Übermittlung vom Katalog des § 301 Abs. 1 SGB V abgedeckt ist. Ich habe die Universitätskliniken um Erläuterung gebeten.

– Die Erhebung der Daten bei der Krankenhausaufnahme erfolgt in fünf sogenannten Aufnahmestützpunkten. Ich habe kritisiert, daß alle Mitarbeiter aller Aufnahmestationen Zugriff auf die Daten aller Patienten haben.

– Angemahnt habe ich die Festlegung von Löschungsfristen hinsichtlich der im System gespeicherten Daten. Auch widerspricht die Absicht, alle Daten auf Dauer im Direktzugriff zu halten, dem Saarländischen Krankenhausgesetz, wonach Patientendaten, die im automatisierten Verfahren mit der Möglichkeit des Direktabrufes gespeichert sind, unmittelbar nach Abschluß der Behandlung zu löschen sind. Lediglich Daten, die zur Auffindung archivierter Daten erforderlich sind, dürfen auskunftsfähig gespeichert bleiben.

– Es ist eine terminalspezifische Zuordnung der Kennungen vorzunehmen. Außerdem muß das Windows-System auf den Arbeitsplatzrechnern gegen mißbräuchliche Nutzung abgesichert werden. Ein BIOS-Paßwortschutz der PC ist zu aktivieren.

- Die Protokollierung von Zugriffen ist nicht datenschutzgerecht gestaltet, insbesondere werden fehlerhafte Paßworteingaben nicht protokolliert und Mehrfachfehleingaben führen zu keinem Sperren der Anwendung.

- Lesende Zugriffe auf Patientendaten werden nicht protokolliert.

- Ein Paßwortänderungsintervall ist zwar einstellbar, doch wird eine sichere Paßwortänderung nicht überwacht, so daß z. B. eine Minimaländerung am alten Paßwort (nur eine Stelle neu) möglich ist.

- Ein automatischer Verfahrensabbruch bei längerer Nichtbenutzung ist nicht realisiert.

- Alle Erfassungskräfte können alle Patientendaten lesen und schreiben; eine Beschränkung auf Buchstabengruppen ist nicht möglich.

- Alle Rechte können von jedem beliebigen Terminal aus genutzt werden; eine terminalspezifische Zuordnung von Benutzerkennungen ist nicht vorhanden.

Für eine spätere Version der Software ist eine Behebung der Probleme zugesagt. Teilweise kann den Problemen durch die Netzwerksoftware begegnet werden, indem z. B. ein übergeordnetes Paßwort vor der Nutzung des SAP-Systems abgefragt wird, deren Modalitäten vom Klinikrechenzentrum gesteuert werden können.

Da die datenschutzrechtlichen Probleme beim Einsatz der Software SAP R/3 inzwischen bei der Prüfung mehrerer Datenschutzbeauftragter bei Anwendern in ihren Ländern festgestellt wurden, ist beabsichtigt, die Erkenntnisse in einer Arbeitsgruppe zusammenzutragen und in einer gemeinsamen Stellungnahme den Lieferanten zur Behebung aufzufordern.

6 Allgemeines Datenschutzrecht

6.1 Datenschutz im Rahmen der Europäischen Union

Markstein für die Entwicklung des Datenschutzes auf europäischer Ebene im Berichtszeitraum war die EU-Datenschutzrichtlinie („Richtlinie 95/46/EG des Europäischen Parlamentes und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr"). Nach mehrjährigen Verhandlungen konnte sie unter deutscher Präsidentschaft im Juli 1995 im Ministerrat beschlossen und vom Parlament am 24. Oktober 1995 verabschiedet werden.

Ein einklagbares europäisches Grundrecht auf Datenschutz, wie es nicht nur wiederholt die Datenschutzbeauftragten des Bundes und der Länder angeregt hatten, sondern von den Beauftragten aller Mitgliedsländer der Europäischen Union im September 1995 gefordert worden war, ist in den Gemeinschaftsverträgen zwar noch nicht verwirklicht. Dies bleibt ein Anliegen für die weitere Entwicklung der Gemeinschaft. Obwohl in einzelnen Bereichen weiterhin spezifische Regelungen fehlen, ist zu begrüßen, daß mit der Richtlinie ein großer Fortschritt für den Datenschutz auf europäischer Ebene erreicht wird (vgl. Entschließung der DSB-Konferenz vom 9./10. 11. 1995, Anlage 5).

Erfreulicherweise beschränkt sich die Richtlinie nicht auf Minimalregeln, die Hemmnisse im freien Handels- und Dienstleistungsverkehr auf kleinstem gemeinsamem Nenner ausschließen sollen. Sie bemüht sich vielmehr durchaus um eine Harmonisierung des Datenschutzes auf hohem Niveau, auf dem dann zugleich in der EU ein grenzüberschreitender Datenverkehr künftig ohne Beschränkungen stattfinden kann. Dies macht, da die Richtlinie nicht unmittelbar gilt, in der dreijährigen Anpassungsfrist bei vielen Mitgliedsstaaten erhebliche Verbesserungen im Rechtsstatus für die Bürger notwendig und zwingt zu positiver Angleichung auch dort, wo dieser spezielle Persönlichkeitsschutz bereits bislang normiert war.

Erforderlich ist nicht die wörtliche Übernahme des Richtlinientextes in das nationale Recht, sondern die Gewährleistung eines entsprechenden Schutzniveaus. Damit besteht insbesondere in der organisatorischen Ausgestaltung Spielraum für die jeweiligen Staaten. Gleichwohl gibt es in

vielen Punkten einen zwingenden Anpassungsbedarf in den allgemeinen und bereichsspezifischen Datenschutzbestimmungen.

6.2 Bundesdatenschutzgesetz

Im deutschen Recht ist von der Anpassungspflicht an die EU-Richtlinie in erster Linie das Bundesdatenschutzgesetz betroffen, vor allem wegen seiner Geltung für den nicht-öffentlichen Bereich. Die Stärkung der Bürgerrechte im wirtschaftlichen und sonstigen privatrechtlichen Bereich ist ja gerade ein wesentliches Anliegen der Gemeinschaftsinitiative gewesen. Das BDSG hat überdies unmittelbare Geltung für öffentliche Stellen auch im Bereich der Länder; ihm kommt auch für die Landesregelungen Modellcharakter zu.

Die Datenschutzbeauftragten des Bundes und der Länder haben hierzu aus ihren Erfahrungen und Kenntnissen einen umfangreichen Katalog von Änderungsanregungen zusammengestellt und zwischenzeitlich an den federführenden Bundesinnenminister übermittelt. Es ist selbstverständlich, daß sie sich an der weiteren Beratung beteiligen und ihren Rat einbringen werden. Gleiches gilt ebenso auf Landesebene für die Anpassung des SDSG und spezifischen Datenschutzrechts; auch dem Minister des Innern habe ich diese Vorschläge unterbreitet.

Während der Bundesinnenminister - auch aus Zeitgründen - die Gesetzesänderung lediglich in dem für die Anpassung unumgänglichen Umfang anstrebt, gehen die Vorschläge darüber hinaus. Gemeinsam mit meinen Kollegen in Bund und Ländern und auch den obersten Aufsichtsbehörden für den nichtöffentlichen Bereich (Düsseldorfer Kreis) halte ich es für sinnvoll, die jetzt notwendige Anpassung des Bundesdatenschutzgesetzes nicht auf den drängendsten Bedarf zu begrenzen, sondern die Chance zu einer Fortentwicklung zu nutzen. Das gesamte Datenschutzrecht sollte modernisiert werden, damit das Selbstbestimmungsrecht des Bürgers entsprechend den veränderten rechtlichen, technischen und sozialen Entwicklungen gewährleistet werden kann.

Die wesentlichen Gesichtspunkte und Zielsetzungen für eine Modernisierung des Datenschutzrechtes, die im Zusammenhang mit der Umsetzung der EU-Datenschutzrichtlinie vorgenommen werden sollte, haben die Da-

tenschutzbeauftragten in einer Entschließung vom 14./15. März 1996 zusammengefaßt, die als Anlage 6 beigefügt ist.

Herausgehoben seien lediglich einige Aspekte:

Die Richtlinie unterscheidet bei den „für die Datenverarbeitung Verantwortlichen" nicht zwischen natürlichen und juristischen Personen sowie zwischen öffentlichem und privatem Bereich. Mit der Normierung in gemeinsamen Vorschriften trägt sie der Erkenntnis Rechnung, daß die Persönlichkeitsrechte durch nicht-öffentliche Stellen nicht prinzipiell weniger gefährdet sind und deswegen dort keines geringeren Schutzes bedürfen; die Rechtsformen sind im übrigen weitgehend austauschbar.

Wesentlich ist, daß gleichermaßen für öffentlichen wie privaten Bereich ein hoher Datenschutzstandard erreicht wird. Das bedeutet nicht zwangsläufig, daß der nationale Gesetzgeber zwischen beiden Bereichen nicht mehr differenzieren dürfe, zumal die datenschutzrechtlich besonders relevanten Bereiche Justiz und Sicherheit vom Geltungsbereich der Richtlinie nicht umfaßt sind. Selbstverständlich wird es nach wie vor besondere Anforderungen an die öffentlichen Stellen geben (müssen), weil die Rechtsbeziehungen zu diesen von denen unter Privaten abweichen. Die Vereinheitlichung der Kontrollstellen liegt zwar nahe, wird aber ebenfalls von der Richtlinie nicht erzwungen.

Generell sind von vornherein bei allen Regelungen, die sich auf Inhalt und Grenzen der Persönlichkeitsrechte beziehen, eingehend die Risiken hierfür zu bewerten und durch verfahrensmäßige Kontrollmöglichkeiten einzugrenzen. Dies setzt entsprechend ausgestattete unabhängige Instanzen voraus.

Notwendig ist aber auch, innerhalb der öffentlichen Stellen selbst stärker als bisher interne Verantwortlichkeiten herauszuarbeiten und mit effektiven Instrumenten der Eigenprüfung zu unterstützen.

Gerade die Herausforderung durch neue Techniken macht wesentlich, dem Aspekt Datensicherheit größere Bedeutung beizumessen und dies organisatorisch abzusichern. Lassen Gefahren sich nicht durch Verwendung datensparsamer Technologien von Beginn an begrenzen, müssen

vor allem auch die Techniken selbst genutzt werden, möglichst sichere und „unschädliche" Lösungen zu finden.

Zur konkreten Umsetzung bei Novellierung des BDSG werden die Datenschutzbeauftragten - auch im Rahmen ihrer gegenseitigen Zusammenarbeit und mit den Aufsichtsbehörden - sich mit Anregungen und Vorschlägen beteiligen.

6.3 Saarländisches Datenschutzgesetz

Soweit das Landesrecht von der Anpassungspflicht betroffen ist, erscheint sinnvoll, vor detaillierten Vorschlägen zur Änderung des SDSG das Gesetzgebungsverfahren zum Bundesdatenschutzgesetz abzuwarten. In diesem Zusammenhang können und sollten dann auch die Erfahrungen mit dem Gesetz von 1993 und neuere Entwicklungen berücksichtigt werden. Auf mögliche Änderungen bezüglich des Dateienregisters oder behördlicher Datenschutzbeauftragter hatte ich bereits in TZ 3.2 hingewiesen.

Im Berichtszeitraum blieben dieses Gesetz und seine verfassungsrechtliche Grundlage unverändert. Der Vorschlag der Fraktion Bündnis 90/Die Grünen, das Wahlverfahren für den Landesbeauftragten zu ändern, wurde von den anderen Fraktionen abgelehnt (vgl. TZ 1).

6.4 Parlamentarischer Datenschutz

Auch in den Parlamenten werden personenbezogene Daten zunehmend mit moderner Informations- und Kommunikationstechnik verarbeitet und einem breiteren Kreis von Interessenten erschlossen. Dabei geht es nicht allein um Angaben über die Abgeordneten selbst, sondern - etwa bei Eingaben oder der parlamentarischen Kontrolle konkreter Verwaltungsvorgänge - um Daten „normaler Bürger".

Der in der Verfassung (Art. 2 SVerf) für jedermann verbriefte Schutz des informationellen Selbstbestimmungsrechts gilt selbstverständlich auch hier; an konkretisierenden Bestimmungen, die dieses Recht gegen höher-

rangige Allgemeininteressen und Rechtsgüter anderer abwägen, fehlt es aber weitgehend. So gilt im Saarland ausdrücklich das (allgemeine) Datenschutzrecht des SDSG nur, soweit der Landtag „Verwaltungsaufgaben" wahrnimmt (§ 2 Abs. 1 Satz 2). Im „eigentlichen parlamentarischen" Bereich finden sich nur punktuelle Vorschriften über den Umgang mit (personenbezogenen) Daten.

In Erkenntnis dieses Regelungsdefizits haben die Parlamentspräsidenten von Bund und Ländern Empfehlungen erarbeiten lassen, mit denen die Datenschutzbeauftragten befaßt waren. Dem Präsidenten des Landtags habe ich meine Auffassung mitgeteilt. Eben weil nicht allein Daten der Parlamentarier selbst betroffen sind, erscheint wesentlich, über bloße Geschäftsordnungen hinaus Regelungen mit verbindlicher Außenwirkung zu schaffen. Soweit hierbei an eine „Datenschutzordnung" gedacht wird, die als eigenständige Regelungsform neben dem förmlichen Gesetz bislang nicht ausdrücklich vorgesehen ist, habe ich zu erwägen gegeben, die Möglichkeit im Rahmen der derzeitigen Enquête-Kommission zur Verfassungsreform zu prüfen.

6.5 Abgrenzung öffentlicher/privater Bereich

Im Berichtszeitraum hatte ich mich aufgrund von Einzelfällen, die an mich herangetragen wurden, mit der Frage zu befassen, ob privat-rechtlich organisierte Unternehmen, an denen das Land, Gemeinden, Gemeindeverbände oder der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts beteiligt sind, meiner Kontrollkompetenz unterliegen oder ob die Einhaltung der datenschutzrechtlichen Bestimmungen bei diesen Unternehmen von dem Ministerium des Innern als Aufsichtsbehörde für den Datenschutz im privaten Bereich kontrolliert wird. Es geht hier nicht allein um die Abgrenzung der Zuständigkeiten zwischen verschiedenen Behörden; die Entscheidung über die zuständige Kontrollinstanz hat vielmehr auch praktische Auswirkungen. Während beispielsweise der Landesbeauftragte für Datenschutz bei den seiner Kontrolle unterliegenden Stellen jederzeit und ohne besondere Voraussetzungen Datenschutzprüfungen durchführen kann, hat die Aufsichtsbehörde für den Datenschutz im privaten Bereich dieses Recht nur, wenn ihr hinreichende Anhaltspunkte für eine Verletzung von Vorschriften über den Datenschutz vorliegen.

Ausgangspunkt der Beurteilung ist die Vorschrift des § 2 Abs. 1 Satz 1 des Saarländischen Datenschutzgesetzes, der den Anwendungsbereich des Gesetzes festlegt. Über die in § 2 Abs. 1 Satz 1 SDSG genannten Gebietskörperschaften (Land, Gemeinden, Gemeindeverbände) und sonstigen öffentlich-rechtlich organisierten juristischen Personen unter Aufsicht des Landes hinaus sind danach auch „deren Vereinigungen" öffentliche Stellen.

Auch wenn das Saarländische Datenschutzgesetz - anders als das Bundesdatenschutzgesetz und verschiedene übrige Landesdatenschutzgesetze - auf den Zusatz „... ungeachtet ihrer Rechtsform" verzichtet, kann über eine derartige Auslegung kein Streit bestehen; die Begründung zu Absatz 1 der Neuregelung 1993 (Landtagsdrucksache 10/526) führt ausdrücklich aus: „Die Normadressaten in Absatz 1 entsprechen dem bisherigen Recht. Dazu gehören auch Vereinigungen öffentlicher Träger in Privatrechtsform, soweit sie Aufgaben der öffentlichen Verwaltung wahrnehmen."

Über Fälle einer „Formalprivatisierung" hinaus, in denen ein oder mehrere öffentliche Rechtsträger sämtliche Anteile einer privatrechtlichen Organisation halten, schließt es die Qualifikation als „öffentliche Stelle" nicht aus, wenn sich an der Vereinigung auch „echte" private Stellen (natürliche Personen oder juristische Personen des Privatrechts) beteiligen. Bei bloß untergeordneter Fremdbeteiligung könnte sonst der Normzweck durch „Flucht in das Privatrecht" unterlaufen werden.

Weil hier aber Norm- und Kontrollkompetenzkonflikte entstehen, muß eine Abgrenzung erfolgen: Eine öffentliche Stelle ist in Abstimmung mit dem Ministerium des Innern dann anzunehmen, wenn die öffentlichen Rechtsträger (insgesamt) beherrschenden Einfluß auf die Vereinigung ausüben. Von einem beherrschenden Einfluß gehe ich jedenfalls dann aus, wenn den öffentlichen Rechtsträgern insgesamt die absolute Mehrheit der Besitzanteile und entsprechendes Stimmengewicht zustehen.

Voraussetzung für das Vorliegen einer „Vereinigung" im Sinne des § 2 Abs. 1 SDSG ist nicht, daß sich hieran mehrere öffentliche Rechtsträger beteiligen. Die teilweise vertretene abweichende Meinung hätte das Ergebnis zur Folge, daß ein öffentlicher Rechtsträger sich durch Formalpri-

vatisierung von Aufgaben dann teilweise öffentlich-rechtlich bestehender Bindungen entledigen könnte, wenn er allein alle Anteile hält, jedoch bei jeder - auch untergeordneter - Beteiligung Dritter an der neuen Einrichtung der Kontrolle des Landesbeauftragten für Datenschutz unterworfen bleibt.

Aus dem Normzweck ist schließlich als zusätzliches Kriterium zu fordern, daß die Vereinigung „Aufgaben der öffentlichen Verwaltung" wahrnehmen muß, wenn sie als „öffentliche Stelle" der Kontrollkompetenz des Landesbeauftragten für Datenschutz unterworfen sein soll. Verwaltungsaufgaben sind dabei in weiterem Umfang zu verstehen als hoheitliche Aufgaben, denn im letzeren Fall gilt gemäß § 2 Abs. 4 Satz 2 BDSG selbst ein Privatrechtssubjekt ohne jegliche Beteiligung der öffentlichen Hand als öffentliche Stelle.

Unter Zugrundelegung dieser Kriterien stufe ich die in der Trägerschaft von Gemeinden und Gemeindeverbänden betriebenen Krankenhäuser als meiner Kontrollkompetenz unterliegende Einrichtungen ein. Ein anderes Beispiel ist die Versorgungs- und Verkehrsgesellschaft einer Stadt, für die ich trotz ihrer privatrechtlichen Organisationsform meine Kontrollkompetenz in Anspruch nehme. Dies wird von dieser Gesellschaft mit der nach meiner Auffassung unzutreffenden Argumentation bestritten, sie sei keine „Vereinigung" im datenschutzrechtlichen Sinne, da deren Anteile vollständig von nur einem Eigentümer, der Stadt, gehalten würden.

Eine gesetzliche Abgrenzung der Kontrollzuständigkeit wäre auch aus Sicht der Betroffenen wünschenswert. Nicht sinnvoll erschiene jedoch, hierbei allein an die formalrechtliche Gestaltung anzuknüpfen, wie es in einem anderen Bundesland vorgeschlagen wurde.

7 Polizei

7.1 Europol

Daß die Kriminalitätsbekämpfung nicht allein regional erfolgen kann, sondern der Zusammenarbeit über die Landesgrenzen hinweg bedarf, wird immer deutlicher. Bund und Länder bemühen sich schon seit längerer Zeit

darum, die verbindlichen Rechtsgrundlagen für die Zusammenarbeit von Bundes- und Länderpolizeien zu schaffen, die eng verbunden ist mit der angestrebten gemeinsamen Kriminalitätsbekämpfung auf der Ebene aller EU-Staaten.

So liegt der Entwurf eines Gesetzes vor, mit dem das Übereinkommen der Mitgliedsstaaten der Europäischen Union vom 25.7.1995 über die Errichtung eines europäischen Polizeiamtes (Europol-Gesetz) in national verbindliches Recht umgesetzt werden soll. Dieser Entwurf verweist in zahlreichen Bestimmungen auf den im Gesetzgebungsverfahren schon weiter fortgeschrittenen Entwurf eines Gesetzes über das Bundeskriminalamt (BKA), das die noch gültige Fassung aus dem Jahre 1973 ablösen soll.

So sehr zu begrüßen ist, daß der Gesetzgeber die längst überfällige normative Regelung nunmehr trifft, können die derzeitigen Vorstellungen noch nicht befriedigen. Dies betrifft nicht nur die gesamtstaatliche Aufgabenverteilung, die durch beide Gesetzentwürfe zu Lasten der Länder eingegrenzt wird. Länderinteressen sind insoweit in besonderem Maße berührt, als landesrechtlicher Gesetzgebungskompetenz sowohl das Polizeirecht als auch das Datenschutzrecht unterliegen. Die föderativen Grundsätze sind auch bei Verwirklichung eines vereinten Europas zu gewährleisten (Art. 23 GG).

Vor allem aber muß vermieden werden, daß man sich - um der gedeihlichen Zusammenarbeit mit den Nachbarstaaten willen - im Polizeirecht auf einen recht kleinen gemeinsamen Nenner des Datenschutzniveaus einigt. Die mit den anderen Staaten diskutierten Vorschläge für weitere Bestimmungen, die zusätzlich zur Konvention für die Tätigkeit von Europol noch erlassen werden müssen, lassen eine derartige Befürchtung allzu gerechtfertigt erscheinen.

Zum Entwurf des BKA-G hatte die Konferenz der Datenschutzbeauftragten bereits in einer Entschließung vom 9./10.3.95 (Anlage 7) Anforderungen an die notwendige gesetzliche Regelung formuliert. Ob das künftige Gesetz diesen entsprechen wird, läßt sich wegen der noch andauernden Beratungen mit dem Europol-Gesetz noch nicht abschließend beurteilen.

7.2 Gemeinsame Grenzkommissariate

Die an Frankreich angrenzenden Bundesländer Baden-Württemberg, Rheinland-Pfalz, Saarland haben Verhandlungen mit Frankreich über ein polizeiliches Zusammenarbeitsabkommen aufgenommen. Das Innenministerium hat mich hierbei beteiligt und Entwurfsfassungen vorgelegt, zu denen ich teilweise kritisch Stellung genommen habe. Die Verhandlungen dauern noch an; die letzte Fassung des Datenschutzartikels (Art. 12), der auf die Anwendbarkeit des Schengener Durchführungsübereinkommens für den Informationsaustausch verweist, räumt die Bedenken gegen die Vorentwürfe aus.

7.3 Novelle Polizeigesetz

Mit dem Erfordernis europäischer Zusammenarbeit wurde auch eine Novellierung des Saarländischen Polizeigesetzes begründet.

Zum einen wird hiermit die Rechtsgrundlage für eine Informationsübermittlung der Polizei an ausländische Polizeibehörden geschaffen. Daß ein solcher Datenaustausch notwendig ist, für den das Innenministerium in einer Verordnung nähere Regelungen zu treffen hat, liegt auf der Hand. Aus der Sicht des Datenschutzes gab es dazu im Gesetzgebungsverfahren zur Änderung des Polizeigesetzes selbstverständlich keine Einwände. Das Ministerium des Innern hat inzwischen den Entwurf einer Rechtsverordnung vorgelegt, der nach unserer Stellungnahme in einigen Punkten noch verbessert werden könnte. Die endgültige Fassung ist mir bislang nicht bekannt.

Ganz anders zu beurteilen ist allerdings die im Vordergrund stehende Initiative mit dem Ziel, den Datenschutzstandard des seit 1990 geltenden Polizeigesetzes in wesentlichen Bestimmungen abzusenken.

In der 1. Lesung des Gesetzentwurfs, den die SPD-Landtagsfraktion im Juni 1995 zur Änderung eingebracht hatte, wurde durch Abgeordnete der beiden großen Landtagsfraktionen verdeutlicht, daß „die fortschreitende Integration und Verhältnisse in Europa eine neue Dimension polizeirechtlicher Zusammenarbeit erfordere". Wegen der „äußerst restriktiven Bedingungen" des Saarländischen Polizeigesetzes sei ein Informationsaus-

tausch mit internationalen Einrichtungen nicht möglich. Eine „Abmilderung der Restriktionen des Datenschutzes" sei nunmehr erforderlich.

Bedauerlicherweise entbehrte der Entwurf - im Gegensatz zu Regierungsentwürfen - einer schriftlichen Begründung, anhand derer die Stichhaltigkeit dieser Argumentation näher hätte beurteilt werden können. Bei diesem Verfahren bestand für den LfD auch erst während der Beratungen im Innenausschuß des Saarländischen Landtags die Möglichkeit, auf Bedenken hinzuweisen. Letztlich hat die Einmütigkeit unter den großen Fraktionen erwartungsgemäß zur Verabschiedung der Gesetzesänderung geführt, die im April 1996 in Kraft getreten ist.

Ich will gleichwohl knapp aus meiner Argumentation vor dem Ausschuß wiedergeben, in welchen Punkten die Datenschutzrechte der Bürgerinnen und Bürger des Landes im Kontakt mit der Polizei gemindert werden:

– Datenerhebungen, die die Vollzugspolizei im Vorfeld künftiger Straftaten - also ohne Bezug zur Verfolgung bereits begangener Taten und auch nicht zur Abwehr unmittelbar drohender Gefahren - über mögliche Täter, Kontaktpersonen oder Opfer vornimmt, dürfen nur unter engen Voraussetzungen zugelassen werden. Bislang sollte das Erfordernis „tatsächlicher" Anhaltspunkte Gewähr dafür bieten, daß Datenerhebungen nicht nur auf bloßen Spekulationen oder Vermutungen gründen. Die Streichung des Wortes „tatsächliche" (Anhaltspunkte) im neuen Gesetz legt schon vom Wortlaut her die Sorge nahe, daß der Boden der Tatsachen jetzt verlassen werden kann, wenn die Vollzugspolizei über nur potentiell Verdächtige, künftige Kontaktpersonen, künftige Opfer von Straftaten, künftige Zeugen, Hinweisgeber oder sonstige Auskunftspersonen Daten erhebt.

– Nach einer weiteren Änderung der einschlägigen Bestimmung muß sich die Vollzugspolizei, um die Erforderlichkeit der Datenerhebung darzutun, nicht mehr auf die Feststellung konkreter Tatsachen in der Gegenwart berufen. Es reicht nunmehr aus, daß Erfahrungen vorliegen, die anderswo oder in der Vergangenheit gewonnen wurden.

– Bei minder schwerwiegender Kriminalität, bei der der Einsatz sog. Verdeckter Ermittler nicht in Betracht kommt, diente die geänderte Rechtsgrundlage auch stets als Befugnisnorm für die nicht offen ermittelnde

Vollzugspolizei. Der betroffene Personenkreis erfährt nur durch Zufall von einer Datenerhebung durch die Polizei auf derart abgesenktem Niveau.

- Nicht nur bei der Erhebung, sondern auch bei der Speicherung personenbezogener Daten in Dateien wurde bei der Novelle ein „Nachbesserungsbedarf" gesehen. Nach der geänderten Rechtslage darf die Polizei aus Strafermittlungsverfahren Personen, gegen die ein Tatverdacht bestanden hat, ebenfalls nach abgeschwächten Kriterien in ihren Dateien speichern, sofern sie als Wiederholungstäter eingeschätzt werden.

Welche Gefahren aus „Verdachtsspeicherungen" erwachsen können, wird an Hand eines anschaulichen Falles eines Petenten im Folgenden dargestellt.

7.4 „Mords"-Verdacht

Ein Petent hatte sich bei der Bundeswehrverwaltung als Berufssoldat beworben. Im Rahmen des Bewerbungsverfahrens wurde ihm vorgeworfen, er hätte der Verwaltung Angaben über sich verheimlicht. Auf sein Bestreiten hin wurden ihm polizeiliche Vorgänge gezeigt, nach denen gegen ihn in der Vergangenheit wegen angeblicher Tötung eines Kindes ermittelt worden war. Durch die Vorhaltungen der Bundeswehrverwaltung hat der Petent von dieser Angelegenheit erstmals erfahren.

Die Überprüfung des Falles hat ergeben, daß das Verfahren mangels hinreichenden Verdachts einer Straftat von der Staatsanwaltschaft eingestellt worden war. Da es sich offensichtlich um Phantastereien eines 8-jährigen Kindes gehandelt hatte, war der Petent im Ermittlungsverfahren auch nicht angehört worden.

Letztlich ist vor diesem Hintergrund der Vorgang aus der Personalakte entfernt worden. Leider ließ sich nicht klären, welche öffentliche Stelle die unzulässige Datenübermittlung veranlaßt hatte.

Der Fall zeigt indes, welchen Unannehmlichkeiten der Betroffene ausgesetzt wird, wenn „Verdachtsfälle aus dem Nichts heraus" über Jahre hin-

weg bei öffentlichen Stellen - sei es in Akten oder in Dateien - gespeichert bleiben. In jeder Speicherung liegt auch die Gefahr einer unzulässigen Datenübermittlung oder einer unzulässigen Nutzung durch die speichernde Stelle.

Nach den gesetzlichen Bestimmungen des im Hinblick auf die Löschungsfristen unveränderten Polizeirechts hat jeder Verdachts- und prognostizierte Wiederholungsfall eines Erwachsenen unter 70 Jahren mit einer maximal 10-jährigen Speicherung zu rechnen. Die Aufbewahrungsfrist der Staatsanwaltschaft beträgt für eingestellte Verfahren 5 Jahre. Für die unterschiedlichen Fristen bei Polizei und Staatsanwaltschaft sehe ich angesichts des Resozialisierungsgedankens keine Rechtfertigung.

7.5 Weitere Speicherungsfälle

1. Fall

Speicherungen bei der saarländischen Polizei können jetzt unter denselben Voraussetzungen erfolgen wie nach Polizeirecht eines anderen Bundeslandes, aus dem mir eine Eingabe vorgelegt wurde.

Der Petent, ein Jurastudent, hat mir mitgeteilt, er beabsichtige, die Prüfungen zum ersten Staatsexamen abzulegen. An der Beseitigung jedweden Verdachts einer Straffälligkeit bestehe daher seinerseits ein erhebliches Interesse. In diesem Zusammenhang sei nicht einzusehen, daß er bei der Polizei eines anderen Bundeslandes wegen folgenden Vorfalls gespeichert sei:

Zusammen mit mehreren Personen habe er nachts eine Gaststätte verlassen, vor deren Eingang Blumenkästen gestanden hätten und eine Fahne an einem Seil befestigt gewesen sei. Als Angehöriger dieser Personengruppe wurde er wegen Verdachts des gemeinschaftlichen Diebstahls und der Sachbeschädigung festgenommen und erkennungsdienstlich behandelt. Nach Aussage der Polizeibeamten sei er sowohl an der Wegnahme der Fahne als auch an der Zerstörung des Seils beteiligt gewesen. Auch hinsichtlich der Beschädigung der Blumenkästen sei der Tatverdacht gegen ihn nicht ausgeräumt, da beim Passieren der Gaststät-

te ein dumpfer Lärm zu hören gewesen sei und eine Person aus seiner Gruppe einen Blumenstock in der Hand getragen habe. Von der Staatsanwaltschaft ist das Verfahren gegen ihn mangels Strafantrags eingestellt worden.

Die Polizei des anderen Bundeslandes hat die Speicherung auf 5 Jahre für gerechtfertigt gehalten, da der Tatverdacht (wegen des fehlenden strafgerichtlichen Verfahrens) nicht ausgeräumt werden konnte.

Da für den Wohnsitz des Petenten die saarländische Staatsanwaltschaft zuständig war und hier das Verfahren eingestellt wurde, konnte ich mich von der Richtigkeit seines Vortrags überzeugen.

Zwar wäre nach interner Regelung der saarländischen Polizei eine gleiche Verfahrensweise hier derzeit nicht anzunehmen. Nach dem Wortlaut des novellierten Polizeirechts hätte ich indes dem Petenten, ebenso wie der in der Sache zuständige Kollege des anderen Bundeslandes, bestätigen müssen, daß die Speicherung bei der Polizei nicht zu beanstanden gewesen wäre. Es ist insofern mehr als unbefriedigend, daß nur jederzeit leicht abänderbare untergesetzliche Verwaltungsvorschriften (Rahmenrichtlinie „Informationsverarbeitung") die weiteren gesetzlichen Speicherungsbefugnisse der Polizei einschränken.

2. Fall

Nach Inkrafttreten des Saarländischen Polizeigesetzes im Jahre 1990 hatte ich Verständnis dafür, daß alle noch auf der Grundlage des Preußischen Polizeiverwaltungsgesetzes gespeicherten Daten nicht schlagartig bereinigt werden konnten. Nicht verständlich erscheint mir jedoch die vom Landeskriminalamt vertretene Auffassung, bei Verfahren, deren Ausgang nicht bekannt sei, könnten Speicherungen weiterhin bestehen bleiben. Derartige Ungewißheiten dürfen nicht zu Lasten des Betroffenen gehen, in dessen informationelles Selbstbestimmungsrecht mit der Speicherung seiner personenbezogenen Daten bei der Polizei gravierend eingegriffen wird.

So wurde in einer Eingabe zu Recht moniert, daß in einem neuen Ermittlungsverfahren gegen den Petenten 17 frühere Einträge bei der Polizei

vermerkt waren, die längst hätten gelöscht sein müssen. Darunter befand sich auch ein als solcher nicht erkennbarer Freispruch, der als weiterbestehender Tatverdacht gespeichert war. Nach länger andauerndem kontroversem Schriftwechsel hat das LKA sich meiner Auffassung angeschlossen, daß im konkreten Fall nur nachvollziehbare Tatverdachtsfälle gespeichert werden dürfen.

Nach Darstellung der Staatsanwaltschaft, die ich hierzu befragt habe, wären für ihre Entscheidungen ohnehin nur die ihr bekannten Taten und Einträge beim Bundeszentralregister maßgeblich. Die Einführung der allein bei der Polizei vorhandenen Tatverdachtsspeicherungen in das aktuelle Verfahren war nach Auffassung der Staatsanwaltschaft somit gar nicht erforderlich. Welche Bedeutung solche Speicherungen überhaupt haben sollen, bleibt damit unklar.

7.6 Rahmenrichtlinie Informationsverarbeitung

Die vorhergehenden Ausführungen belegen, wie wichtig es ist, bei der Polizei angemessene Speicherfristen verbindlich festzulegen und die darauf folgende Löschung personenbezogener Daten vorzuschreiben.

Um so bedauerlicher ist die Tatsache, daß die in der novellierten Fassung vorgelegte „Rahmenrichtlinie Informationsverarbeitung" zwar ebenso wie die vorhergehende Richtlinie die Voraussetzungen für Speicherungen eingehend dargelegt, für die Löschung der Daten aber keine Regelungen enthält.

Ich habe darum gebeten, die Richtlinie dahingehend zu ergänzen.

7.7 Neufassung der landesspezifischen ED-Richtlinien

Zu den Richtlinien über die erkennungsdienstliche Behandlung, zu der nach dem Polizei- und Strafverfahrensrecht schwerwiegende Eingriffe wie Abnahme von Finger- und Handflächenabdrucken, die Aufnahme von Lichtbildern, die Feststellung äußerer körperlicher Merkmale und Mes-

sungen zählen, hatte ich bereits Anfang des Jahres 1995 umfassend Stellung genommen.

Ich hatte das Ministerium des Innern darum gebeten, den Entwurf nach meinen Anregungen zu bereinigen und mir ein Exemplar der endgültigen Fassung der ED-Richtlinien zu übersenden. Der Bitte ist bislang nicht entsprochen worden.

7.8 Verwaltungsvorschrift zur Blutalkohol- und Drogenfeststellung

Bei der Blutalkohol- und Drogenfeststellung erhält nach derzeitiger Praxis das hiermit befaßte Personal der Untersuchungsstelle nähere Kenntnis von höchst sensiblen persönlichen Lebensumständen des Betroffenen, weil das Material mit Namensangabe angeliefert wird. Nach dem heutigen Stand der Technik ist aber durchaus möglich, Anonymisierungsverfahren anzuwenden, bevor das Material mit personenbezogenen Daten an sachverständige Stellen zur Untersuchung übermittelt wird. Für die Durchführung des Untersuchungsauftrags werden die persönlichen Daten nicht benötigt.

Zum Entwurf einer bundeseinheitlichen Verwaltungsvorschrift über die Feststellung von Alkohol im Blut bei Straftaten und Ordnungswidrigkeiten und über die Sicherstellung und Beschlagnahme von Fahrausweisen habe ich in Übereinstimmung mit Datenschutzbeauftragten aus anderen Bundesländern darum gebeten, diese bislang noch nicht praktizierte Anonymisierung verbindlich vorzuschreiben. Die Übersendung einer Ausfertigung des Blutentnahmeprotokolls an die Untersuchungsstelle muß wegen der darin enthaltenen detaillierten Angaben zur Person und deren Lebensweise unterbleiben.

Außerdem habe ich darum gebeten, die Aufbewahrungsfrist von 10 Jahren zu halbieren. Ich vertrete auch die Auffassung, daß angesichts des geringen Unrechtsgehaltes von Ordnungswidrigkeiten anderen Personen als Beschuldigten oder Opfern ohne ihre Einwilligung eine Blutentnahme oder körperliche Untersuchung in Ordnungswidrigkeitenverfahren grundsätzlich nicht zumutbar ist.

Bisher wurde ich nicht darüber informiert, ob Anonymisierungsverfahren zwischenzeitlich zur Anwendung kommen und meine weiteren Anregungen berücksichtigt wurden.

7.9 Überprüfung der Erforderlichkeit polizeilicher Befugnisse; Rechtstatsachensammelstelle des BKA

Die Errichtung einer Rechtstatsachensammelstelle beim Bundeskriminalamt hatten die Datenschutzbeauftragten des Bundes und der Länder bereits im Jahre 1995 (Anlage 8) begrüßt.

Diese soll insbesondere dazu dienen, die Wirksamkeit polizeilicher Ermittlungsbefugnisse und Ermittlungsmethoden zu überprüfen, die vor allem durch das Gesetz zur Organisierten Kriminalität (OrgKG) im Jahre 1992 normiert wurden. Durch dieses Gesetz haben die Rasterfahndung, der Einsatz technischer Mittel und der Einsatz verdeckter Ermittler gesetzliche Grundlagen gefunden. Von all diesen Maßnahmen sind auch Unverdächtige in besonderer Weise betroffen; gerade der Schutz ihrer Persönlichkeitsrechte verlangt, auch gesetzlich bestimmte Befugnisse daraufhin zu prüfen, ob sie erforderlich sind und angesichts der Schwere des Eingriffs weiterhin aufrechterhalten bleiben dürfen.

Wenn jedoch aus dem Saarland und, nach meinem Wissensstand, zumindest aus einem weiteren Bundesland bis Anfang des Jahres 1996 keine Fälle an die Rechtstatsachensammelstelle gemeldet wurden, läßt dies Zweifel an der Erforderlichkeit der im Jahre 1992 neu normierten Instrumente aufkommen, die einer kritischen Analyse durch neutrale Experten bedürfen. Bleiben Meldungen von Fällen an die Rechtstatsachensammelstelle aus, ist auch in Frage zu stellen, ob das hierfür erstellte Themenraster geeignet ist.

7.10 Kontrolle der Akten über den Einsatz von Vertrauenspersonen und Verdeckten Ermittlern

Verdeckte Ermittlungsmethoden der Polizei, von denen der Betroffene in der Regel wegen ihres heimlichen Charakters nichts erfährt und deshalb

auch kaum Rechtsschutzvorkehrungen treffen kann, bedürfen einer verstärkten Kontrolle durch die Datenschutzbeauftragten des Bundes und der Länder.

Um so bedauerlicher war, daß ich bei einer beabsichtigten Prüfung hieran massiv behindert worden bin. Die Staatsanwaltschaft hatte nämlich die Polizei des Landes angewiesen, dem Landesbeauftragten für Datenschutz und seinen Mitarbeitern wegen des angeblich vertraulichen Charakters der zu Vertrauenspersonen und Verdeckten Ermittlern geführten Akten keinen Zugang zu den zu überprüfenden Vorgängen zu gewähren.

Man hat hier den bekannten und daher wenig originellen Ansatz gewählt, das Erfordernis besonderer Geheimhaltung gegen Stellen wie den LfD zu wenden, die - ebenso wie die datenverarbeitende Stelle - gerade zur Gewährleistung dieses Erfordernisses berufen sind.

Ich habe das Mißverständnis zu entkräften versucht, daß es sich bei meiner Prüfung um die zweckändernde Weitergabe von Daten handele, und darauf aufmerksam gemacht, daß der Gesetzgeber die Kontrolle personenbezogener Daten eben nicht als eine Datenverarbeitung zu anderen Zwecken erachtet (§ 13 Abs. 3 SDSG). Auch zwangsweise ist nicht mit einer Offenbarung der bei dieser Kontrolle gewonnenen Kenntnisse zu befürchten, denn dem LfD und seinen Bediensteten steht - im Gegensatz zu den Bediensteten der öffentlichen Stellen - ein Zeugnisverweigerungsrecht zu (§ 23 Abs. 4 SDSG i.V.m. § 12 Abs. 3 BDSG).

Es bedurfte der Einschaltung der obersten Landesbehörden, die dann - ebenfalls nicht in absolutem Einklang mit der Rechtslage - den Versuch unternommen haben, die Kontrollabläufe theoretisch festzulegen. Dieser Versuch stand vor allem im Widerspruch zu § 26 Abs. 2 SDSG, wonach zwar die Kontrolle auf die Person des LfD beschränkt werden darf; dann müssen personenbezogene Daten eines Betroffenen, dem von der datenverarbeitenden Stelle Vertraulichkeit besonders zugesichert worden ist, auch ihm gegenüber nicht offenbart werden. Das Gesetz bindet diese Einschränkung jedoch lediglich an einen Einzelfall, in dem die Sicherheit des Bundes oder eines Landes dies gebietet. Ein derartiger Einzelfall wurde nicht präsentiert, der Zugang wurde vielmehr generell verwehrt.

Die Staatsanwaltschaft hat in der Folge, nach Rücksprache mit dem Ministerium der Justiz, ihre Auffassung revidiert. Das Ministerium des Innern hat sich dagegen auch nach längerem Schriftwechsel nicht in der Lage gesehen, eine praktikable und gleichzeitig mit dem Gesetz in Einklang stehende Verfahrensweise vorzuschlagen.

Für die Zukunft erwarte ich, daß die Wahrnehmung meiner Befugnisse bei Kontrollen vor Ort dem Gesetz entsprechend gewährleistet wird.

8 Verfassungsschutz

8.1 Sicherheitsüberprüfung und Widerspruchsrecht des Betroffenen

Mit dem Landesamt für Verfassungsschutz (LfV) wurde die Diskussion um datenschutzrechtliche Fragen, die bereits im 15. TB (S. 53 ff) dargestellt wurden, fortgeführt. Es ging hierbei insbesondere um die Kontrolle der Sicherheitsüberprüfungsakten; die Frage war auch Gegenstand einer Sitzung des Landtagsausschusses für Datenschutz. Bedauerlicherweise ist in diesem Zusammenhang festzustellen, daß im Saarland - anders als für den Bereich des Bundes und verschiedener anderer Länder - das Verfahren der Sicherheitüberprüfung bislang immer noch nicht auf eine gesetzliche Grundlage gestellt wurde. Kontroverse Standpunkte, die auch in der Unterredung mit dem LfV nicht bereinigt werden konnten, hätten in einem Sicherheitsüberprüfungsgesetz eine klarstellende Lösung finden können.

Auf der Grundlage der gegenwärtigen gesetzlichen Bestimmungen ist nach meiner Auffassung vor allem die Frage, ob Referenz- und Auskunftspersonen grundsätzlich Vertraulichkeitsschutz gegenüber dem LfD zukommt, zu verneinen; dieser käme in der Wirkung dem normierten Widerspruchsrecht gleich, das im Bundesdatenschutzgesetz für einige wenige Fälle vorgesehen ist (§ 24 Abs. 2 i.V.m. Abs. 6). Zu den Personen, die einer Kontrolle der auf sie bezogenen Daten im Einzelfall gegenüber dem LfD widersprechen können, zählt auch derjenige, über den eine Personalakte oder eine Sicherheitsüberprüfungsakte geführt wird.

Der Ausschluß der Datenschutzkontrolle durch Erklärung des Betroffenen selbst ist nachvollziehbar, geht es doch insoweit primär um die Gewähr-

leistung der Persönlichkeitsrechte eben dieses Betroffenen. Würde man dagegen allen in Personalakten oder Sicherheitsüberprüfungsakten aufgeführten (anderen) Personen ein Widerspruchsrecht zugestehen, so würde der Kreis der Widerspruchsberechtigten in das Uferlose ausgedehnt und das gesetzliche Ziel verfehlt. Es widerspräche völlig der besonderen Schutzfunktion der Datenschutzkontrolle, in diesem sensiblen Bereich korrekte Datenverarbeitung zu gewährleisten, wenn der Vertrauliehkeitssschutz - als ein Aspekt des Datenschutzes - gegen die Personen gewendet würde, die seine Einhaltung sichern sollen, also die Datenschutzbeauftragten. Eine Ausweitung der Widerspruchsrechte auf andere Personenkreise als die im BDSG aufgeführten ist deshalb nicht zu befürworten.

8.2 Dienstvorschrift für die Durchführung des Gesetzes zu Art. 10 GG

Im Berichtszeitraum hat das Landesamt für Verfassungsschutz zahlreiche Dienstanweisungen im Entwurf zur Stellungnahme vorgelegt.

Datenschutzrechtlich von herausgehobener Bedeutung war dabei der Entwurf einer Dienstvorschrift für die Durchführung des Gesetzes zu Art. 10 Grundgesetz (G 10), das bei Überwachungsmaßnahmen besonders schwerwiegende Eingriffe in das Recht auf informationelle Selbstbestimmung zuläßt. Nach Maßgabe dieses Gesetzes wird das Brief-, Post- und Fernmeldegeheimnis beschränkt. Es gehört zu den Aufgaben des Landesamtes für Verfassungsschutz, solche Beschränkungsmaßnahmen mit nachrichtendienstlichen Mitteln durchzuführen. Nachrichtendienstliche Mittel dienen der heimlichen Informationsbeschaffung. Während der Beobachtung erfährt der mit verdeckten Methoden Beobachtete in der Regel nicht, daß er beobachtet wird. Er hat von daher auch keine tatsächliche Möglichkeit, die Rechtmäßigkeit der gegen ihn gerichteten Maßnahme gerichtlich oder außergerichtlich überprüfen zu lassen. Um so wichtiger ist es, daß bei diesen tief in das Persönlichkeitsrecht des Einzelnen eingreifenden Maßnahmen staatlicher Stellen der Staat selbst durch unabhängige Kontrollorgane für eine Überprüfung sorgt.

Als Ausgleich für die Heimlichkeit der angewandten Methoden bei diesen Grundrechtseingriffen hat das Bundesverfassungsgericht (BVerfGE 67,

157; NJW 1985, 121) eine Kontrolle verlangt, die in der materiellen und verfahrensmäßigen Überprüfung der gerichtlichen Kontrolle gleichwertig ist; es hat dabei die Kontrolle durch die G 10-Kommission und diejenige durch die Datenschutzbeauftragten als gleichberechtigt nebeneinander gestellt. Dieser Rechtsprechung wird der Entwurf der Dienstanweisung zum G 10 nicht gerecht, wenn dort unter Nr. 7 konstatiert wird, die Kontrolle personenbezogener Daten unterliege nach dem G 10 und dem Saarländischen Durchführungsgesetz zu diesem Gesetz ausschließlich der G 10-Kommission.

Zwar ist richtig, daß nach § 24 Abs. 2 und Abs. 6 BDSG die Kontrolle durch den Datenschutzbeauftragten insoweit ausgeschlossen ist, als sie der G 10-Kommission zugewiesen ist und diese nicht um Mitwirkung des LfD ersucht. Wegen der gesetzlich begrenzten Aufgabenstellung der G 10-Kommission führt dies jedoch nicht zur gebotenen umfassenden Kontrolle, sondern läßt wesentliche Teilbereiche aus, die nach meiner Auffassung der LfD mit seiner Kontrollkompetenz auszufüllen hat. Während sich die G 10-Kommission im wesentlichen nur mit der Zulässigkeit und Notwendigkeit von Beschränkungsmaßnahmen, wie etwa dem Verzicht auf eine Mitteilung an den Betroffenen, befaßt und insofern auch eine Datenschutzprüfung vornimmt, bleibt gerade die konkrete Durchführung der Beschränkungsmaßnahmen durch das LfV weitgehend unkontrolliert. Dies ist in diesem sehr sensiblen Bereich nicht vertretbar.

Die noch notwendigen Kontrollen umfassen beispielsweise die Auswertung, Speicherung und Übermittlung personenbezogener Daten durch das LfV (soweit darüber nicht die Kommission entschieden hat), die Verarbeitung und Nutzung personenbezogener Daten im Vorfeld und zur Vorbereitung von Überwachungsmaßnahmen, die technischen und organisatorischen Maßnahmen sowie die Einhaltung der Vorschriften zugunsten von Personen, über die Daten verarbeitet werden, die nicht Betroffene von Überwachungsmaßnahmen sind und daher durch das G 10 nicht geschützt werden.

Meine Anfrage an das Ministerium des Innern, wer (wenn nicht der Landesbeauftragte für Datenschutz) diese Datenverarbeitungen vor Ort kontrolliert, ist bislang unbeantwortet geblieben.

8.3 Dateienverarbeitung in Prüffällen

Im 15. TB (TZ 5.1.4) wurde bereits moniert, daß das LfV personenbezogene Daten in Dateien speichert, obwohl die erforderliche Festlegung als Beobachtungsobjekt, die der Zustimmung des Ministeriums des Innern bedarf, (noch) nicht erfolgt ist (sogen. Prüffälle). Hieran ist auch nach der anschließenden Erörterung mit den Vertretern des LfV festzuhalten; entgegenstehende Festlegungen in Dienstanweisungen sind zu ändern.

Die Dateiverarbeitung widerspricht dem eindeutigen Wortlaut des § 10 Abs. 1 Saarländisches Verfassungsschutzgesetz (SVerfSchG). Mit Recht wird diese Verarbeitungsform als potentiell belastender angesehen und deswegen an strengere Voraussetzungen gebunden als die Verarbeitung in Akten, die weniger leicht systematisch ausgewertet werden können. Eine Datenverarbeitung in Dateien setzt die Festlegung als Beobachtungsobjekt voraus; diese hat ihrerseits für die personenbezogene Datenspeicherung in Dateien zur Voraussetzung, daß tatsächliche Anhaltspunkte für den Verdacht einer nachdrücklichen Unterstützung eines verfassungsfeindlichen Personenzusammenschlusses gegeben sind (§ 5 Abs. 1 Satz 2 i.V.m. § 7 Abs. 2 SVerfSchG). Auch in anderen Bundesländern ist die Verarbeitung personenbezogener Daten in Dateien erst zulässig, wenn sich tatsächliche Anhaltspunkte für verfassungsfeindliche Bestrebungen ergeben haben (vgl. Hessisches Gesetz über das Landesamt für Verfassungsschutz, § 6 Abs. 4).

In Prüffällen sind diese gesetzlichen Vorgaben gerade nicht erfüllt; ihr Vorliegen wird erst überprüft. Eine „Korrektur" der gesetzlichen Entscheidung kann das LfV auch nicht mit der Argumentation vornehmen, daß es selbst in diesen Prüffällen mit Zustimmung des Ministeriums des Innern nachrichtendienstliche Mittel einsetzen, also ganz gravierende Eingriffe in die informationelle Selbstbestimmung vornehmen dürfe. Es macht vielmehr Sinn und ist keineswegs ein gesetzgeberisches Versehen, bei der Art der Datenverarbeitung zu differenzieren. Wenn sowohl im Prüffall als auch nach Festlegung eines Beobachtungsobjektes mit nachrichtendienstlichen Mitteln gearbeitet wird und zugleich eine Verarbeitung personenbezogener Daten in Dateien stattfindet, gäbe es für den Prüffall im Vergleich zum „normalen" Beobachtungsfall keinerlei Abstufung hinsichtlich der Eingriffsintensität der Beobachtungstätigkeit des LfV.

Entgegenstehende Anweisungen sind im Interesse des Persönlichkeitsschutzes erst zu überprüfender Personen nicht hinnehmbar. Soweit die vorgelegten Dienstanweisungen die Verfahrensweise in Prüffällen mit der Verfahrensweise für ein festgelegtes Beobachtungsobjekt gleichsetzen, ist eine Bereinigung unumgänglich.

8.4 Allgemeines zu weiteren Dienstanweisungen des LfV

Grundsätzlich begrüße ich die Vorlage einer einheitlichen Dienstanweisung für alle Auswertungsbereiche (Links- und Rechtsextremismus) sowie das Führen einer auf dem aktuellen Stand gehaltenen Liste der Beobachtungsobjekte.

In den Entwürfen, die mir vorgelegt wurden, habe ich allerdings folgende Aspekte noch nicht ausreichend berücksichtigt gesehen und deshalb um Modifikation gebeten:

- Das Ministerium des Innern ist als Aufsichtsbehörde über das LfV über die Auswertungsergebnisse des LfV grundsätzlich in nicht personenbezogener Weise zu unterrichten. Eine personenbezogene Unterrichtung wird nur im Falle des sogenannten „militanten Einzelkämpfers" erforderlich, der als Beobachtungsobjekt mit Zustimmung des Ministeriums des Innern festgelegt wurde (§ 5 Abs. 1 Satz 3 SVerfSchG).

- Verfassungsfeindliche Bestrebungen eines Personenzusammenschlusses können Einzelpersonen nur zugerechnet werden, wenn diese den Zusammenschluß „nachdrücklich unterstützen" (§ 5 Abs. 1 Satz 2 SVerfSchG). „Einfache" Mitgliedschaften in extremistischen Organisationen erfüllen nach Auffassung des LfD nicht ohne weiteres diese gesetzlichen Voraussetzungen. Auch sollte der Begriff der Anhängerschaft wegen seiner Unbestimmtheit keine Verwendung finden. Bei Unterstützern und Kontaktpersonen ist darauf zu achten, daß nur eine nachdrückliche Unterstützung zu einer Speicherung im Gegensatz zur Erhebung und Nutzung führen darf.

- Zur Wahrung des Zweckbindungsgebotes bei Daten, die aus einer Beschränkungsmaßnahme nach dem Gesetz zu Art. 10 GG herrühren, müssen konkrete Vorkehrungen zur Kennzeichnung der Daten getrof-

fen werden, um sie als Daten aus G 10-Maßnahmen erkennbar und kontrollierbar zu machen.

– Gegen Auswertungskurzvermerke bestehen auch in amtsinternen Arbeitsdateien Bedenken, wenn zur Beurteilung eines Sachverhalts nicht mehr die Akte herangezogen wird.

– Es sollten abgestufte Prüffristen für die Löschung von Daten festgelegt werden.

9 Kommunen

9.1 Ausländerbehörde der Landeshauptstadt Saarbrücken

Während des Berichtszeitraums wurde die Ausländerbehörde der Landeshauptstadt Saarbrücken überprüft.

Dabei wurden einige Mängel bei der Verarbeitung personenbezogener Daten von Ausländern festgestellt.

– Die in den Karteikarten enthaltenen Datenfelder waren im Umfang nicht auf die in §§ 3 und 4 der Ausländerdateienverordnung aufgeführten Datenfelder beschränkt. Sie enthielten darüber hinaus Angaben über
  a) Erwerbstätigkeit
  b) Daten von Ehegatten, die nicht Ausländer sind
  c) Daten von Kindern, die nicht Ausländer sind.

  Die Landeshauptstadt Saarbrücken hat zugesagt, die Begrenzungen durch die Ausländerdateienverordnung auf bestimmte Datensätze nach Einführung des automatisierten Verfahrens (LADIVA) zu beachten, mit dem das manuelle Verfahren noch im Laufe des Jahres 1995 ersetzt werden sollte. Bislang liegt jedoch keine Meldung über die Einführung des automatisierten Verfahrens vor.

– Die Ausländerbehörde hat zwei Ausländerdateien (A und B) zu führen, die sich nach der Ausländerdateienverordnung durch ihren Datenumfang unterscheiden.

Stirbt der Ausländer oder zieht er aus dem Bezirk der Ausländerbehörde fort, so sind seine Daten in der Datei A zu löschen und in die Datei B aufzunehmen. Während bei Fortzug alle Daten der Datei A in die Datei B übernommen werden können, dürfen bei Tod des Ausländers nur die Grunddaten in der Datei B weitergeführt werden. Insofern bedarf es ebenfalls der Bereinigung.

- Es wurden Karteikarten vorgefunden, an die weitere Belege angeheftet waren (z.B. Durchschrift der Meldebescheinigung des Einwohnermeldeamtes, AZR-Anfragen). Ich halte dies für unzulässig, da dadurch der Datenumfang der Ausländerdatei B in nicht vorgesehenem Umfang erweitert wird.

- Löschungen und Vernichtungen wurden nicht im erforderlichen Umfang nach Ablauf der 10-Jahresfrist vorgenommen. Es waren noch Daten Deutscher (Doppelstaater) vorhanden, für die ausländerrechtliche Zuständigkeiten nicht mehr gegeben waren.

- Der schwerwiegendste Mangel zeigte sich darin, daß die Ausländerbehörde über eine Online-Verbindung umfassend auf das Einwohnermelderegister zugreifen konnte, ohne daß für ihre Aufgaben solch weitreichende Kenntnisse notwendig sind. Abrufbar waren alle Daten sämtlicher Einwohner der Landeshauptstadt Saarbrücken, darunter sogar solche, die dem Steuergeheimnis unterliegen.

Die verbindliche Zusage der Stadt Saarbrücken, daß auch insofern Abhilfe geschaffen werde, steht noch aus.

9.2 Prüfung einer Stadtverwaltung

Aufgrund der Querschnittsprüfung einer Stadtverwaltung mußte ich in verschiedenen Bereichen datenschutzrechtliche Defizite feststellen, die dringend einer Abhilfe bedürfen. Mit der folgenden Darstellung geht es mir nicht darum, die betroffene Gemeinde an den Pranger zu stellen, sondern modellhaft darzustellen, welche Probleme bestehen, zumal ich davon ausgehen muß, daß bei vielen anderen Gemeindeverwaltungen eine ähnliche Situation anzutreffen ist. Es erscheint notwendig, daß auch die

Kommunalaufsicht verstärkt darauf achtet, daß die gesetzlichen Verpflichtungen eingehalten werden.

Eine Prüfung der verschiedenen Ämter in der Stadtverwaltung vor Ort und der beim LfD vorliegenden Meldungen zum Dateienregister ergaben folgende wesentlichen datenschutzrechtlichen Mängel:

- eine Risikoanalyse des IT-Einsatzes und ein darauf aufbauendes Sicherheitskonzept waren nicht vorhanden,

- eine Dienstanweisung zur Regelung der Informationsverarbeitung und zum Telefaxbetrieb war nicht in Kraft,

- nur ein Teil der laufenden Verfahren mit Verarbeitung personenbezogener Daten war zur Aufnahme ins Dateienregister gemeldet; teilweise waren Meldungen nicht auf dem aktuellen Stand,

- die eingesetzten Verfahren waren nicht freigegeben und die gesetzlich vorgeschriebene Beteiligung des LfD vor der Freigabe war ebenfalls versäumt worden,

- das Geräteverzeichnis war nicht vollständig und entsprach nicht den gesetzlichen Anforderungen,

- die nach § 11 SDSG zu treffenden, technischen und organisatorischen Maßnahmen waren nur zum Teil umgesetzt,

- die Zuständigkeiten waren formal nicht vollständig geklärt,

- eine Funktionstrennung zwischen der Systemtechnik und der Anwendung von Verfahren war nicht sichergestellt,

- vorhandene Zugriffssicherungen über individuelle Benutzerkennungen und individuelle Paßworte wurden teilweise nicht genutzt,

- Bearbeiter konnten in einzelnen Bereichen auf den gesamten Datenbestand zugreifen, obwohl dieser Umfang für ihre Arbeit nicht erforderlich war,

- die Dokumentation der Verfahren war unvollständig; wegen nicht ausreichender Protokollierung konnte teilweise eine Eingabekontrolle nicht vorgenommen werden,

- die Sicherung der Programme und Daten war nicht vollständig geregelt,

- eine Notfall und Katastrophenplanung war nicht vorhanden,

- Verträge mit externen Dienstleistern waren nicht datenschutzgerecht gestaltet; in der Regel basierten sie auf firmenspezifischen Vertragsmustern,

- Daten wurden teilweise doppelt (manuell und automatisiert) geführt,

- die private Nutzung von Geräten und Programmen war nicht verboten,

- für Eigenentwicklungen in den Abteilungen gab es keinen Auftrag und vor allem kein geregeltes Freigabeverfahren,

- Löschungsfristen waren teilweise nicht eingehalten oder nicht festgelegt.

Allerdings hatte der Bürgermeister schon vor Ankündigung meiner Prüftätigkeit damit begonnen, den IT-Bereich neu zu ordnen und einen Datenschutzbeauftragten bestellt, der auch schon tätig geworden war. Im Zusammenhang mit der anstehenden Neubeschaffung der Informationstechnik, einschließlich der Telekommunikationsanlage, tagte eine Arbeitsgruppe.

Der Bürgermeister nahm die von mir vorgelegten Prüfungsergebnisse, Vorschläge und Arbeitshilfen auf, um bei der anstehenden Neuorganisation nicht nur die technische Abwicklung der IT-Verfahren reibungslos umsetzen zu können, sondern auch dem Datenschutz im gesetzlich geforderten Umfange zu entsprechen (siehe auch TZ 4.14).

10 Meldewesen

10.1 Novelle Meldegesetz

Das geänderte Melderechtsrahmengesetz des Bundes hatte 1994 die Länder u. a. dazu verpflichtet, in ihren Meldegesetzen dem informationellen Selbstbestimmungsrecht stärker als bisher Rechnung zu tragen. Der Saarländische Gesetzgeber ist dem Anpassungsauftrag im Berichtszeitraum nachgekommen und hat im Jahre 1996 das novellierte Meldegesetz (MG) verabschiedet; bei der Vorbereitung war ich beteiligt (15.TB TZ 7.1).

Von größerer Bedeutung war in der Folgezeit die Bestimmung über Melderegisterauskünfte in besonderen Fällen (§ 35), die im novellierten Meldegesetz nunmehr für alle dort geregelten Fälle ein Widerspruchsrecht der Betroffenen vorsieht. Es werden dort drei Fälle von Datenübermittlungen an private Stellen geregelt:

- durch Absatz 1 erhält die Meldebehörde die Befugnis, an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen im Zusammenhang mit allgemeinen Wahlen, Auskunft aus dem Melderegister zu bestimmten Gruppen von Wahlberechtigten zu erteilen.

- Absatz 2 erlaubt eine Melderegisterauskunft an private Stellen über Alters- oder Ehejubiläen von Einwohnern.

- Absatz 3 ermächtigt zur Weitergabe der Adreßdaten an Adreßbuchverlage. Auf dieser Grundlage sind einem Verlag Daten übermittelt worden, der zwischenzeitlich ein Adreßbuch für die Landeshauptstadt Saarbrücken herausgeben hat; die Absicht hierzu hatte im Sommer 1996 ein großes, wenn auch nicht überwiegend positives, Medienecho hervorgerufen. Die Landtagsfraktionen haben in Aussicht genommen, sich mit dieser Bestimmung erneut zu befassen.

10.2 Datenübermittlung an Adreßbuchverlage

Als die Absicht zur Herausgabe eines Adreßbuchs für Saarbrücken bekannt geworden war, forderten empörte Bürger von mir, die Weitergabe

ihrer Daten durch die Meldebehörde zu unterbinden. Viele wollten gewährleistet wissen, daß die Meldedaten eben nur für öffentliche Zwecke genutzt und nicht an Private gegeben werden dürften. Auch reiche die - von vielen überlesene - amtliche Bekanntmachung der Landeshauptstadt mit dem Hinweis auf die Widerspruchsmöglichkeit nicht aus. Die Befürchtungen reichten von Belästigung durch unerwünschte Werbung bis zu gravierenden Sicherheitsbedenken.

Ich konnte der Forderung natürlich nicht entsprechen und mußte auf die gesetzliche Erlaubnis der Stadt verweisen, die Daten nach ihrem pflichtgemäßen Ermessen zu übermitteln. Ich habe allerdings eingefordert, daß insbesondere Vorkehrungen gegen die Gefahren getroffen werden, die bei Verfügbarkeit der Daten in elektronisch lesbarer und weiterverarbeitbarer Form drohen.

Von der Herausgabe einer CD-ROM, die dem Vernehmen nach zunächst ebenfalls geplant war, wurde - nicht zuletzt aufgrund eines Erlasses des Ministeriums des Innern - wieder Abstand genommen. Dieser Erlaß weist zu Recht darauf hin, daß das Melderecht nur eine Datenübermittlung an Adreßbuchverlage zulasse. Gegenüber der Buchform eröffneten dagegen Adressenverzeichnisse in automatisierter Form weitere Auswertungs- und Verknüpfungsmöglichkeiten; für diese Form bedürfte es hinsichtlich der Übermittlung von Meldedaten einer eigenen Rechtsgrundlage mit entsprechenden Schutzvorkehrungen.

Letztlich haben zwar über 6000 Einwohner der Landeshauptstadt einer Aufnahme ihrer Adresse in einem Adreßbuch widersprochen; die weitaus größte Zahl der Erwachsenen sind jedoch nach Name und Adresse verzeichnet .

Gegenüber dem Landtagsausschuß für Innere Verwaltung, der sich aufgrund der öffentlichen Diskussion mit der Problematik befaßt hat, habe ich mich in erster Linie dafür ausgesprochen, auf die bisher im Melderecht vorgesehene Datenübermittlung an Adreßbuchverlage künftig gänzlich zu verzichten. Denn für jeden gesetzlichen Eingriff in die Persönlichkeitsrechte ist erforderlich, daß er im „öffentlichen Interesse" erfolgt. Privates (meist wirtschaftliches) Interesse, das für die Herausgabe von Adreßbüchern spricht, kann kein öffentliches Interesse in dem Sinne begründen,

daß Daten einer öffentlichen Stelle für diese Zwecke nutzbar gemacht werden.

Da auch die gegenwärtig normierte Widerspruchslösung keine hinreichende Gewähr dafür gibt, daß Eingriffe in das Recht auf informationelle Selbstbestimmung unterbleiben, wäre die Datenübermittlung jedenfalls an eine ausdrückliche Zustimmung der Betroffenen zu binden.

Dem Vernehmen nach beabsichtigen alle Fraktionen des Saarländischen Landtags, das Melderecht in diesem Sinne zu ändern.

10.3 Datenübermittlung bei der Wahlvorbereitung

Die grundsätzliche Frage, ob Daten, die bei einer öffentlichen Stelle grundsätzlich für öffentliche Zwecke vorgehalten werden, ebenso privaten Stellen zur Verfügung stehen sollen, stellt sich auch für die Übermittlung von Name und Adresse der Wahlberechtigten an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen im Vorfeld einer Wahl. Hierfür gibt es, wie Eingaben zeigen, bei den Bürgern vielfach kein Verständnis.

Nicht genau bekannt sind auch oft die näheren Bedingungen, an die das Gesetz diese Befugnisse derzeit knüpft: Danach können den Parteien und Wählergruppen 6 Monate vor der Wahl - und ausschließlich für diesen Zweck - Name, Doktorgrad und Anschrift von einem Teil der Wahlberechtigten mitgeteilt werden; die ausgewählte Gruppe muß altersmäßig bestimmt sein. Üblich waren in der Vergangenheit Wahlanschreiben an „Jung"- oder „Erstwähler".

Im letzten Tätigkeitsbericht (15.TB TZ 7.1) hatte ich schon angeregt zu prüfen, ob nicht die Befugnis hierzu wegen anderer Möglichkeiten entfallen könnte, die diesen privaten Stellen in den modernen Medien auch für Wahlwerbezwecke zur Verfügung stehen. Denn sind die Daten bei den privaten Stellen einmal vorrätig, so ist nur eingeschränkt möglich, das Einhalten der Zweckbindung und die gesetzlich vorgeschriebene Löschung der Daten nach dem Bundesdatenschutzgesetz zu überprüfen (Anlaßkontrolle).

Leider hat sich bei einer saarländischen Meldebehörde erneut gezeigt, wie nachlässig mit Daten der Einwohner während eines Wahlkampfes umgegangen wird:

Einwohner der Gemeinde hatten sich darüber beschwert, daß sie unter ihrem Namen und ihrer Adresse von einer Partei bzw. einem Wahlbewerber angeschrieben worden waren, um eben den Kandidaten dieser Partei zu unterstützen. Daß die Daten aus dem Melderegister der Gemeinde entnommen worden waren, lag nahe.

Im konkreten Fall hatte ich u. a. deswegen Anlaß, die Zulässigkeit zu bezweifeln, weil Bürger ganz gezielt als EU-Bürger angeschrieben worden waren, die bei dieser Wahl erstmals das Stimmrecht erhalten hatten. Allein aufgrund einer Gruppenauskunft, die nach dem Lebensalter differenziert, hätte die Partei solch gezielte Anschreiben nicht fertigen können.

Die Gemeinde hat zunächst die Übermittlung von Daten der EU-Bürger bestritten und hieran auch auf Nachfragen festgehalten. Während eines ebenfalls anhängigen Wahlanfechtungsverfahrens hat die Gemeinde dann aber eingeräumt, die Daten seien auf Weisung eines Juristen der Gemeinde an die Parteien übermittelt worden.

Ich habe die Sache förmlich beanstandet. Am wenigsten nachvollziehbar erschien das Verhalten der Gemeindevertreter, die während der Prüfung und auch bei Gelegenheit zur schriftlichen Stellungnahme Recherchen unterlassen und damit gegenüber dem Landesbeauftragten für Datenschutz unwahre Angaben bewirkt hatten.

10.4 Daten über Alters- und Ehejubiläen an politische Parteien

Für Melderegisterauskünfte über Alters- und Ehejubiläen ergibt sich mit dem neuen Meldegesetz und der ebenfalls novellierten Meldedatenübermittlungsverordnung eine veränderte Rechtslage gegenüber dem früheren Rechtsstand, um dessen datenschutzrechtliche Bewertung mich eine Gemeinde gebeten hatte.

Die Weitergabe innerhalb der Gemeinde und die Übermittlung an andere Behörden oder sonstige öffentliche Stellen ist auf Ersuchen möglich, so-

weit die empfangende Stelle sie zur Vornahme von Ehrungen benötigt (§ 33 Abs. 2 MG).

Geändert hat sich die Rechtslage für regelmäßige Datenübermittlungen an andere öffentliche Stellen: Während nach der früheren Meldedatenübermittlungsverordnung diese Daten zu bestimmten Stichtagen an bestimmte Funktionsträger (Landrat, Stadtverbandspräsident, Minister des Innern, Chef der Staatskanzlei) übermittelt werden konnten, wird ein Bedürfnis hierfür offenbar nicht mehr gesehen. Eine regelmäßige Datenübermittlung kommt damit auch an eine öffentlichen Stelle nicht mehr in Betracht.

Melderegisterauskünfte über Alters- oder Ehejubiläen sind schließlich nach der Spezialbestimmung des § 35 Abs. 2 MG auch Privaten gegenüber zulässig. Dies gilt auch für Parteien, die offenbar gern Glückwünsche zu solchen Anlässen aussprechen, jedoch nicht-öffentliche Stellen im Sinne des Datenschutzrechts sind. Zur Auskunftsberechtigung wird aber in der Fachliteratur eine den Personenkreis einschränkende Auffassung vertreten: auch bei diesem gesetzlich normierten Sonderfall einer Gruppenauskunft an Private müsse wie bei jeder Gruppenauskunft ein öffentliches Interesse an der Auskunft erkennbar bleiben. Dies sei nur - wie in einzelnen Landesmeldegesetzen ausdrücklich normiert - für Abgeordnete oder sonstige Mandatsträger als Empfänger zu bejahen. Diese Auffassung teile ich.

Der Gemeinde, die eine Datenübermittlung über Alters- oder Ehejubiläen an Parteien auf der Grundlage einer - zu erfragenden - Einwilligung der Betroffenen in Erwägung gezogen hat, habe ich zu bedenken gegeben, ob es Aufgabe einer öffentlichen Stelle sein darf, Einwilligungen für Datenübermittlungen an private Stellen einzuholen, die der Gesetzgeber nicht derart umfassend vorgesehen hat.

10.5 Auskunft über Neubürger

Auch in einem weiteren Fall entsteht der Eindruck, die Meldebehörde betrachte die Melderegisterdaten als ihr Eigentum und könne dementsprechend frei darüber verfügen:

Eine Gemeinde hat sich für befugt gehalten, die Daten der Neubürger an ein Presseorgan zu liefern, das damit neue Geschäftsbeziehungen anbahnen konnte. Das Presseerzeugnis wurde zwar zunächst kostenlos geliefert und damit den Empfängern möglicherweise nicht lästig. Damit wurden aber Ansprechpartner für weitere (nicht kostenlose) Lieferungen gegenüber einer privaten Stelle offenbart, deren Interesse am Vertrieb ihres Produktes von rein wirtschaftlicher Art war.

Meine Intervention hat zur sofortigen Einstellung der Aktion geführt.

10.6 Auskunft der Meldebehörde an Nachlaßpfleger und Gläubiger

Nicht immer aber sind die Beschwerden begründet, mit denen sich Bürger wegen der Datenverarbeitung durch die Meldebehörde an mich wenden:

Ein Nachlaßpfleger hatte bemängelt, daß ihm die Meldebehörde Auskünfte über ehemalige Bewohner eines von ihm zu verwaltenden Hauses verweigert habe, die er im Zwangsversteigerungsverfahren jedoch benötige; in einem solchen Verfahren hat der Nachlaßpfleger die rechtliche Stellung des Eigentümers inne.

Ich habe den Nachlaßpfleger darauf hingewiesen, daß nach Melderecht der Wohnungsgeber (z.B. Eigentümer) oder sein Beauftragter auskunftspflichtig gegenüber der Meldebehörde ist, welche Personen bei ihm wohnen oder gewohnt haben (§ 20 MG). Die Meldebehörde ist hingegen nicht verpflichtet, den Wohnungsgeber darüber zu unterrichten, wer jemals in einem Hause gewohnt hat. Ich habe auch zu bedenken gegeben, daß das Melderegister aufgrund von Versäumnissen bei der An- und Abmeldung nicht den aktuellen Stand wiedergeben muß, so daß Daten Nichtbetroffener durch die Meldebehörde offenbart würden.

Die Meldebehörde hat deshalb die Auskunft zu Recht aus Datenschutzgründen verweigert. Es war zu begrüßen, daß sie die schutzwürdigen Belange aller möglichen ehemaligen Bewohner des Hauses zu wahren wußte.

In einem weiteren Fall war die Meldebehörde eindeutig in ihren Möglichkeiten überfordert:

So hat ein Petent sich darüber beschwert, daß aufgrund einer Namensverwechslung Zwangsvollstreckungsmaßnahmen gegen ihn getroffen würden.

Meine Überprüfung bei dem Gerichtsvollzieher, der als öffentliche Stelle meiner Kontrolle unterliegt, führten jedoch zu der Erkenntnis, daß dem Gerichtsvollzieher die Adresse mitgeteilt worden war, weil keine weitere gleichnamige Person in der Gemeinde wohnhaft war. Der Gläubiger war indes der Meinung, der Schuldner wolle sich durch den Hinweis auf eine Verwechslung lediglich seiner Verpflichtung entziehen, und hatte trotz des Hinweises durch den Gerichtsvollzieher gleichwohl beharrlich an seinem Vollstreckungsverlangen und an der Behauptung, es sei der richtige Schuldner, festgehalten.

Der Vorwurf an die Meldebehörde, daß diese überhaupt die Adreßauskunft gegeben hatte, war insofern unangebracht. Eine Klärung der Angelegenheit auf dem Rechtswege schien auch nach Auffassung des Petenten unvermeidbar, weil alle Identifizierungsmöglichkeiten der Meldebehörde ausgeschöpft waren.

11 Sonstige Bereiche der Innenverwaltung

11.1 Neues Personenstandsrecht in Vorbereitung

Nach Jahren des Stillstandes sind auf Bundesebene die Vorarbeiten zur Änderung des Personenstandsgesetzes wieder aufgenommen worden. Der Vorentwurf für ein 5. Personenstandsänderungsgesetz enthält im Vergleich zu dem jetzigen Recht deutliche Verbesserungen. Die grundsätzlichen, in der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 1988 vorgetragenen Forderungen wurden weitgehend berücksichtigt:

- Die Auskunfts- und Einsichtsrechte werden neu geregelt; die zur Zeit noch sehr restriktiven Bestimmungen, z. B. zugunsten der Familienforscher, gelockert.

- Für die Wissenschaft wird der Zugang zu den Personenstandsbüchern erleichtert.

- Die Mitteilungspflichten der Standesbeamten werden im Gesetz aufgenommen.

- Der Umfang der in die Personenstandsbücher einzutragenden Daten wird eingeschränkt; so entfällt z. B. die Berufsangabe.

Bei einer Reihe von Vorschriften müssen jedoch noch Präzisierungen vorgenommen werden. Vor allem bei den abschließend im Gesetz zu regelnden Mitteilungspflichten ist im Interesse der Normenklarheit konkret festzulegen, welche Stellen aus welchem Anlaß zu welchen Mitteilungen verpflichtet sind.

Ich habe das Ministerium des Innern gebeten, die Verbesserungsvorschläge bei den weiteren Beratungen auf Bundesebene zu unterstützen.

11.2 Durchführung der Wahlstatistik

Das verfassungsrechtlich geschützte Wahlgeheimnis bei der Stimmabgabe steht dem verständlichen Interesse vor allem der Parteien entgegen, näheren Aufschluß über unterschiedliches Verhalten der Wählergruppen zu erhalten. Neben - privaten - Befragungen durch Meinungsforschungsinstitute erlaubt in gewissem Umfang auch die staatliche Wahlstatistik Aussagen, indem sie innerhalb von Stimmbezirken eine Aufgliederung nach Geschlecht und Altersgruppen zuläßt. Voraussetzung ist natürlich, daß durch hinreichend große Gruppen und durch die Verfahrensgestaltung das Wahlgeheimnis immer noch ausreichend gewährleistet ist.

Hier gab es Anlaß zur Kritik am saarländischen Verfahren, die bereits im 15. TB (TZ 6) geäußert wurde. Im Berichtszeitraum haben sich die Datenschutzbeauftragten in allgemeinem Zusammenhang mit der Problematik befaßt und am 9./10.3.95 eine Entschließung verabschiedet, die als Anlage 9 abgedruckt ist.

Nach den dort genannten Anforderungen zählt das Saarland zu den wenigen Bundesländern, in denen eine Durchbrechung des Wahlgeheimnisses immer noch nicht hinreichend ausgeschlossen ist.

Zu bedenken wäre auch, ob wegen der mit Wahlstatistiken verbundenen Gefahren für das Wahlgeheimnis nicht gänzlich hierauf verzichtet werden sollte. Denn das Recht auf informationelle Selbstbestimmung, das zumindest in der gegenwärtigen Art der Durchführung gefährdet erscheint, darf auch aufgrund eines Gesetzes nur im überwiegenden Interesse der Allgemeinheit eingeschränkt werden (Art. 2 Satz 3 SVerf). In diesem Zusammenhang ist zu überprüfen, welchen Interessen die Durchführung der repräsentativen Wahlstatistik dient. Zu fragen ist, ob wirklich überwiegende Interessen der Allgemeinheit hierfür vorliegen.

12 Justiz

12.1 Justizmitteilungsgesetz

Das inzwischen mit einem konkreten Entwurf eingeleitete Gesetzgebungsverfahren des Bundes läßt hoffen, daß sich die endlos erscheinende Geschichte des Justizmitteilungsgesetzes dem Ende zuneigt.

In beträchtlichem Umfang werden personenbezogene Daten, die aus Straf- oder Zivilverfahren herrühren, nicht nur zur Durchführung oder Umsetzung dieser Verfahren an andere Stellen übermittelt, sondern deswegen, weil diese sie für ihre eigenen Aufgaben benötigen. Es findet also eine Zweckänderung statt; nach den Grundsätzen des Volkszählungsurteils muß der Betroffene über den Inhalt und den Adressaten der Mitteilung unterrichtet werden, denn nur so wird er in die Lage versetzt, seine Rechte gegenüber dieser anderen Stelle wahrzunehmen, in der seine personenbezogenen Daten unter einem anderen Aspekt weiterverarbeitet werden.

Hierfür bedarf es einer normenklaren gesetzlichen Regelung, die noch nicht besteht. Gegenwärtig erfolgen derartige Mitteilungen durch die Justiz vielmehr auf untergesetzlicher Grundlage, insbesondere der „Anordnung über Mitteilungen in Strafsachen (MiStra)" und der

„Anordnung über Mitteilungen in Zivilsachen (MiZi)". Daß aber - mehr als zehn Jahre nach Erlaß des Volkszählungsurteils - eine gesetzliche Basis immer noch nicht geschaffen werden konnte, wird mit beachtlichen Gründen bezweifelt. Die Datenschutzbeauftragten des Bundes und der Länder drängen seit 1984 mit Entschließungen auf entsprechende Normen.

Auch im Berichtszeitraum war ich mit verschiedenen Beispielsfällen befaßt, die den Regelungsbedarf deutlich machen. So etwa im nachfolgenden Fall, mit dem sich ein Petent an mich gewandt hat:

12.2 Strafbefehl an Ärztekammer

In einer Steuerstrafsache wurde gegen einen Arzt ein Strafbefehl erlassen. Der Arzt hat, nicht zuletzt auf Anraten seines Steuerberaters, den Strafbefehl nicht angefochten. Er wurde dann nach Nr. 26 der MiStra der Ärztekammer übersandt, damit diese über die eventuelle Einleitung eines standesgerichtlichen Verfahrens entscheiden kann.

Die Mitteilung erschien mir aus mehreren Gründen nicht zulässig:

- Schon vom Grundsatz her verneinen Teile der Rechtsprechung (z.B. VGH Kassel Urteil vom 22.6.95/GUE 152/92) die Weitergeltung des sogenannten Übergangsbonus für den Gesetzgeber, wonach die Verwaltung nur bis zur Schaffung der Rechtsgrundlagen berechtigt ist, das für die Aufrechterhaltung staatlicher Funktionen Unerläßliche zu veranlassen.

- Selbst die untergesetzliche Übermittlungsregelung der Nr. 2 Abs. 1 MiStra setzt in Steuerstrafsachen die Prüfung voraus, ob die Durchbrechung des Steuergeheimnisses nach § 30 Abgabenordnung zulässig wäre. Dort wird ein zwingendes öffentliches Interesse für die Offenbarung von Steuergeheimnissen verlangt, das insbesondere vor dem Hintergrund der Zweifel an der Weitergeltung des Übergangsbonus zu verneinen ist:

Beispielhaft werden in der Abgabenordnung erwähnt

a) Verbrechen und vorsätzliche schwere Vergehen gegen Leib und Leben oder gegen den Staat und seine Einrichtungen,
b) Wirtschaftsstraftaten, die nach ihrer Begehungsweise oder wegen des Umfangs des durch sie verursachten Schadens geeignet sind, die wirtschaftliche Ordnung erheblich zu stören oder das Vertrauen der Allgemeinheit auf die Redlichkeit des geschäftlichen Verkehrs oder auf die ordnungsgemäße Arbeit der Behörden und der öffentlichen Einrichtungen erheblich zu erschüttern.

Eine Gleichgewichtigkeit mit den aufgezählten Beispielen ließ sich im konkreten Fall jedoch nicht feststellen. Da auch ein Steuerberater eingeschaltet war, konnte weder eindeutig von der Täterschaft des Arztes noch von einer bestimmten Schuldform (Vorsatz oder Fahrlässigkeit) ausgegangen werden. Der Betroffene hat zudem die Einlegung eines Rechtsmittels gescheut, da die Klärung komplexer (steuer-)rechtlicher Fragen in einem Rechtsstreit voraussehbar erhebliche Kosten verursacht hätte.

– Als unerläßlich kann die Übermittlung personenbezogener Daten aus einem Strafbefehlsverfahren auch deswegen nicht angesehen werden, weil hierfür die Besonderheit dieses Verfahrens beachtet werden muß: wegen der beschleunigten Verfahrenserledigung liegt einem Strafbefehl nicht die volle richterliche Überzeugung zugrunde.

Im konkreten Fall ist nach Mitteilung der Ärztekammer des Saarlandes, der ich meine Auffassung dargelegt habe, das standesgerichtliche Verfahren wegen eines Verfahrenshindernisses eingestellt worden.

Wegen der über den Fall hinausreichenden Thematik habe ich das Ministerium der Justiz darum gebeten, sich im Gesetzgebungsverfahren dafür einzusetzen, daß Strafbefehle (wegen der ungewissen Erkenntnisgrundlagen) nur in Ausnahmefällen an andere Stellen übermittelt werden. Erkenntnisse aus Strafverfahren sind für den Betroffenen so belastend, daß die für bestimmte Fälle gesetzlich einzuräumende Anordnungskompetenz zur Mitteilung an andere Stellen dem Richter, Staatsanwalt oder dem Rechtspfleger vorbehalten sein sollte. Für schwierige Abwägungsentscheidungen im Spannungsverhältnis zwischen besonderen Berufs- und

Amtsgeheimnissen (Steuergeheimnis, ärztlicher Schweigepflicht, Sozialgeheimnis) und der Mitteilungspflicht gegenüber anderen Stellen sind auch verfahrensmäßige Vorkehrungen zum verfassungsrechtlich gebotenen Schutz der Persönlichkeitsrechte zu fordern.

12.3 Immunität der Abgeordneten; Mitteilungen über den Ausgang eines Verfahrens

Für Abgeordnete in gesetzgebenden Körperschaften gibt es zusätzliche Mitteilungen aus Strafverfahren, weil aufgrund ihrer Immunität Strafverfolgungs- oder Strafvollstreckungsmaßnahmen durch das Parlament genehmigungsbedürftig sind. Das Verfahren ist in Nr. 191 ff der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) geregelt; es sind verschiedene Informationen der Parlamente vorgesehen, die als Eingriffe in das Recht auf informationelle Selbstbestimmung anzusehen sind.

Eine ausdrückliche gesetzliche Norm, die den Vorgaben des Bundesverfassungsgerichtes entspricht, ist auch für diese Eingriffe nicht vorhanden. Die Datenübermittlung durch die Strafverfolgungsorgane an das Parlament ist indes, unabhängig von der Frage, ob die RiStBV (noch) als Rechtsgrundlage ausreichen, am Grundsatz der Erforderlichkeit zu messen.

Durch die Immunität der Abgeordneten soll die Arbeitsfähigkeit und Unabhängigkeit des Parlaments als solches gegen Einwirkungen einer anderen staatlichen Gewalt geschützt werden.

Für die Entscheidung des Parlaments, ob die Immunität aufgehoben werden soll, ist die Information über die beabsichtigte Einleitung eines Strafverfahrens in der Regel notwendige Voraussetzung. Das gleiche gilt, wenn eine genehmigungsbedürftige Strafverfolgungsmaßnahme oder die Einleitung der Strafvollstreckung beabsichtigt ist. Denn bei jeder Maßnahme, die erneut in die Rechte des Abgeordneten eingreift, ist wieder eine ausdrückliche Aufhebung der Immunität notwendig. Die für diesen Verfahrensschritt jeweils notwendige Information - und zwar die wirklich erforderliche - muß dem Parlament als Entscheidungsgrundlage übermittelt werden können.

Die Notwendigkeit einer Datenübermittlung durch die Strafverfolgungsorgane besteht aber nicht ohne weiteres auch für den weiteren Verfahrensgang; insbesondere für die Verfahrenserledigung bedarf es nur dann einer unaufgeforderten Mitteilung hiervon, wenn die Art der Erledigung für die weitere Tätigkeit des Parlaments bzw. des Abgeordneten von Bedeutung sein kann, nicht aber generell, wie es nach Nr. 192 Abs. 5 RiStBV vorgesehen ist.

Will das Parlament die Aufhebung der Immunität widerrufen, solange das Verfahren noch läuft, wird es eine solche Entscheidung nur fällen, wenn es besondere Umstände für gegeben hält. In diesem Fall ist es meines Erachtens dem Parlament zumutbar, von sich aus eine Auskunft über den Verfahrensstand einzuholen.

Die Immunität gilt jeweils nur für die laufende Legislaturperiode. Wenn der betroffene Abgeordnete auch dem nächsten Parlament angehört, muß das neue Parlament wiederum entscheiden. Die Initiative dazu kann von den Strafverfolgungsbehörden ausgehen (wie dies in der Praxis auch jetzt schon gehandhabt wird). Ist der Abgeordnete zwischenzeitlich aus dem Parlament ausgeschieden, erscheint mir allerdings nicht denkbar, daß dieses noch eine Information über die Erledigung benötigt.

Ich habe daher das Ministerium der Justiz gebeten, Gerichte und Staatsanwaltschaften auf die fehlende gesetzliche Grundlage und die mangelnde Erforderlichkeit einer Mitteilung über die abschließende Entscheidung hinzuweisen. Auch den Präsidenten des Saarländischen Landtags habe ich über meine Auffassung in Kenntnis gesetzt.

Das Ministerium der Justiz hat mir mitgeteilt, innerhalb der Justizministerkonferenz auf die Streichung der entsprechenden Bestimmung hinwirken zu wollen.

12.4 Übermittlung von Daten durch Ermittlungsbehörden an die Medien; Sitzungslisten an die Presse

Von zentraler Bedeutung für die Wahrung des Rechts auf informationelle Selbstbestimmung ist auch, ob und welche Informationen aus Strafverfahren an die Öffentlichkeit gelangen. Die Diskussion hierüber und auch zu

Informationen, die vor der öffentlichen Verhandlung an die Medien geleitet werden, ist aus vielen aktuellen Anlässen auch in anderen Bundesländern wieder aufgelebt und hat die Datenschutzbeauftragten des Bundes und der Länder zu zwei Entschließungen veranlaßt, die als Anlagen 10 und 11 abgedruckt sind.

Ich habe die Angelegenheit im Hinblick auf Sitzungslisten, die im Saarland vor öffentlicher Verhandlung in strafgerichtlichen Verfahren an die Presse gegeben werden, ebenfalls wieder aufgegriffen.

In Strafverfahren treten Grundsätze, die gerade zur Gewährleistung eines fairen und ordnungsmäßigen Verfahrens Öffentlichkeit fordern, sowie das Recht auf Pressefreiheit und Freiheit der Berichterstattung durch Rundfunk und Film (Art. 5 GG) in Widerstreit zu dem Recht auf informationelle Selbstbestimmung des Betroffenen und anderer Verfahrensbeteiligter.

Der Gesetzgeber, der den Ausgleich unter diesen Rechten vorzunehmen hat, verbietet im Strafgesetzbuch (§ 353 d) Mitteilungen über Strafverfahren unter bestimmten Voraussetzungen. Eine umfassende detaillierte Regelung gibt es allerdings nicht.

Das saarländische Ministerium der Justiz hat durch Allgemeine Verfügung „Informationserteilung an Presse und Rundfunk" vom 18.7.1986 Leitlinien gesetzt für einen Ausgleich zwischen den Persönlichkeitsrechten der von einem Verfahren Betroffenen und der freien Berichterstattung über ein Verfahren. Angesichts des Rechts auf ein faires Verfahren sowie des Grundsatzes der Unschuldsvermutung, die erst nach Verurteilung eines Angeklagten widerlegt ist, wurde in dieser Allgemeinen Verfügung unter Nr. 3.3 angeordnet, daß

> die Nennung der Namen von Verfahrensbeteiligten, insbesondere des Beschuldigten und des Opfers, ohne deren Zustimmung unterbleiben soll, soweit dies nicht im Interesse der Aufklärung von Straftaten geboten ist oder soweit es sich nicht um Personen aus dem Bereich der Zeitgeschichte im zeitgeschichtlichen Zusammenhang handelt. Die Nennung der Namen von Jugendlichen ist ohne ihre und ihrer gesetzlichen Vertreter Zustimmung untersagt. Die Namen der Opfer von Sexualstraftaten dürfen ohne deren Zustimmung nicht mitgeteilt werden.

Dasselbe gilt für Angaben, die die Identifizierung des Verfahrensbeteiligten nahelegen.

Hierzu steht die Praxis des Ministeriums der Justiz, wonach Sitzungslisten unter voller Namensnennung der Beschuldigten vor Durchführung der öffentlichen Verhandlung der Presse übermittelt werden, in eklatantem Widerspruch.

Die Mitteilung vor öffentlicher Verhandlung steht auch nicht in Einklang mit dem Prinzip der Gleichzeitigkeit von Anklage und Verteidigung in Strafverfahren.

Unter Bezugnahme auf die genannten Entschließungen der Datenschutzbeauftragten habe ich das Ministerium der Justiz um Stellungnahme zu dieser Verfahrensweise gebeten.

Sowohl das Schreiben meines Amtsvorgängers vom 6.10.1993 als auch meine Bitte um Stellungnahme, in der ich auf die genannten Entschliessungen verwiesen hatte, sind bisher ohne Antwort des Ministeriums der Justiz geblieben.

12.5 Bekanntgabe personenbezogener Daten aus Zivilverfahren

Auch in Zivilverfahren haben sich Petenten an mich gewandt, weil sie sich durch Mitteilungen der Justiz in ihren schutzwürdigen Belangen beeinträchtigt sahen.

1. Fall

So hat ein Petent, der zur Abgabe der eidesstattlichen Versicherung geladen war, kritisiert, daß alle zu diesem Termin geladenen Schuldner mit ausgeschriebenen Vor- und Zunamen in der Sitzungsrolle an der Tür des Sitzungssaales aufgeführt gewesen seien. Zufällig Vorübergehende, aber auch ebenfalls geladene Schuldner hätten auf diese Weise Kenntnis davon erhalten, gegen welche Schuldner ein Termin zur Abgabe der eidesstattlichen Versicherung anberaumt worden war.

Der Petent fühlte sich zu Recht durch diese Verfahrensweise beeinträchtigt, weil es keinen Grund gibt, Schuldner, die allem Anschein nach in Zahlungsschwierigkeiten geraten sind, allgemein zu offenbaren.

Auskünfte aus dem Schuldnerverzeichnis werden gemäß § 915 b Abs. 1 ZPO in Verbindung mit § 915 Abs. 2 ZPO nur zu den dort aufgeführten Zwecken erteilt, die vom Antragsteller darzulegen sind. Das Verfahren ist außerdem nicht öffentlich.

Hinzu kam, daß hier diese Offenbarung zu einem Zeitpunkt erfolgte, zu dem eine Aufnahme in das Schuldnerverzeichnis noch durch Begleichung der Forderung verhindert werden konnte. Und selbst nach Eintragung in das Schuldnerverzeichnis sind Abdrucke aus dem Schuldnerverzeichnis gemäß § 915 Abs. 2 ZPO vertraulich zu behandeln und dürfen Dritten nicht zugänglich gemacht werden.

Meine Bedenken habe ich dem Direktor des betreffenden Amtsgerichts mitgeteilt, der mir auch für den zuständigen Rechtspfleger zugesichert hat, daß in Zukunft - wie auch bereits in anderen Amtsgerichten - vom Anbringen der Terminsrolle im Verfahren zur Abgabe der eidesstattlichen Versicherung abgesehen werde.

2. Fall

Ein weiterer Fall betraf eine Erbschaftsangelegenheit, der folgender Sachverhalt zugrunde lag:

Der Vater des Petenten hatte in einem notariellen Testament einer Person ein Vermächtnis von mehreren Tausend DM zugewandt.

Unmittelbar nach dem Tode des Vaters hat der Petent eine Sterbeurkunde an das Nachlaßgericht gesandt und sich auf das Testament bezogen. Wenig später hat sein Bruder auf dem Wege der Nachlaßermittlung dem Nachlaßgericht mitgeteilt, die Vermächtnisnehmerin sei bereits verstorben; gleichzeitig hat er die Adresse der Tochter dieser Vermächtnisnehmerin angegeben, falls von seiten des Nachlaßgerichtes wegen des Todes der Mutter Nachfragen bestünden.

Kurz darauf erfuhren die Geschwister von der Tochter, daß sie vom Amtsgericht eine Fotokopie des eröffneten Testamentes bekommen habe. Die Frau bezeichnete sich darin als Erbin ihrer Mutter und wolle ihr Erbe antreten.

Der Petent hat ihr - der Rechtslage entsprechend - mitgeteilt, daß das ihrer Mutter zugedachte Vermächtnis mit dem Tode ihrer Mutter erloschen sei und nicht weiter vererbt werden könne.

Gegenüber meiner Dienststelle und dem zuständigen Amtsgericht hat der Petent aber sein Befremden darüber geäußert, daß die unbeteiligte Tochter der verstorbenen Vermächtnisnehmerin eine Kopie des Testamentes in vollem Wortlaut erhalten habe und dadurch über sämtliche letztwilligen Verfügungen des Vaters informiert worden sei.

Um solchen Gefährdungen für die Persönlichkeitsrechte Dritter vorzubeugen, habe ich dem Ministerium der Justiz den Erlaß einer Auslegungshilfe zu den einschlägigen Rechtsbestimmungen vorgeschlagen; diese sollte den einzelnen Rechtsanwendern ermöglichen, sich in der Materie des Erbrechts unter Berücksichtigung der Anforderungen des Datenschutzes schneller zu orientieren. In einer Allgemeinen Verfügung könnten der Begriff des Beteiligten in einer Erbschaftsangelegenheit definiert und die Fälle beispielhaft aufgeführt werden, in denen eine Mitteilung zur Wahrung der Persönlichkeitsrechte von Beteiligten nicht erforderlich erscheint.

Da mir keine abschließende Äußerung des Ministeriums der Justiz vorliegt, gehe ich davon aus, daß dem Vorschlag nicht entsprochen wurde.

3. Fall

Wenn die Geschäftsstellen eines Gerichts für Datenschutzbelange nicht hinreichend sensibilisiert sind, kann schon die bloße Art der Zustellungen Gefährdungen für die Persönlichkeitsrechte Beteiligter entstehen lassen.

In einem Schadensersatzprozeß über eine tätliche Auseinandersetzung war ein Zeuge zur schriftlichen Stellungnahme aufgefordert worden. Er hat zu Recht Beschwerde darüber geführt, daß anläßlich dieser Beweisaufnahme sein Recht auf informationelle Selbstbestimmung in vermeidba-

rer Weise gefährdet worden war. Außer dem Petenten waren nämlich zahlreiche weitere Zeugen ebenfalls zur Stellungnahme aufgefordert worden; der Auflagen- und Beweisbeschluß war jedem Zeugen unter Nennung des Namens und der Adresse aller weiteren Zeugen übersandt worden.

Da hier eine tätliche Auseinandersetzung im Streit stand, schien die Befürchtung des Zeugen nicht unbegründet, er könne Repressalien der Gegenseite, die seine vollständige Anschrift erhalten hatte, ausgesetzt sein. Zudem bestand die Gefahr, daß Absprachen zwischen den einzelnen Zeugen erfolgen könnten, da die Bekanntgabe der Adressaten eine leichte Kontaktaufnahme ermöglicht hätte.

Der Direktor des zuständigen Amtsgerichts hat mir versichert, daß es sich um ein Geschäftsstellenversehen gehandelt habe. Grundsätzlich werde jeder Zeuge individuell angeschrieben und über das Beweisthema informiert. Um den durch die Vielzahl der anzuschreibenden Zeugen bedingten Aufwand zu minimieren, habe man im konkreten Fall den Weg gewählt, Kopien des Beweisbeschlusses zu verschicken. Durch entsprechende Maßnahmen werde aber dafür Sorge getragen, daß sich solche Versehen nicht wiederholen.

12.6 Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich

Welch negative Auswirkungen Speicherungen personenbezogener Daten, die eine öffentliche Stelle nicht mehr benötigt, für das Recht auf informationelle Selbstbestimmung haben können, wurde schon für den Polizeibereich (TZ 7.4) dargestellt.

Speicherungen beinhalten Dauereingriffe in die Rechte der Betroffenen. Die Voraussetzungen für diese Eingriffe sind vom Gesetzgeber am verfassungsrechtlichen Erforderlichkeitsgrundsatz auszurichten und entsprechend festzulegen. Desgleichen ist das gesteigerte Gefahrenpotential, das durch Verarbeitung personenbezogener Daten in Dateien entsteht, durch den Gesetzgeber abzuschätzen und ebenfalls zu begrenzen.

Die lediglich in untergesetzlichen, wenn auch bundeseinheitlichen, Verwaltungsvorschriften festgelegten Aufbewahrungsfristen werden diesen Anforderungen nicht gerecht.

Die Datenschutzbeauftragten des Bundes und der Länder haben am 9./10.3.1995 in einer Entschließung (Anlage 12) zu dieser Thematik die wichtigsten Eckpunkte festgehalten, die der Gesetzgeber in eine entsprechende Regelung umsetzen sollte.

12.7 Korruptionsbekämpfungsgesetz

Auch im Verhältnis zur Öffentlichen Hand sind unlautere Geschäftspraktiken nicht ausgeschlossen; im Gegenteil werden immer wieder Fälle bekannt, in denen es bei Beschaffungen oder bei Auftragsvergabe zu Unregelmäßigkeiten bei den beteiligten Firmen wie bei den staatlichen Stellen kommt. Dies führt nicht nur zu Wettbewerbsverzerrungen innerhalb der Wirtschaft und zu überhöhten Kosten, die der Steuerzahler aufzubringen hat, sondern untergräbt auch das Vertrauen in die Zuverlässigkeit öffentlicher Verwaltung. Es ist deshalb sehr berechtigt, wenn geeignete Gegenmaßnahmen ergriffen werden.

Die Planungen für ein Korruptionsbekämpfungsgesetz haben die Datenschutzbeauftragten des Bundes und der Länder auf ihrer Konferenz am 9./10.11.95 zu einer Entschließung veranlaßt (Anlage 13). In der Entschließung werden Möglichkeiten aufgeführt, welche Effektivität versprechen und gleichwohl die Privatsphäre der unbeteiligten und unschuldigen Bürgerinnen und Bürger nicht antasten.

Um deutlich zu machen, daß auch seitens des Landes gezielt gegen Korruption vorgegangen werden soll, hat die Landesregierung eigene Aktivitäten in diesem Bereich angekündigt. Das Ministerium für Umwelt, Energie und Verkehr hat mir hierzu den Entwurf zu einem Gemeinsamen Erlaß der Landesregierung vorgelegt, nach dem Bewerber und Bieter wegen schwerer Verfehlungen, die ihre Zuverlässigkeit in Frage stellen, von der Auftragsvergabe ausgeschlossen werden sollen.

Obwohl ich großes Verständnis dafür habe, wenn staatliche Stellen über die bestehenden Sanktionsmöglichkeiten des Straf- und Wettbewerbs-

rechts hinaus verstärkt nach Möglichkeiten suchen, Korruption innerhalb und außerhalb des öffentlichen Dienstes zu vermeiden und einzudämmen, mußte ich dem konkreten Regelungsversuch aus Sicht des Datenschutzes Bedenken entgegensetzen.

Der Ausschluß von einer Vergabe eines Auftrags kann für den jeweiligen Bewerber und Bieter von existentieller Bedeutung sein. Sind die Auswirkungen einer Datenverarbeitung gravierend, so kann es nach der Rechtsprechung des Bundesverfassungsgerichtes nicht der Verwaltung überlassen bleiben, die Voraussetzungen für eine Zulassung im Wettbewerb festzulegen (Wesentlichkeitstheorie; Gesetzesvorbehalt). Es ist vielmehr Aufgabe des Gesetzgebers selbst, einen angemessenen Ausgleich zu schaffen zwischen den Interessen öffentlicher Stellen und den Interessen derjenigen, die sich um eine Auftragsvergabe bewerben.

Ich habe weiter konkrete Einzelforderungen erhoben, denen bei Festlegung des Verfahrens entsprochen werden müßte, um mit zulässiger und zuverlässiger Datenübermittlungen sowie der Speicherdauer übermäßige Beeinträchtigungen der Persönlichkeitsrechte auszuschließen.

Trotz meiner grundlegenden Bedenken, die sich vor allem gegen die Regelungsebene richteten, wurde die Veröffentlichung des Erlasses und seine Inkraftsetzung angekündigt.

12.8 Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich

Neue Technologien haben auch das Kommunikationsverhalten der Bürgerinnen und Bürger verändert. Auch ohne daß weitere Leistungsmerkmale dieser Techniken genutzt werden, bieten diese vielfach zusätzliche Möglichkeiten, Aufschluß über Art und Inhalt der Kontakte zu gewinnen. Die Sorge der Datenschutzbeauftragten gilt nunmehr der Aufrechterhaltung des von der Verfassung verbürgten Freiheitsraums, der durch teilweise bessere Kontrollierbarkeit der neuen Medien durch Strafverfolgungsorgane nicht eingeengt werden darf.

Auf der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22/23.10.1996 wurde dazu eine Entschließung gefaßt. Diese

richtet sich vor allem auch gegen ein generelles Verbot einer nicht kontrollierten Verschlüsselung, das aus Sicht der Datenschutzbeauftragten nicht durchsetzbar wäre (Anlage 14; vgl. auch TZ 4.4).

Die Übertragbarkeit des strafprozessualen Instrumentariums auf neue Technologien (z.B. Mailboxen) ist zu überprüfen. Soweit neue Regelungen zu schaffen sind, ist ihre Eingriffsintensität in die Persönlichkeitsrechte Betroffener gegenüber der bisherigen Rechtslage nicht zu verstärken.

12.9 Großer Lauschangriff

Um die Schwerstkriminalität intensiver als bisher verfolgen zu können, wird auf Bundesebene die Einführung von Eingriffsmöglichkeiten erörtert, die das geltende Verfassungsrecht ausschließt. Hierzu gehört die akustische Überwachung von Wohn- und Geschäftsräumen zur Beweismittelgewinnung im Strafverfahren (sogenannter Großer Lauschangriff). Der Entwurf zu einer Änderung des Artikels 13 Grundgesetz und einer dazugehörigen Anpassung des Straf- und Strafverfahrensrechts wird gegenwärtig innerhalb der Bundesregierung diskutiert.

Die danach möglichen Überwachungsmaßnahmen berühren den engsten Bereich privater Lebensgestaltung, der um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen dem Einzelnen verbleiben und staatlicher Ausforschung entzogen sein muß. Die Abwägung zwischen berechtigten Sicherheitsinteressen und Schutz der Persönlichkeitsrechte hatte die Datenschutzbeauftragten des Bundes und der Länder bereits 1992 veranlaßt, sich mit großer Mehrheit gegen jegliche Überwachung in Privatwohnungen zu Strafverfolgungszwecken zu wenden.

Der erneuten Initiative zur Ausgestaltung derartig gravierender Eingriffe stehen auch nach meiner Auffassung erhebliche verfassungsrechtliche Bedenken entgegen. Für den Fall, daß, trotz der grundsätzlichen Zweifel an Tauglichkeit und Angemessenheit solch tiefgreifender Beschränkungen, die innerhalb der Bundesregierung diskutierten Pläne weiterverfolgt werden, halte ich gemeinsam mit meinen Kollegen zum Schutz der Privatsphäre eine klare Begrenzung und verfahrensmäßige Sicherung der Maßnahme für zwingend erforderlich. Solche Beschränkungen und Siche-

rungen sollten vom Grundsatz her im Grundgesetz selbst und nicht erst im ausführenden Gesetz festgelegt sein.

1. Im Grundgesetz selbst ist festzulegen, daß der Einsatz technischer Mittel zur Wohnraumüberwachung nur zur Verfolgung schwerster Straftaten, die im Hinblick auf ihre Begehungsform oder Folgen die Rechtsordnung nachhaltig gefährden und die im Gesetz einzeln bestimmt sind und nur auf Anordnung eines Kollegialgerichts erfolgen darf.

2. Die Maßnahme darf sich nur gegen den Beschuldigten richten. Erfolgt ein Lauschangriff in der Wohnung eines Dritten, müssen konkrete Anhaltspunkte die Annahme rechtfertigen, daß sich der Beschuldigte in der Wohnung aufhält. In allen Fällen muß die durch Tatsachen begründete Erwartung vorliegen, daß in der überwachten Wohnung zur Strafverfolgung relevante Gespräche geführt werden.

3. Das Mittel der Wohnungsüberwachung darf nur angewandt werden, wenn andere Methoden zur Erforschung des Sachverhalts erschöpft oder untauglich sind. Bei einem Lauschangriff in Wohnungen dritter Personen bedeutet dies auch, daß die Maßnahme nur durchgeführt werden darf, wenn aufgrund bestimmter Tatsachen anzunehmen ist, daß ihre Durchführung in der Wohnung des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsorts des Täters führen wird.

4. Das Zeugnisverweigerungsrecht von Berufsgeheimnisträgern und Personen, die aus persönlichen Gründen zur Verweigerung des Zeugnisses berechtigt sind, muß gewahrt werden.

5. Die Dauer der Maßnahme wird zeitlich eng begrenzt. Auch die Möglichkeit der Verlängerung der Maßnahme ist zu befristen.

6. Eine anderweitige Verwendung der erhobenen Daten (Zweckänderung) ist weder zur Beweiszwecken noch als Ermittlungsansatz für andere als Katalogdaten zulässig.

Personenbezogene Erkenntnisse aus einem Lauschangriff dürfen zur Abwehr von konkreten Gefahren für gewichtige Rechtsgüter verwendet werden.

7. Wenn sich der ursprüngliche Verdacht nicht bestätigt, sind die durch den Lauschangriff erhobenen Daten unverzüglich zu löschen.

8. Die Betroffenen müssen unverzüglich und vollständig über die Durchführung der Maßnahme informiert werden, sobald dies ohne Gefährdung des Ermittlungsverfahrens möglich ist.

9. Eine Verfahrenssicherung durch den Zwang zur eingehenden Begründung und durch detaillierte jährliche Berichtspflichten der Staatsanwaltschaft für die Öffentlichkeit ähnlich den gerichtlichen Wire-Tape-Reports in den USA einschließlich einer Erfolgskontrolle ist vorzusehen. Anhand der Berichte ist jeweils - wegen der Schwere des Eingriffs - in entsprechenden Fristen zu überprüfen, ob die gesetzliche Regelung weiterhin erforderlich ist.

10. Die effektive Kontrolle der Abhörmaßnahme und der Verarbeitung und Nutzung der durch sie gewonnenen Erkenntnisse durch Gerichte und Datenschutzbeauftragte ist sicherzustellen.

Über diese notwendigen gesetzlichen Verfahrenssicherungen habe ich den Ministerpräsidenten und den Minister der Justiz unterrichtet.

Ein Gesetzgebungsvorhaben, das wie dieses grundgesetzliche Freiheitsverbürgungen bis in die Intimsphäre hinein weiter einengt, verlangt nach meiner Auffassung, daß die Abstimmung ohne Rücksichtnahme auf „Fraktionsdisziplin" allein der freien Mandatsausübung und Gewissensentscheidung aller Abgeordneten des Bundestages anheimgestellt bleiben muß (Art. 38 Abs. 1 Satz 2 GG).

13 Kataster/Bauwesen

13.1 Direktauskunft der Bewertungsstellen aus dem Liegenschaftskataster (DABLIKA)

Für die steuerliche Bewertung benötigen die Finanzämter zuverlässige Informationen, die im Zusammenhang mit den betroffenen Grundstücken stehen. Bislang erhalten sie hierzu in Papierform entsprechende Mitteilungen durch die Katasterämter. Im Rahmen der Zusammenarbeit zwischen der Finanz- und Katasterverwaltung wurde ein Konzept für Direktauskünfte der Bewertungsstellen bei den Finanzämtern aus dem bei den Katasterämtern automatisiert geführten Liegenschaftsbuch zwischen den beiden Verwaltungen Anfang 1995 entwickelt. Im Mai 1995 war die Programmierung abgeschlossen. 3 Finanzämter waren jeweils mit der notwendigen Hardware ausgestattet. Auch war eine Pilotinstallation erfolgreich getestet. Mitte Juli 1995 wurde der Landesbeauftragte für Datenschutz über die bevorstehende Verfahrenseinführung unterrichtet.

Die datenschutzrechtliche Bewertung zeigte, daß für die Ausweitung der Abrufmöglichkeiten auf die Bewertungsstellen der Finanzämter die gemäß § 10 Abs. 1 SDSG notwendige gesetzliche Grundlage nicht vorhanden ist. Das Verfahren wurde daraufhin eingestellt. Die fehlende gesetzliche Grundlage soll durch eine Novellierung des Katastergesetzes geschaffen werden. Bei frühzeitiger Beteiligung meiner Dienststelle vor Fertigstellung des Verfahrens hätte auch von hier auf die fehlende Rechtsgrundlage hingewiesen werden können. Dies hätte somit dazu beigetragen, unnötige Personal- und Geräteinvestitionen zu vermeiden.

13.2 Einsicht in Bauakten

In einem Streitfall begehrte der Eigentümer eines Grundstückes Einsicht in die Bauakten seines Nachbarn, da er illegale Um- und Anbauten vermutete. Nachdem die Verwaltung dieses Ersuchen abschlägig beschieden hatte, erhob er Widerspruch. Nach Mitteilung der Behörde wurde dem Eigentümer aufgrund der Entscheidung des Rechtsausschusses Akteneinsicht in die Bauakte des Nachbarn gewährt.

Von der Entscheidung des Rechtsausschusses erfuhr der Eigentümer des betroffenen Grundstückes nichts, so daß ihm eine Überprüfung der Entscheidung nicht möglich war. In der unterbliebenen Zustellung des Widerspruchsbescheids liegt ein Verstoß gegen Rechtsnormen des Datenschutzes, nach denen jeder grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen hat. Das Recht, vor Akteneinsicht durch den Nachbarn gegen den Widerspruchsbescheid selbst Klage zu erheben und damit eine Überprüfung der Rechtmäßigkeit der Akteneinsicht zu erreichen, wurde dadurch vereitelt (vergl. Art. 19 Abs. 4 GG).

13.3 Einwilligung auf Bauanträgen

Baut jemand ein Haus, erhält er oft eine Vielzahl nützlicher, aber auch manchmal lästiger privater (Werbe-) Informationen. Adressen und Bauabsicht werden von Bauaufsichtsbehörden an private Vermittler mitgeteilt. Die Bauanträge enthielten hierzu bisher lediglich eine Einwilligungserklärung für die Weitergabe verschiedener Daten an Baustelleninformationsdienste. Durch die Novellierung des SDSG im Jahre 1993 hat der Gesetzgeber in § 4 klargestellt, daß der Betroffene - falls er in die Verarbeitung seiner Daten einwilligt - in geeigneter Weise über die Bedeutung dieser Einwilligung, insbesondere über den Verwendungszweck der Daten und bei einer beabsichtigten Übermittlung über die Empfänger der Daten aufzuklären ist. Außerdem ist er unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß er die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen kann.

Das Ministerium für Umwelt, Energie und Verkehr hat mir eine Textergänzung vorgelegt, die diesen Anforderungen entspricht. Allerdings wollte das Ministerium vor Änderung des Antragsformulars prüfen, ob selbst mit Einwilligung des Betroffenen für die Zukunft überhaupt noch an der Übermittlung festgehalten werden soll; das Ergebnis ist mir nicht bekannt.

14 Steuern

Im steuerlichen Bereich haben uns Fragen der Auftragsdatenverarbeitung in zweierlei Hinsicht beschäftigt:

Der Zwang, die Kosten der öffentlichen Verwaltung zu senken, führt dazu, Dienstleistungen an private Dritte zu vergeben. Die für die Finanzverwaltung, die das Steuergeheimnis des § 30 Abgabenordnung zu wahren hat, aus datenschutzrechtlicher Sicht besonders zu beachtenden Anforderungen habe ich bereits in meinem 15. Tätigkeitsbericht (TZ 11.6) eingehend dargestellt. Desweiteren ist in § 5 Abs. 3 SDSG ausdrücklich geregelt, daß der Landesbeauftragte für Datenschutz vom Auftraggeber über die Beauftragung zu unterrichten ist.

Die Erfassung von Einkommensteuererklärungen durch ein privates Dienstleistungsunternehmen in Rheinland-Pfalz, von der ich durch das Ministerium für Wirtschaft und Finanzen erfahren habe, ist demgegenüber so problematisch, daß ich mich dagegen aussprechen mußte.

Hinsichtlich der Auftragsdatenverarbeitung enthält die Abgabenordnung keine bereichsspezifische Regelung. Da somit eine Verarbeitung der steuerlichen Daten außerhalb der Finanzverwaltung grundsätzlich nicht zulässig wäre, es aber offensichtlich ein praktisches Bedürfnis gab, die Rechenkapazität außerhalb der Finanzämter in speziellen Einrichtungen zu bündeln, wurden Rechenzentren durch Änderung des § 6 Abs. 2 AO „als Finanzbehörden" in der Abgabenordnung namentlich genannt. Dadurch erhielten sie die ausdrückliche gesetzliche Befugnis, Steuerdaten zu verarbeiten. Eine Datenverarbeitung von Steuerdaten durch Dritte könnte demnach allenfalls bei einer öffentlichen Stelle und dann auch nur für technisch-mechanische Hilfstätigkeiten in Betracht kommen. Für die Zulässigkeit der Beauftragung einer privaten Stelle mit der Datenverarbeitung von besonders sensiblen Daten im Steuerbereich ist auf jeden Fall eine eindeutige bereichsspezifische Rechtsgrundlage erforderlich.

Hinzu kommt, daß die Daten der Einkommensteuererklärung einen umfassenden Überblick über alle persönlichen und wirtschaftlichen Verhältnisse eines Steuerpflichtigen geben. Die Offenlegung solch sensibler Daten betrifft den Kernbereich des grundgesetzlich verankerten Persönlichkeitsrechts auf informationelle Selbstbestimmung sowie des Steuergeheimnisses. Durch die Erfassung außerhalb des räumlichen Bereichs der Finanzverwaltung in Räumen eines privaten Unternehmens, das zudem noch in einem anderen Bundesland seinen Sitz hat, ist die Einhaltung der vertraglichen Bestimmungen, insbesondere über die technisch-organisa-

torischen Datensicherungsmaßnahmen, in der Praxis kaum zu gewährleisten.

Trotz meiner erheblichen datenschutzrechtlichen Bedenken wurde die Erfassung dieser sehr sensiblen Daten an das private Unternehmen in Rheinland-Pfalz vergeben, um - wie es heißt - zeitlich begrenzt einen Bearbeitungsrückstand abzubauen.

Für weniger problematisch halte ich eine andere Hilfstätigkeit:

Verschiedene Gemeinden hatten im Berichtszeitraum angefragt, inwieweit die Kuvertierung und Zustellung von Lohnsteuerkarten durch ein privates Unternehmen erfolgen darf.

Lohnsteuerkarten enthalten zwar ebenfalls eine Reihe steuerlicher Daten, die jedoch bei weitem nicht so sensibel sind wie die der Einkommensteuererklärung. Zudem erstreckt sich die Tätigkeit des privaten Dritten auf reine Hilfsfunktionen, die keine gezielte Kenntnisnahme der Daten erfordern. In Übereinstimmung mit dem Ministerium für Wirtschaft und Finanzen halte ich diese Auftragsdatenverarbeitung für hinnehmbar. Dabei muß allerdings das eingesetzte Personal nach dem Verpflichtungsgesetz verpflichtet werden, es dürfen keine Personen eingesetzt werden, die aus in ihrer Person liegenden Gründen strafrechtlich nicht zur Verantwortung gezogen werden können, die öffentliche Stelle muß als Absender für den Betroffenen erkennbar bleiben und der Umschlag darf keine Hinweise auf das Privatunternehmen enthalten.

Allerdings wäre auch hier grundsätzlich zu fordern, daß eine gesetzliche Ermächtigung zur Auftragsdatenverarbeitung in die Abgabenordnung aufgenommen wird. Es ist Aufgabe des Gesetzgebers und nicht der Finanzverwaltung, zwischen vertretbaren und nicht vertretbaren Einschränkungen des Rechts auf informationelle Selbstbestimmung zu differenzieren.

15 Wirtschaft

15.1 Ablichtung des Bundespersonalausweises bei Sparkassen

Verschiedene Petenten haben sich gegen die Praxis der Sparkassen - wie anderer Kreditinstitute - gewandt, bei Kontoeröffnungen stets den Bundespersonalausweis abzulichten. Die Sparkassen sehen sich hierzu verpflichtet und verweisen dabei oft auf das Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz), und zwar auch, wenn bei den betreffenden Kontoeröffnungen keine Transaktion im Sinne des Geldwäschegesetzes erfolgte.

Zwar müssen sich die Sparkassen vor der Kontoeröffnung Gewißheit über die Person und Anschrift des Verfügungsberechtigten verschaffen und die entsprechenden Angaben auf dem Konto festhalten, denn nach § 154 Abgabenordnung (AO) darf niemand auf einen falschen oder erdichteten Namen für sich oder einen Dritten ein Konto einrichten. Weitergehende gesetzliche Grundlagen insbesondere für das Anfertigen von Kopien des Bundespersonalausweises enthält die AO aber nicht.

Das Geldwäschegesetz sieht dagegen eine entsprechende Möglichkeit ausdrücklich vor. Unabhängig zu der Legitimationsprüfung gemäß § 154 AO muß nämlich danach eine Identifizierung erfolgen, bei der auch Art, Nummer und ausstellende Behörde des vorgelegten amtlichen Ausweises festgehalten wird. § 9 Geldwäschegesetz läßt eine Aufzeichnung der Identifizierungsdaten durch Kopieren der vorgelegten Dokumente zu. Die Identifizierung darf unterbleiben, wenn der Kunde der Sparkasse persönlich bekannt ist und die Identität schon anläßlich früherer Transaktionen festgestellt und dokumentiert wurde. Da aber das Gesetz nur bei Geldgeschäften mit einer Größenordnung ab 20.000 DM Anwendung findet (oder bei konkreten Anhaltspunkten, daß dieser Schwellenwert künstlich unterschritten wird), besteht diese gesonderte Identifizierungspflicht nicht, so daß bei geringeren Beträgen keine Rechtsgrundlage für das Kopieren amtlicher Ausweise besteht. Dies stellt vielmehr eine unzulässige Datenvorratshaltung dar, da diese Daten in vielen Fällen überhaupt nicht und ansonsten frühestens bei Transaktionen nach dem Geldwäschegesetz erforderlich werden; dann aber reicht es zur Aufgabenerfüllung der Sparkassen aus, die Daten entsprechend den Bestimmungen des Geldwäschegesetzes zum Zeitpunkt der Transaktion zu erheben und zu spei-

chern. (In jedem Fall bestünden selbst dann datenschutzrechtliche Bedenken, mit den Kopien im Geldwäschegesetz nicht vorgesehene Identifizierungsdaten wie z.B. das Bild des Betroffenen, Angaben über Körpergröße und Augenfarbe festzuhalten).

Auch der BGH hat in seinem Urteil vom 18.10.1994 (DuD 6/95 Seite 363 ff) entschieden, daß die Identifikationspflicht des Geldwäschegesetzes selbständig ist und neben die Pflichten des § 154 AO tritt. § 154 AO wird durch das Geldwäschegesetz nicht erweitert. Die Zielrichtung beider Vorschriften ist nämlich unterschiedlich: Während die in § 154 AO enthaltene Identifikationspflicht aus steuerlichen Gründen zugunsten des Fiskus angeordnet ist, will das Geldwäschegesetz den Strafverfolgungsbehörden Anhaltspunkte für Geldwäschetransaktionen, spezifisch für die Bekämpfung der Geldwäsche, verfügbar machen.

Trotz der eindeutigen Rechtslage empfiehlt allerdings das Bundesaufsichtsamt für das Kreditwesen, das zuständige Kontrollbehörde für die Sparkassen ist, die Ausweispapiere bereits bei der Geschäftsanbahnung, d.h. bei Kontoeröffnung zu speichern, so daß sich die Sparkassen in einer Konfliktsituation befinden. Dabei ist auch wenig hilfreich, die Rechtsgrundlage für Erhebung und Speicherung der Daten nach dem Geldwäschegesetz in einer stillschweigenden Einwilligung der Betroffenen zu suchen. Die vorliegenden Eingaben beweisen eindeutig, daß nicht jeder mit der praktizierten Verfahrensweise einverstanden ist. Außerdem setzt eine Einwilligung im Sinne des Datenschutzgesetzes voraus, daß der Betroffene zuvor über Zweck, Inhalt und Verwendung seiner Daten umfassend aufgeklärt wurde. Zudem bedarf die Einwilligung im Regelfall der Schriftform. Diese Voraussetzungen liegen jedoch bei einer stillschweigenden Einwilligung gerade nicht vor.

Die Bundesregierung hat zwischenzeitlich einen Entwurf eines Gesetzes zur Verbesserung der Geldwäschebekämpfung vorgelegt (BR-Drucksache 554/96). Durch den Gesetzentwurf soll der Anwendungsbereich der Strafvorschrift zur Geldwäsche erweitert, das strafprozessuale Ermittlungsinstrumentarium verbessert, Unsicherheiten bei der Handhabung des Geldwäschegesetzes beseitigt und die Aufsicht des Bundesaufsichtsamtes für das Kreditwesen auf Wechselstuben erstreckt werden.

gen den Willen eines Unverdächtigen (§ 163 b Abs. 2 Satz 2 StPO).

In meiner Stellungnahme gegenüber den zuständigen Ressorts habe ich - nicht zuletzt aufgrund der Eingaben - gefordert, die Regelung im § 9 Geldwäschegesetz, die die Feststellung der Identität des Betroffenen durch Kopie des amtlichen Ausweises erlaubt, zu streichen. Selbst nach einer Stellungnahme des Bundesaufsichtsamtes für das Kreditwesen hat sich der Zweck dieser Regelung, mit den Fotokopien bessere Ermittlungsansätze zu schaffen, in der Praxis nicht realisiert. Von fast allen Landeskriminalämtern sei dies ebenfalls eingeräumt worden.

Unter diesen Voraussetzungen darf die Bestimmung nicht weiter aufrechterhalten bleiben.

15.2 Maßnahmen zum Schutz vor Banküberfällen (Videoaufzeichnung; Sprachaufzeichnung)

Im Interesse der Kunden und Kundinnen sowie zum Schutze der Mitarbeiterinnen und Mitarbeiter hat der Sparkassen- und Giroverband Überlegungen angestellt, wie in den Sparkassen der zunehmenden Häufigkeit von Banküberfällen begegnet werden könnte. Dabei hat man eine Außenüberwachung der Geschäftsstellen und eine Sprachaufzeichnung im Innenbereich der Geschäftsstellen in Betracht gezogen.

Ich habe dazu folgende Auffassung vertreten:

1. Außenüberwachung der Geschäftsstellen

   Nach der Rechtssprechung können Filmaufzeichnungen über der Öffentlichkeit zugängliche Bereiche mittels Videogerät auch dann einen unzulässigen Eingriff in das Persönlichkeitsrecht des Betroffenen darstellen, wenn keine Absicht zur Verbreitung der so hergestellten Bildnisse einer Person besteht (BGH, Urteil vom 25.4.1995, NJW 1995, 1955).

   Dabei ist stets unter Würdigung aller Umstände des Einzelfalles eine Güter- und Interessenabwägung zwischen den rechtlich geschützten Positionen der Beteiligten vorzunehmen. Von besonderer Bedeutung ist hierbei, daß die Überwachung (auch) Personen betreffen soll, die

mit den Sparkassen keinerlei Beziehung verbindet, weil die technische Einrichtung insbesondere auch den öffentlichen Verkehrsraum erfassen soll, um bereits Maskierungen oder dergleichen vor Betreten der Geschäftsräume erkennen und für spätere Ermittlungen vorhalten zu können. Die in Ausübung des Hausrechts das Grundstück beobachtende Videoüberwachung, die datenschutzrechtlich weniger problematisch erscheint, kann deswegen außer Betracht bleiben.

Videoaufzeichnungen, die im Hinblick auf mögliche Raubüberfälle überwiegend Unbeteiligte im öffentlichen Verkehrsraum erfassen, sind in erster Linie bedenklich, weil jeder Eingriff in das Recht auf informationelle Selbstbestimmung durch öffentliche Stellen und nichtöffentliche Stellen im Sinne des Bundesdatenschutzgesetzes entweder einer gesetzlichen Grundlage oder der Einwilligung des Betroffenen bedarf (§ 4 BDSG).

Eine gesetzliche bereichsspezifische Grundlage für derartige Videoaufzeichnungen durch die Sparkassen ist nicht vorhanden; die Einholung der Einwilligung aller Betroffenen ist nach den Gesamtumständen nicht möglich.

Soweit erkennbar, lassen sich für die Kontrolle des öffentlichen Verkehrsraums etwaige Eingriffsbefugnisse nur nach den Vorschriften der Straßenverkehrsbestimmungen und der Straßengesetze für die in diesen Gesetzen bezeichneten öffentlichen Stellen herleiten. Die Verfolgung und Verhütung von Straftaten im öffentlichen Raum ist ausschließliche Aufgabe der Strafverfolgungsbehörden und der Polizei. Auch im übrigen läßt sich keine sachliche Zuständigkeit für die gezielte Überwachung des öffentlichen Verkehrsraums durch die Sparkassen zum Zwecke der Gefahrenabwehr herleiten.

Dieses Ergebnis wird durch die Rechtslage im Hinblick auf die den zuständigen öffentlichen Stellen eingeräumten Befugnisse zur Videoüberwachung bestätigt. Die Aufnahme von Lichtbildern zählt polizeirechtlich und strafprozessual zu den sogenannten erkennungsdienstlichen Maßnahmen (§ 10 Abs. 3 Saarländisches Polizeigesetz; SPolG, § 81 b Strafprozeßordnung; StPO). Strafprozessuale Maßnahmen dieser Art sind nur gegen Beschuldigte/Verdächtige zulässig, nicht jedoch gegen den Willen eines Unverdächtigen (§ 163 b Abs. 2 Satz 2 StPO).

Zulässige Maßnahmen zur Gefahrenabwehr sind für die Polizeibehörden in §§ 9, 10 SPolG näher umschrieben, wobei für Objekte oder Personen unmittelbar Gefährdungen vorhanden sein müssen. Selbst an solch gefährdeten Objekten sind an den Grundsatz der Verhältnismäßigkeit besondere Anforderungen zu stellen, so daß Personen, die offensichtlich in keiner Beziehung zu dem mit der Maßnahme verbundenen Zweck stehen, nicht überprüft und gegebenenfalls auch nicht erkennungsdienstlich behandelt werden dürfen. Gerade dieser unbeteiligte Personenkreis würde allerdings durch die geplante Überwachung in großem Umfang erfaßt.

Wegen der fehlenden Rechtsgrundlage für einen derart weitgehenden Eingriff in die Rechte Unbeteiligter konnte ich die Maßnahme nicht befürworten.

2. Sprachaufzeichnungen im Innenbereich der Geschäftsstellen

Die Aufzeichnung aller Gespräche in den Innenräumen einer Sparkasse begegnet erheblichen datenschutzrechtlichen Bedenken.

Nach § 201 StGB stellt die unbefugte Aufnahme des nicht-öffentlich gesprochenen Wortes eines anderen auf einen Tonträger eine Straftat in Form der Verletzung der Vertraulichkeit des Wortes dar.

Eine gesetzliche Befugnis der Sparkassen zur Aufzeichnung des nicht-öffentlich gesprochenen Wortes ist nicht erkennbar. Die Strafbarkeit kann daher nur bei Vorliegen von Rechtfertigungs- bzw. Entschuldigungsgründen entfallen. Diese Gründe setzen nach den §§ 32 ff StGB jedoch ausnahmslos einen „gegenwärtigen" Angriff oder eine „gegenwärtige" Gefahr voraus. Die abstrakte Gefahr der Möglichkeit eines Überfalls erfüllt die Voraussetzungen nicht. In den Fällen der sogenannten Sozialadäquanz kann ebenfalls ein Tatbestandsausschluß in Betracht kommen. Es entspricht jedoch keineswegs der Tradition, jegliche geschäftliche Verhandlung aufzuzeichnen, um dadurch Gefahren abzuwehren, die außerhalb der konkreten Geschäftsbeziehung liegen.

Da hier Straftatbestände verwirklicht würden, habe ich von einer derartigen Maßnahme abgeraten.

Unabhängig von den generellen Bedenken habe ich noch darum gebeten, die in Betracht gezogenen Vorkehrungen nach einem strengen Maßstab darauf zu überprüfen, ob sie zur Verhütung von Raubüberfällen überhaupt geeignet wären.

Die Eignung ist ein Teilaspekt des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes und auch des engeren Erforderlichkeitsgrundsatzes. Eingriffe in die Persönlichkeitsrechte Unbeteiligter wären nur dann zulässig, wenn schwerwiegenden Beeinträchtigungen der Kunden, der Mitarbeiter und Mitarbeiterinnen nicht in anderer Weise zumutbar begegnet werden kann.

Die Eignung der ständigen Videoüberwachung und erst recht der Aufzeichnung des gesprochenen Wortes zur Verhütung von Überfällen erscheinen mir äußerst fragwürdig. Das gilt gleichermaßen für den erhofften „Abschreckungseffekt", der durch deutliche Hinweise auf die Kontrollmaßnahmen eintreten sollte, wie auch für Erleichterungen einer Täterermittlung bei einem konkreten Überfall, da solche Vorkehrungen mit einfachen Mitteln von Seiten der Täter außer Kraft gesetzt werden können: Bei der Planung eines Raubüberfalles kann eine unauffällige Maskierung gewählt werden, der Aufzeichnung des gesprochenen Wortes kann mit Gesten und ausschließlich schriftlichen Anweisungen durch den Täter begegnet werden.

Ich gehe davon aus, daß die Überlegungen wegen der gravierenden datenschutzrechtlichen Bedenken nicht weiterverfolgt wurden.

15.3 Verwaltungsvorschrift zum Vollzug der §§ 14, 15 und 55c Gewerbeordnung

Mit Änderung der (bundesrechtlichen) Gewerbeordnung (GewO) 1994 waren auch die landesrechtlichen Ausführungsvorschriften zu ändern; meinen Anregungen zur Verbesserung der datenschutzrechtlichen Bestimmungen ist das Ministerium für Wirtschaft und Finanzen in einigen Punkten gefolgt.

Unter einem Aspekt, den ich für besonders wichtig halte, nämlich bei Auskünften aus dem Gewerberegister an nicht-öffentliche Stellen wie Adreßbuchverlage oder Meinungsforschungsinstitute, vertritt das Ministerium aber eine „datenschutzunfreundliche" Haltung:

Nach der früheren Rechtslage waren derartige Datenübermittlungen eindeutig nur mit Einwilligung der Gewerbetreibenden zulässig; hierauf hatte ich noch im Vorfeld des Erlasses der neuen Verwaltungsvorschrift auf Anfrage einer Gewerbebehörde hingewiesen. Allerdings wußte ich auch von der größten Gewerbebehörde im Land, daß die Gewerbetreibenden in ihrer Mehrzahl solche Einwilligungen nicht erteilt hatten, sie also mit der Einschränkung des Rechts auf informationelle Selbstbestimmung nicht einverstanden waren.

Weil die novellierte Gewerbeordnung eine Auskunft bereits zuläßt, wenn der Auskunftbegehrende ein „berechtigtes Interesse" an der Kenntnis der Daten glaubhaft macht, möchte das Wirtschaftsministerium generell - auch bei Gruppenauskünften, wie sie Adreßbuchverlage begehren, - auf das Erfordernis einer Einwilligung verzichten. Ein „berechtigtes Interesse" ist jedes Interesse, das im Einklang mit der Rechtsordnung steht, wobei es sich um ein ideelles oder wirtschaftliches Interesse handeln kann; letzteres wäre bei Adreßbuchverlagen anzunehmen. Folge ist, daß nicht-öffentlichen Stellen die in der GewO bezeichneten Daten des gesamten Gewerberegisters zur Verfügung stehen und damit weite Verbreitung finden.

Demgegenüber verlangt das Bundesverfassungsgericht - in Übereinstimmung mit der Saarländischen Verfassung (Art. 2 Satz 3) - für jede Einschränkung des Rechts auf informationelle Selbstbestimmung ein überwiegendes Allgemeininteresse (BVerfGE 65, 43-44). Für die Sonderform Gruppenauskünfte kommt hinzu, daß es an der gebotenen normenklaren Regelung fehlt, weil aus dem Gesetzestext als solchem nicht zweifelsfrei hervorgeht, daß auch solche Datenübermittlungen über eine Vielzahl von Betroffenen zugelassen werden sollen.

Betont werden muß ferner, daß ebenso wie im Melderecht die Erlaubnistatbestände der Gewerbeordnung nicht zur Auskunftserteilung verpflichten, sondern eine jeweilige (Ermessens-) Entscheidung der Gewerbebehörde erfordern. Um der verfassungsrechtlichen Wertentscheidung Rech-

nung zu tragen, wurde dem Ministerium empfohlen, solche Auskünfte auch künftig an die ausdrückliche Einwilligung der Gewerbetreibenden zu binden, wie dies in der entsprechenden Regelung des Landes Niedersachsen auch niedergelegt ist. Die neue Verwaltungsvorschrift ist dem nicht gefolgt.

16 Verkehr, Umwelt

16.1 Gegenseitige Information der Behörden über Bürgereingaben

Ein Bürger einer saarländischen Gemeinde hatte einige kritische Anmerkungen zu dem Bau einer Landstraße vorzubringen und richtete ein entsprechendes Schreiben an das damalige Umweltministerium. Eine Kopie des Antwortschreibens schickte das Ministerium an die Wohnortgemeinde des betreffenden Bürgers, wo das Schreiben in einer öffentlichen Ortsratssitzung unter Nennung seines Namens verlesen wurde.

Der betreffende Bürger empörte sich darüber, daß ein an ihn gerichtetes Schreiben in fremde Hände gelangt war.

Das Ministerium hat auf meine Anfrage seine Vorgehensweise damit zu rechtfertigen versucht, daß die von dem Petenten angesprochenen Themen von allgemeinem Interesse für die betreffende Gemeinde seien. Damit die Gemeinde für künftige Anfragen ihrer Bürger in die Lage versetzt werde, entsprechende Anfragen selbst zu beantworten, sei die Abschrift an die Gemeinde versandt worden. Das Ministerium sei nicht dafür verantwortlich zu machen, daß die Gemeinde den Inhalt solcher Schreiben in öffentlichen Ortsratssitzungen verlese.

Die Argumentation des Ministeriums kann mich nicht überzeugen. Der von dem Ministerium angegebene Zweck kann auch dann erfüllt werden, wenn Namen nicht genannt werden. Die Begründung verkennt außerdem, daß der Eingriff in das informationelle Selbstbestimmungsrecht nicht erst in der öffentlichen Verlesung des betreffenden Briefes lag, sondern bereits in der Weitergabe an die Gemeinde.

Mittlerweile hat das Ministerium seine Abteilungen angewiesen, die Namen der Adressaten unkenntlich zu machen, wenn Schreiben, in denen

Einzelanfragen beantwortet werden, in Durchschrift an Gemeinden oder Kreise versandt werden.

16.2 Einholung eines Gutachtens für die Erteilung der Fahrerlaubnis zur Fahrgastbeförderung

Im 15. TB (TZ 16.1) wurde die Anordnung des Ministeriums für Umwelt, Energie und Verkehr bemängelt, vor Erteilung von Fahrerlaubnissen zur Fahrgastbeförderung (z.B. für Busfahrer) in jedem Fall eine medizinisch-psychologische Untersuchung zu verlangen. Die bundesgesetzliche Regelung schreibt nämlich den Straßenverkehrsbehörden vor, nach ihrem Ermessen zu entscheiden, ob die geistige und körperliche Eignung auch mit anderen (weniger tief in die Persönlichkeitssphäre eingreifenden) Gutachten nachgewiesen werden kann.

Daß das Umweltministerium entgegen gesetzlicher Bestimmmung und trotz Hinweises auf eine vergleichbare Entscheidung des Bundesverwaltungsgerichtes durch Erlaß vorschreibt, dieses Ermessen gar nicht zu betätigen, mußte ich beanstanden.

Zu meinem großen Bedauern ist die Haltung des Ministeriums vom Ausschuß für Datenschutz nicht mißbilligt worden. Die Abgeordneten haben sich vom Verweis einer Verwaltungsbehörde auf höherrangige Werte mehr beeindruckt gezeigt als von der Beachtung des Bundesgesetzes, mit dem das Parlament eben diese Abwägung von Werten getroffen hat; befremdlicherweise spricht das Ministerium neben den Rechtsgütern „Leben und Gesundheit der Verkehrsteilnehmer" auch dem Rechtsgut „Eigentum" höheren Rang als der informationellen Selbstbestimmung zu.

Trotz der Billigung des Ausschusses (vgl. TZ 2) darf der Widerspruch zwischen Rechtslage und tatsächlicher Verfahrensweise nicht bestehen bleiben.

16.3 Saarländisches Abfallwirtschaftsgesetz

Im Berichtszeitraum hat mir das Ministerium für Umwelt, Energie und Verkehr den Entwurf eines Abfallwirtschaftsgesetzes (SAWG) vorgelegt. Ziel des Gesetzes ist nach der Gesetzesbegründung neben der Harmonisierung mit dem Kreislaufwirtschafts- und Abfallgesetz des Bundes und dem EG-Recht, neuen Entwicklungen und Erfordernissen der modernen Abfallwirtschaft Rechnung zu tragen.

Das Ministerium hat die Gelegenheit wahrgenommen, in einem speziellen Paragraphen die Voraussetzungen zulässiger Datenverarbeitung im Bereich des Abfallrechts zu regeln. Dies wird grundsätzlich begrüßt. Allerdings genügt die Vorschrift nicht den Anforderungen, die das Bundesverfassungsgericht für zulässige Eingriffe in das Recht auf informationelle Selbstbestimmung nennt. Im Volkszählungsurteil aus dem Jahre 1983 hat das Gericht ausgeführt, daß Eingriffe in das Recht 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 entspricht.

Die Regelung des Gesetzentwurfs beschränkt sich demgegenüber im wesentlichen auf die Aussage, daß die zuständigen Behörden zum Zwecke und im Rahmen der ihnen durch Gesetz zugewiesenen Aufgaben personenbezogene Daten erheben, speichern und übermitteln dürfen.

Ich habe gefordert, daß im Gesetz selbst die einzelnen Verarbeitungszwecke, zu denen personenbezogene Daten erhoben und übermittelt werden dürfen, festgelegt werden; in einer Rechtsverordnung könnten dann die Einzelheiten geregelt werden. Außerdem habe ich angeregt, im Gesetzentwurf eine Ermächtigung zur Festlegung von Aufbewahrungsfristen aufzunehmen.

Darüber hinaus habe ich vorgeschlagen, in das Gesetz eine Regelung aufzunehmen, wonach die notwendigen personenbezogenen Daten bei den Betroffenen mit deren Kenntnis zu erheben sind. Nur ausnahmsweise, wenn andernfalls die Erfüllung der Aufgaben nach dem Abfallwirtschaftsgesetz gefährdet werden, ist eine Erhebung auch ohne Kenntnis der Betroffenen zulässig.

Kritisch auseinandergesetzt habe ich mich mit einer Vorschrift des Gesetzes, wonach das Landesamt für Umweltschutz von allen abfallrechtlich relevanten Vorgängen in Kenntnis zu setzen ist. Für mich stellt sich bei Daten mit Personenbezug die Frage, ob es angemessen und erforderlich ist, daß das Landesamt für Umweltschutz über alle Vorgänge informiert wird, die ein Eingreifen nach abfallrechtlichen Vorschriften erfordern können. Ich sehe die Gefahr, daß an einer zentralen Stelle im Saarland sämtliche Informationen über Verstöße gegen abfallrechtliche Vorschriften gespeichert werden, obwohl es im Regelfall ausreichend sein dürfte, wenn die entsprechenden Vorgänge bei den jeweils zuständigen Behörden geführt werden.

Bemängelt habe ich in diesem Zusammenhang, daß eine Zweckbestimmung der übermittelten Informationen im Gesetzentwurf fehlt, so daß unklar bleibt, wie die Informationen beim Landesamt für Umweltschutz weiterverarbeitet werden. So stellt sich etwa die Frage, ob die Errichtung von Verzeichnissen mit „Abfallsündern" geplant ist oder wann die dem Landesamt für Umweltschutz übermittelten Informationen wieder gelöscht werden.

17 Gesundheit

17.1 Kostenabrechnung bei Schwangerschaftsabbrüchen

Aufgrund des durch Artikel 5 des Schwangeren- und Familienhilfeänderungsgesetzes eingeführten Gesetzes zur Hilfe für Frauen bei Schwangerschaftsabbrüchen in besonderen Fällen hat eine Frau bei einem rechtswidrigen, aber straffreien Schwangerschaftsabbruch ab 1. Januar 1996 einen Anspruch auf Übernahme der Kosten, wenn ihr die Aufbringung der Mittel für den Abbruch der Schwangerschaft nicht zuzumuten ist. Die Leistungen werden auf Antrag durch die gesetzlichen Krankenkassen gewährt; die Länder erstatten den Kassen die entstehenden Kosten.

Ich habe mich bei dem zuständigen Ministerium über Einzelheiten des Verfahrens informiert, um festzustellen, ob der Forderung des Gesetzgebers ausreichend Rechnung getragen wird, wonach im gesamten Verfah-

ren das Persönlichkeitsrecht der Frau unter Berücksichtigung der besonderen Situation der Schwangerschaft zu achten ist (§ 3 Abs. 5 des Gesetzes zur Hilfe bei Frauen bei Schwangerschaftsabbrüchen in besonderen Fällen).

Ich habe etwa Wert darauf gelegt, daß die Antragsunterlagen bei den Krankenkassen vernichtet werden, wenn sie zur Aufgabenerfüllung nicht mehr erforderlich sind. Das Ministerium geht wegen des Erfordernisses der Rechnungsprüfung von einer 5-jährigen Löschungsfrist aus.

Nach einem Vertrag zwischen dem Saarland und den Verbänden der Krankenkassen im Saarland wird dem Ministerium lediglich das Geburtsdatum und die Postleitzahl der betreffenden Frau mitgeteilt.

Besonders wichtig war für mich die Feststellung, daß die den Schwangerschaftsabbruch durchführenden Ärzte direkt mit den Krankenkassen abrechnen, eine Einschaltung der Kassenärztlichen Vereinigung bei der Abrechnung somit nicht erfolgt. Jede Einbeziehung einer weiteren Stelle in das Abrechnungsverfahren in diesem sensiblen Bereich, erhöht die Gefahr einer Verletzung der Persönlichkeitsrechte der betroffenen Frauen. Dementsprechend bestimmt § 3 Abs. 4 des Gesetzes zur Hilfe für Frauen bei Schwangerschaftsabbrüchen in besonderen Fällen, daß der Arzt mit der Krankenkasse abrechnet.

17.2 Ehrenamtliche Mitarbeiter im Krankenhaus

Mir wurde von der Praxis in einem Krankenhaus berichtet, wonach ehrenamtlichen Mitarbeitern gestattet wurde, ohne Absprache mit den Patienten Einsicht in deren Krankenunterlagen zu nehmen.

So anerkennenswert das ehrenamtliche Engagement in Krankenhäusern ist, müssen doch die zum Schutz der Persönlichkeitsrechte der Patienten erlassenen Datenschutzbestimmungen beachtet werden. Der zulässige Umgang mit Patientendaten im Krankenhaus ist im Saarländischen Krankenhausgesetz geregelt. Die Gewährung von Einsicht in die Krankenunterlagen stellt datenschutzrechtlich eine Übermittlung von Patientendaten an Personen außerhalb des Krankenhauses dar. Eine gesetzliche Befugnis zur Übermittlung der Patientendaten an ehrenamtliche Mitarbeiter oh-

ne ausdrückliche Einwilligung der Patienten existiert nicht. Ein datenschutzkonformes Vorgehen könnte so aussehen, daß die Patienten über die Tätigkeit der ehrenamtlichen Helfer unterrichtet und befragt werden, ob ein Kontakt hergestellt und eine Einsichtnahme in die Krankenakten gestattet werden soll.

17.3 Löschung von Patientendaten im Krankenhaus

Ein Problem, das mich immer wieder beschäftigt, ist die Frage, wann und unter welchen Voraussetzungen Patientendaten im Krankenhaus, die in automatisierten Verfahren gespeichert sind, gelöscht werden müssen. Die Fragestellung wird in Zukunft noch an Brisanz gewinnen, je mehr die Krankenhäuser dazu übergehen, über die reinen Verwaltungsdaten hinaus ganze Krankenakten EDV-mäßig zu speichern. Im Berichtszeitraum haben mich die Universitätskliniken Homburg von der Absicht der Psychiatrie der Universitäts-Nervenklinik informiert, die Entlassungsbriefe bisher behandelter Patienten auch nach deren Entlassung jederzeit zugreifbar automatisiert zu speichern. Ich wurde gebeten, die datenschutzrechtliche Zulässigkeit dieser Vorgehensweise zu bewerten.

Maßgebend für die Beurteilung ist die Vorschrift des § 29 Abs. 5 Saarländisches Krankenhausgesetz (SKHG). Nach dieser Vorschrift sind Patientendaten, die im automatisierten Verfahren mit der Möglichkeit des Direktabrufes gespeichert sind, unmittelbar nach Abschluß der Behandlung zu löschen. Gespeichert bleiben darf nur ein Restdatensatz, der für das Auffinden der Krankenakten erforderlich ist (§ 29 Abs. 5 Satz 3 SKHG). Daten entlassener Patienten dürfen nach diesen gesetzlichen Vorschriften nicht mehr direkt zugreifbar sein. Abgeschlossene Zeiträume sind auf externen Datenträgern zu sichern; die Daten auf dem betriebsfähigen System sind zu löschen. Wenn ein Patient das Krankenhaus erneut zur Behandlung aufsucht, müssen seine Daten von dem externen Datenträger in das automatisierte System wieder übernommen werden.

Wenn ein Patient das Krankenhaus verlassen hat, ist es nicht mehr notwendig, daß die Krankenhausbediensteten Zugriff auf seine Krankheitsdaten haben. Insofern ist § 29 Abs. 5 SKHG Ausfluß des das Datenschutzrecht beherrschenden Grundsatzes der Erforderlichkeit.

Maßgebend für die Beseitigung des Direktabrufes ist der „Abschluß der Behandlung". Auch wenn es zutrifft, daß nach Schätzung der Klinik bei etwa 60 % der psychiatrisch behandelten Patienten eine Wiederaufnahme notwendig ist, ist doch davon auszugehen, daß mit der Entlassung die Behandlung zunächst beendet ist. Auch unter diesem Gesichtspunkt kann deshalb eine dauerhafte Vorhaltung der Patientendaten im Direktzugriff nicht akzeptiert werden.

Ausgehend von der derzeitigen Rechtslage kann daher das Vorhaben der Psychiatrie der Universitäts-Nervenklinik nicht ohne Verstoß gegen die datenschutzrechtlichen Vorschriften des Saarländischen Krankenhausgesetzes realisiert werden.

17.4 Auskunft über Aids-Erkrankung

Ein Krankenhausarzt hatte sich wegen des Auskunftsersuchens eines Sozialamtes an mich gewandt. Das Sozialamt wollte wissen, ob ein bestimmter Hilfeempfänger an Aids infiziert ist und ob die vierwöchige stationäre Behandlung auf die Immunschwäche zurückzuführen ist. Werden diese Fragen bejaht, sind die Kosten der während der stationären Behandlung vom Sozialamt gewährten Sozialleistungen (z. B. Wohnungsmiete) vom überörtlichen Träger der Sozialhilfe, also dem Land, zu erstatten. Die sachliche Zuständigkeit des überörtlichen Trägers der Sozialhilfe nach § 100 BSHG tritt auch dann ein, wenn - wie in diesem Falle - der Hilfeempfänger krankenversichert ist und demnach die gesetzliche Krankenkasse die stationären Behandlungskosten trägt.

Der Patient war nach Darstellung des Krankenhauses mit der Datenübermittlung an das Sozialamt nicht einverstanden. Eine Übermittlung war folglich nur zulässig, wenn eine Rechtsvorschrift sie erlaubt. Das Sozialamt hatte sein Auskunftsersuchen nicht auf eine spezielle Vorschrift - etwa des BSHG - stützen können. Auch die Übermittlungsregelungen des Saarländischen Krankenhausgesetzes (SKHG) boten keine Rechtsgrundlage. Eine gesetzliche Mitteilungspflicht (§ 29 Abs. 4 Nr. 3 SKHG), wie sie etwa gegenüber dem Gesundheitsamt nach dem Bundesseuchengesetz vorgesehen ist, bestand nicht. Auch die Voraussetzungen des § 29 Abs. 4 Nr. 5 SKHG, der eine Datenübermittlung an die Kostenträger zur Erfüllung deren gesetzlicher Aufgaben erlaubt, lagen nicht vor. Kostenträger im

Sinne dieser Vorschrift ist die Stelle, die die stationären Behandlungskosten zu übernehmen hat.

Die vom Sozialamt gestellten Fragen durften vom Krankenhausarzt also nur beantwortet werden, wenn der Sozialhilfeträger auch die Kosten der stationären Versorgung im Krankenhaus hätte übernehmen müssen. In diesem Falle waren jedoch die Behandlungskosten nicht vom Sozialamt, sondern von der gesetzlichen Krankenkasse getragen worden. Das Sozialamt kann demnach die ärztlichen Auskünfte nur erhalten, wenn der Sozialhilfeempfänger seine Einwilligung erteilt.

17.5 Datenschutzprüfung beim Staatlichen Gewerbearzt

Der Staatliche Gewerbearzt ist ein Landesamt im Geschäftsbereich des Ministeriums für Frauen, Arbeit, Gesundheit und Soziales. Zu seinen Aufgaben gehört insbesondere die Erstattung von Gutachten bei Berufskrankheiten im Rahmen der gesetzlichen Unfallversicherung, die Überwachung von Gewerbebetrieben im Hinblick auf den medizinischen Arbeitsschutz und die Ermächtigung von Ärzten nach der Strahlenschutzverordnung.

Die anfallenden Informationen werden in automatisiert geführten Dateien erfaßt. Dabei enthält insbesondere die Datei der Berufskrankheitenverfahren sensible Gesundheitsdaten. Bereits der im Aktenzeichen aufgenommene Berufskrankheitenschlüssel kann Hinweise auf bestimmte Krankheiten geben (z.B. Nr. 1301: Schleimhautveränderungen, Krebs oder andere Neubildungen der Harnwege durch aromatische Amine). Darüber hinaus ist es für die Dokumentation des Verfahrens jedoch nicht erforderlich, auch noch den Krankheitenschlüssel (ICD) zu speichern und damit jederzeit abrufbereit zu halten.

Künftig wird auf das Datenfeld sowohl in der Berufskrankheitendatenbank als auch in der Datenbank, in der Informationen über Betriebsbesichtigungen erfaßt werden, verzichtet. Bereits gespeicherte Krankheitsdaten werden gelöscht. Für alle Dateien, darunter auch die vorgesehene Speicherung der Gutachtentexte im automatisierten System, sind Löschungsfristen festzulegen.

Außerdem wurden Maßnahmen zur Verbesserung der Datensicherung bei der automatisierten Datenverarbeitung und im konventionellen Bereich vorgeschlagen.

17.6 Gesundheitsdienstgesetz

Der öffentliche Gesundheitsdienst ist bislang nur unzureichend gesetzlich geregelt. Weil es bei den gesundheitlichen Daten über die Bevölkerung um personenbezogene Daten von höchster Sensibilität geht, ist auch vom Landesbeauftragten für Datenschutz seit Jahren die Forderung erhoben worden, das noch unter national-sozialistischer Herrschaft in Kraft getretene „Gesetz zur Vereinheitlichung des Gesundheitswesens" durch ein modernes Gesundheitsdienstgesetz zu ersetzen (zuletzt 15. TB, TZ 1).

Im Berichtszeitraum hat mir das Ministerium für Frauen, Arbeit, Gesundheit und Soziales den Entwurf eines Gesundheitsdienstgesetzes vorgelegt. Das Gesetz beschreibt die Aufgaben der Behörden des öffentlichen Gesundheitsdienstes (zuständiges Ministerium als oberste Landesgesundheitsbehörde, Landesamt für Arbeitsschutz und Gesundheit, Gesundheitsämter). In einem speziellen Teil sind die Voraussetzungen des zulässigen Umgangs mit personenbezogenen Daten geregelt.

Neben einer Vielzahl von Verbesserungen im Detail habe ich folgende Änderungen bzw. Ergänzungen angeregt:

- Die Aufgaben und Befugnisse des neu zu errichtenden Landesamtes für Arbeitsschutz und Gesundheit werden im Gesetzentwurf nur schlagwortartig umrissen. Weil sich die Datenverarbeitungsbefugnisse nach der Aufgabenzuweisung richten, ist eine normenklare Aufgabenbeschreibung aus datenschutzrechtlicher Sicht besonders wichtig.

- Wenn ein Bürger ein Beratungsangebot des Gesundheitsamtes wahrnimmt, muß ihm auf Wunsch die Möglichkeit eingeräumt werden, gegenüber den Mitarbeitern des Gesundheitsamtes anonym zu bleiben.

- Es muß sichergestellt sein, daß persönliche Geheimnisse, die der Bürger den Bediensteten des öffentlichen Gesundheitsdienstes in Wahrnehmung eines Beratungsangebotes anvertraut, nicht bei der Aus-

übung hoheitlicher Aufgaben verwertet werden. Dies erfordert der legitime Vertrauensanspruch des Bürgers. Nur wenn dies gewährleistet ist, werden die Bürger die Beratungsangebote des Gesundheitsamtes überhaupt in Anspruch nehmen. Das Verbot, die zu einem bestimmten Zweck freiwillig gegebenen Informationen zu anderen Zwecken zu verwenden, muß insbesondere auch innerhalb des Gesundheitsamtes gelten.

- Wenn die Behörden des öffentlichen Gesundheitsdienstes Gutachten und Zeugnisse erstellen, soll der die Untersuchung veranlassenden Stelle grundsätzlich lediglich das Ergebnis der Untersuchung übermittelt werden.

Es bleibt abzuwarten, inwieweit meine Vorschläge im weiteren Verlauf des Gesetzgebungsverfahrens Berücksichtigung finden.

17.7 Heilberufekammergesetz

Ebenfalls hat mir das Ministerium für Frauen, Arbeit, Gesundheit und Soziales den Entwurf eines Saarländischen Heilberufekammergesetzes (SHKG) zur Stellungnahme vorgelegt. Ziel des Gesetzes ist im wesentlichen, die drei geltenden Kammergesetze für Ärzte, Tierärzte und Apotheker in einem Gesetz zusammenzufassen, sowie die grundlegenden Regelungen dieser drei Gesetze den berufs- und gesundheitspolitischen Entwicklungen anzupassen.

Aus Anlaß der Novellierung wurden in den Entwurf auch Vorschriften aufgenommen, die die Zulässigkeit der Verarbeitung personenbezogener Daten der Kammermitglieder regeln. Damit wurde meiner Forderung (siehe zuletzt 15. TB, TZ 12.2) nach bereichsspezifischen Datenverarbeitungsvorschriften in diesem Bereich Rechnung getragen.

In folgenden Punkten halte ich den Gesetzentwurf für änderungs- oder ergänzungsbedürftig:

- Die Notwendigkeit, dem zuständigen Ministerium als Aufsichtsbehörde das bei den Kammern zu führende Mitgliederverzeichnis in personenbezogener Form zur Verfügung zu stellen, kann ich nicht erkennen.

– In dem Gesetzentwurf ist die Ermächtigung für die Kammern enthalten, die Daten ihrer Mitglieder zu verarbeiten, „soweit dies für die Wahrnehmung der ihnen in diesem Gesetz übertragenen Aufgaben erforderlich ist." Da die von den Kammern wahrzunehmenden Aufgaben in dem Gesetz nicht abschließend aufgeführt sind - die Landesregierung kann den Kammern weitere Aufgaben übertragen -, fehlt dieser Rechtsgrundlage zur Verarbeitung personenbezogener Daten die notwendige Normenklarheit.

– Für unzureichend geregelt halte ich die Voraussetzungen zulässiger Datenübermittlungen: Der Gesetzentwurf verweist hierzu auf die Übermittlungsvorschriften des Saarländischen Datenschutzgesetzes. Dies halte ich nicht für sachgerecht, da das Saarländische Datenschutzgesetz als Auffangvorschrift naturgemäß die Besonderheiten der Verarbeitung der bei den Kammern über ihre Mitglieder vorhandenen Daten nicht gerecht werden kann. Ich kann auch nicht erkennen, aus welchen Gründen der vorgelegte Gesetzentwurf hinter der derzeit geltenden Regelung im Gesetz über die Apothekerkammer des Saarlandes zurückbleibt, in dem die Voraussetzung zulässiger Datenübermittlungen abschließend geregelt sind.

– Da es im Rahmen der Erteilung der Befugnis zur Weiterbildung an Kammermitglieder unter Umständen erforderlich sein kann, Einsicht in Patientenakten zu nehmen, habe ich für diesen Eingriff in das informationelle Selbstbestimmungsrecht der Patienten die Schaffung einer gesetzlichen Grundlage gefordert.

– Der Gesetzentwurf sieht vor, daß bei Verhängen einer Geldbuße oder Entzug des aktiven und passiven Wahlrechts zur Kammerversammlung die Entscheidung im Mitteilungsblatt der jeweiligen Kammer veröffentlicht werden kann. Wenn das Berufsgericht feststellt, daß das Kammermitglied unwürdig ist, den Beruf auszuüben, ist diese Entscheidung sogar öffentlich bekannt zu machen. Ausweislich der Begründung sollen diese Veröffentlichungen der Verstärkung des Sanktionscharakters dieser Strafen dienen.

Ich sehe in solchen Veröffentlichungen einen unverhältnismäßigen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen.

Es handelt sich um einen besonders schwerwiegenden Eingriff, weil der Empfängerkreis der Informationen groß ist und die Veröffentlichung erhebliche Auswirkungen auf das Ansehen und die wirtschaftliche Situation der betroffenen Kammermitglieder hat. Derartige „Pranger-Maßnahmen" werte ich als unverhältnismäßige Eingriffe in die Persönlichkeitssphäre der Betroffenen. Sie sind außerdem der geltenden Rechtsordnung fremd; weder die Strafprozeßordnung noch die Disziplinarordnungen für Beamte sehen die Veröffentlichung getroffener Entscheidungen vor. Ich habe deshalb die Streichung der entsprechenden Vorschrift gefordert.

- Eine Vorschrift über die Aufbewahrungsdauer für Unterlagen über berufsgerichtliche Verfahren sollte in das Gesetz aufgenommen werden.

17.8 Krebsregister

Der 14. Tätigkeitsbericht hat sich ausführlich mit der datenschutzrechtlichen Problematik epidemiologischer Krebsregister befaßt und auch das seit 1967 bestehende Saarländische Krebsregister kritisch unter die Lupe genommen.

Im Berichtszeitraum ist am 1.1.1995 das Bundeskrebsregistergesetz in Kraft getreten.

Hervorzuheben sind insbesondere die Regelungen über die Beteiligung des Patienten bei der Meldung zum Register und zur Organisation der Krebsregister. Das Gesetz hat sich für eine Meldeberechtigung der Ärzte mit einem Widerspruchsrecht für die Patienten entschieden. Um eine größtmögliche Anonymität der Patienten zu wahren, bestehen die Krebsregister aus selbständigen, räumlich, organisatorisch und personell voneinander getrennten Vertrauensstellen und Registerstellen.

Während das Meldeverfahren in den Ländern abweichend von der bundesgesetzlichen Regelung gestaltet werden kann, steht die Trennung der Krebsregister in Vertrauens- und Registerstellen nicht zur Disposition der Landesgesetzgeber.

Schon allein aus diesem Grund besteht die Notwendigkeit der Novellierung des geltenden Saarländischen Krebsregistergesetzes. An einem Referentenentwurf wird derzeit im Ministerium für Frauen, Arbeit, Gesundheit und Soziales gearbeitet; erste Gespräche haben bereits stattgefunden.

17.9 Forschungsprojekte beim Saarländischen Krebsregister

Das Saarländische Krebsregister hat mich um eine datenschutzrechtliche Stellungnahme zu einer beabsichtigten Studie mit dem Titel „Fall-Kontroll-Studie zu arbeitsplatzbedingten Risikofaktoren seltener Krebsformen unbekannter Ursache" gebeten.

Ziel der Studie ist es festzustellen, inwieweit Umstände am Arbeitsplatz Ursache für bestimmte Krebsarten sein können. Die Studie läuft in der Weise ab, daß alle Personen, die im Saarland in einem bestimmten Zeitraum an den definierten Krebsarten erkrankt sind, erfaßt werden. Diejenigen Patienten, die sich bereit erklären, an der Studie teilzunehmen, sollen auf Fragebögen Angaben zu ihrer Berufsbiographie, zur medizinischen Vorgeschichte sowie zu ihrem Lebensstil (Rauchen, Alkohol) machen.

Positiv ist zu vermerken, daß mich das Krebsregister so frühzeitig beteiligt hat, daß einige Schwachstellen, die ich in dem Datenschutzkonzept festgestellt habe, behoben werden konnten:

- Es muß sichergestellt sein, daß keine Daten des Krebsregisters für die Durchführung der Studie genutzt werden und daß Angaben, die die Betroffenen im Rahmen der Studie machen, nicht im Krebsregister gespeichert werden. Über den im Saarländischen Krebsregistergesetz festgelegten Datenkatalog dürfen im Krebsregister keine Daten gespeichert werden. Eine Nutzung personenbezogener Daten zu Forschungszwecken sieht das Krebsregistergesetz derzeit nicht vor.

Um diesem Abschottungsgebot Rechnung zu tragen, war von der Projektleitung von vornherein eine personelle Trennung vorgesehen. Eine personelle Verknüpfung habe ich allerdings darin gesehen, daß eine der für die Studie vorgesehenen Interviewerinnen gleichzeitig Mitarbei-

terin im Krebsregister ist. Die Projektleitung hat mittlerweile vom Einsatz dieser Krebsregistermitarbeiterin als Interviewerin abgesehen.

- Das Datenschutzkonzept ging davon aus, daß bestimmte „Basisinformationen" wie Name, Wohnort, Geburtsdatum, Geschlecht, Diagnose auch dann an das Erhebungsbüro übermittelt werden dürfen, wenn der Patient sein Einverständnis nicht erteilt. Eine solche Vorgehensweise ist mit den Regeln über die ärztliche Schweigepflicht und, soweit die Daten von Krankenhäusern übermittelt werden, mit den Vorschriften des Saarländischen Krankenhausgesetzes nicht vereinbar. Die Projektleitung hat diesen Einwand akzeptiert; die Daten der Patienten, die mit einer Erfassung nicht einverstanden sind, werden nur noch codiert übermittelt.

- Nach der Forschungsregelung (§ 28) des Saarländischen Datenschutzgesetzes sind die Daten zu anonymisieren, sobald der Forschungszweck es gestattet; die Merkmale, mit deren Hilfe der Personenbezug wiederhergestellt werden kann, sind gesondert zu speichern. Diesem Erfordernis war ursprünglich insofern nicht entsprochen, als die Absicht bestand, die personenbezogenen Merkmale von den diagnostischen Informationen zwar abzutrennen, aber in einem Stahlschrank gemeinsam aufzubewahren.

- In der Einverständniserklärung fehlte der ausdrückliche Hinweis auf die Freiwilligkeit und darauf, daß keine Nachteile bei Nichtteilnahme entstehen (§ 4 Satz 3 SDSG).

Im Berichtszeitraum wurde ich noch zu dem Datenschutzkonzept einer weiteren Studie, deren Gegenstand die Untersuchung potentiell vemeidbarer Verzögerungen bei der diagnostischen Abklärung von Krebserkrankungen ist, gehört. Beim Datenschutzkonzept dieser Studie waren, nicht zuletzt aufgrund der bei dem vorerwähnten Forschungsprojekt gewonnenen Erkenntnisse nur noch geringfügige Änderungen im Detail erforderlich.

17.10 Transplantationsgesetz

In der modernen Medizin wird immer mehr möglich, daß Menschen mit Hilfe fremder Körperteile überleben oder erfolgreich behandelt werden. In der Regel werden diese Teile einem anderen Körper entnommen, bei dem alle Hirnfunktionen irreversibel ausgefallen sind (sog. Hirntod), aber die biologische Funktionstüchtigkeit von Organen über das künstliche Aufrechterhalten von Herz- und Kreislauffunktionen noch vorübergehend erhalten bleiben kann.

Ob und unter welchen Voraussetzungen menschliche Organe entnommen werden dürfen, um sie anderen Menschen zur Krankenbehandlung oder sogar zur Lebensrettung zur Verfügung zu stellen, berührt grundlegende ethische und juristische Fragen: es geht um die Grenzziehung zwischen Leben und Tod sowie um die Möglichkeit, solidarische Einstandspflichten der Bürger bei einer Organspende für andere zu begründen. Dem Bundestag liegen hierzu verschiedene Gesetzentwürfe vor.

Zentraler Diskussionspunkt ist dabei nicht nur, ob - wie bislang fast einmütig angenommen - in juristischer Hinsicht der Hirntod materielles Kriterium für das Ende menschlichen Lebens ist. Entscheidend für die Zulässigkeit ist insbesondere das gebotene Maß und die Art, mit dem der Betroffene oder ggf. die Angehörigen das Einverständnis mit dieser Organspende ausdrücken (müssen) und wie dies dokumentiert wird. Die Spanne reicht von generellem Ausschluß bis zu grundsätzlicher Zulässigkeit eines solchen Eingriffs und setzt verfahrensrechtlich teilweise Ausweispflichten oder das Führen von Registern voraus, die ein schnelles Erkennen eines Widerspruchs oder der Zustimmung zulassen.

Weil deshalb die Diskussion in ganz wesentlichen Fragen auch datenschutzrechtliche Aspekte hat, haben sich die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 14./15.3.1996 (Anlage 15) hierzu geäußert. Sie betonen, daß von den im Gesetzgebungsverfahren diskutierten Modellen die „enge Zustimmungslösung" - also eine ausdrückliche Zustimmung des Organspenders - den geringsten Eingriff in das Recht auf informationelle Selbstbestimmung darstellt. Sie zwingt niemanden, eine Ablehnung zu dokumentieren und setzt auch kein Organspenderegister voraus.

18 Soziales

18.1 Rechtsanspruch auf einen Kindergartenplatz

Aufgrund des neuen Kinder- und Jugendhilfegesetzes haben Kinder ab dem vollendeten 3. Lebensjahr seit dem 1.1.1996 einen Rechtsanspruch auf einen Kindergartenplatz.

Um diesen Anspruch erfüllen zu können, ist es für die Träger der öffentlichen Jugendhilfe wichtig zu wissen, für wieviele Kinder ein Platz zur Verfügung zu stellen ist. Zwar kann die Zahl der anspruchsberechtigten Kinder theoretisch aufgrund statistischer Angaben aus dem Melderegister ermittelt werden. Für die tatsächliche Nachfrage spielen aber örtliche Lage und pädagogische Ausrichtung der Einrichtung eine wichtige Rolle. In der Praxis hat sich nach Aussagen der Kindergartenträger gezeigt, daß viele Eltern ihre Kinder bei mehreren Kindergärten anmelden, so daß die Zahl der einen Kindergartenplatz nachfragenden Kinder höher erscheint, als dies tatsächlich der Fall ist. Um einen realistischen Überblick über die Zahl der tatsächlich anspruchsberechtigten Kinder zu bekommen, haben verschiedene Jugendhilfeträger vorgeschlagen, eine zentrale Meldestelle auf kommunaler Ebene einzurichten, an die die Kindergärten die auf ihren Warte- und Anmeldelisten stehenden Kinder melden müssen.

Im Gegensatz zu einzelnen anderen Bundesländern besteht im Saarland keine Verpflichtung der Träger von Kindertageseinrichtungen, an den Jugendhilfeträger personenbezogene Daten der angemeldeten Kinder zu übermitteln.

Allerdings halte ich entsprechende Datenübermittlungen für zulässig, wenn folgende Voraussetzungen erfüllt werden:

- Zuständig für die Entgegennahme der Meldungen ist lediglich der für die Gewährleistung des Rechtsanspruchs auf einen Kindergartenplatz zuständige Träger der öffentlichen Jugendhilfe.

- Die Daten dürfen von diesem nur für die Feststellung von Mehrfachanmeldungen benutzt werden.

- Die Übermittlung ist auf solche Daten zu beschränken, die den Personenbezug nicht unmittelbar deutlich werden lassen (Geburtsdatum und Straßennamen ohne Hausnummer). Es muß jeder Versuch unterbleiben, den Namen der Kinder etwa mit Hilfe des Einwohnermelderegisters festzustellen.

- Die Daten sind zu löschen, sobald die Zahl der einen Kindergartenplatz suchenden Kinder festgestellt ist.

18.2 Namentlicher Aufruf beim Sozialamt

Mehrere Sozialhilfeempfänger haben sich über die Praxis eines Sozialamtes beschwert, die Sozialhilfeempfänger bei der Scheckausgabe mit Namen aufzurufen. Die Betroffenen sehen es als einen Eingriff in ihre Persönlichkeitsrechte an, wenn den übrigen wartenden Sozialhilfeempfängern ihr Name bekannt gegeben wird.

Ich halte das in dem betreffenden Sozialamt praktizierte namentliche Aufrufen der Hilfeempfänger für einen Verstoß gegen das Sozialgeheimnis. Jeder Sozialleistungsempfänger hat Anspruch auf die Wahrung des Sozialgeheimnisses durch den Leistungsträger (§ 35 SGB I). Dazu gehört, daß die Leistungsträger durch organisatorisch-technische Maßnahmen sicherstellen, daß Dritten die Tatsache des Bezugs von Sozialleistungen nicht offenbart wird. Ich habe deshalb das Sozialamt aufgefordert, den Verfahrensablauf so zu ändern, daß eine Namensnennung unterbleibt.

Das betreffende Sozialamt hat die datenschutzrechtliche Problematik seiner Verfahrensweise zugestanden und versichert, im Rahmen organisatorischer und finanzieller Möglichkeiten ein Verfahren zu finden, das datenschutzrechtlich unbedenklich ist. Mitgeteilt wurde, daß man in Verhandlungen mit einer Sparkasse stehe, um durch die Einrichtung von Guthabenkonten Barzahlungen zu vermeiden. Wie weit diese Verhandlungen mittlerweile gediehen sind, stand bei Redaktionsschluß noch nicht fest.

18.3 Gewährung von Sachleistungen an Sozialhilfeempfänger

Ich wurde darüber informiert, daß es in vielen Kommunen des Saarlandes üblich sein soll, daß ein Teil der Sozialhilfe nicht in bar ausgezahlt wird. Statt dessen schließen die Sozialhilfeträger mit Privatfirmen Verträge über Dienstleistungen, wie z.B. Malerarbeiten, oder die Lieferung von Waren, wie z.B. Herden, Kühlschränken oder Waschmaschinen. Die datenschutzrechtliche Problematik dieser Verfahrensweise ist offenkundig: Den Firmen wird bekannt, daß es sich bei dem Kunden um einen Sozialhilfeempfänger handelt; aufgrund der Kenntnis entsprechender Vereinbarungen mit den Sozialhilfeträgern gilt dies auch dann, wenn der Sozialhilfebezug nicht ausdrücklich genannt oder aus äußeren Umständen wie der Bezeichnung des Amtes offenkundig deutlich wird.

Ich bin der Auffassung, daß es eine Befugnis zur Übermittlung dieser Sozialdaten an die Privatfirmen nicht gibt, so daß die geschilderte Vorgehensweise der Sozialämter eine Verletzung des Sozialgeheimnisses darstellt. Namentlich die Voraussetzungen der hier in Betracht kommenden Übermittlung nach § 69 Abs. 1 Nr. 1 SGB X sind nicht erfüllt, da es zur Gewährung von Hilfe zum Lebensunterhalt nicht erforderlich ist, einem Dritten (hier den Lieferfirmen) Sozialdaten zu übermitteln. Denn dem Sozialamt bieten sich statt dessen rechtlich unbedenkliche Alternativen: Entweder gewährt es die Hilfe als Geldleistung und vermeidet damit von vornherein die Übermittlung von Sozialdaten. Oder es gewährt die Hilfe in Form einer Sachleistung, darf dabei allerdings nicht in das informationelle Selbstbestimmungsrecht des Hilfeempfängers eingreifen. Das Sozialamt muß auf jeden Fall ein Verfahren wählen, bei dem der Sozialhilfebezug des betroffenen Dritten nicht bekannt gegeben werden muß. Ist dies nicht praktikabel, so hat die Hilfeleistung in Geld zu erfolgen.

Die Gewährung der Sozialhilfe in Form von Sachleistungen kann allenfalls in Fällen gerechtfertigt sein, in denen Anhaltspunkte dafür bestehen, daß der Hilfeempfänger die Geldleistung nicht für den vorgegebenen Zweck verwenden wird. Nicht hinnehmbar ist aber, daß allen Sozialhilfeempfängern aus wirtschaftlichen Gründen die Sozialhilfe in Form von Sachleistungen gewährt wird.

Ich habe zu der Problematik das Ministerium für Frauen, Arbeit, Gesundheit und Soziales um Stellungnahme gebeten. Das Ministerium hat mitge-

teilt, daß es die von mir vertretene Rechtsauffassung teilt; die örtlichen Sozialhilfeträger seien gebeten worden, bei entsprechenden Feststellungen die rechtswidrige Verfahrensweise abzustellen.

18.4 Bankauskünfte in der Sozialhilfe

Immer wieder muß ich bei Prüfungen von Sozialämtern und aufgrund von Bürgereingaben feststellen, daß Sozialämter bei der Einholung von Einwilligungen für Bankauskünfte gegen datenschutzrechtliche Bestimmungen verstoßen.

So hat mich eine Petentin auf die Praxis eines Sozialamtes aufmerksam gemacht, das automatisch bei jeder Antragstellung eine Einwilligung zur Einholung von Bankauskünften verlangt. Nachdem die Petentin sich geweigert hatte, die entsprechende Unterschrift zu leisten, wurde die Gewährung von Sozialhilfe eingestellt.

Ich habe das Sozialamt auf die Rechtswidrigkeit seines Verhaltens hingewiesen. Zwar ist derjenige, der Sozialleistungen beantragt oder erhält, zur Mitwirkung verpflichtet (§ 60 SGB). Er hat unter anderem alle Tatsachen anzugeben, die für die Leistung erheblich sind und auf Verlangen des zuständigen Leistungsträgers der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen. Die Einholung einer Bankauskunft kann aber nur dann als erforderlich angesehen werden, wenn konkrete Anhaltspunkte dafür vorliegen, daß die Angaben des Antragstellers zu seinen Einkommens- und Vermögensverhältnissen unrichtig sind.

Das Sozialamt konnte keine Anhaltspunkte für die Unrichtigkeit der Erklärungen der Petentin vorbringen und mußte, nachdem die Petentin im einstweiligen Anordnungsverfahren vor dem Verwaltungsgericht obsiegt hatte, die Sozialhilfe weiter gewähren.

In einem weiteren Fall beschwerte sich ein Bürger darüber, daß er sämtliche Banken seines Wohnortes vom Bankgeheimnis gegenüber dem Sozialamt entbinden sollte. Auch diese Verhaltensweise des betreffenden Sozialamtes habe ich als datenschutzrechtlich unzulässig kritisiert. Ich sehe in dieser Maßnahme kein geeignetes Mittel, den Sachverhalt aufzuklären. Es lagen keinerlei konkrete Anhaltspunkte dafür vor, daß der Pe-

tent außer bei seinen Hausbanken gerade bei anderen Geldinstituten seines Wohnortes weitere Konten unterhält.

Hinzu kam noch, daß das Sozialamt von dem Petenten verlangte, die Formulare blanko zu unterschreiben. Es war beabsichtigt, erst nachträglich die Anschriften der jeweiligen Institute und den Übermittlungszweck einzutragen. Eine Einwilligung kann jedoch nur rechtsverbindlich sein, wenn der Betroffene darüber informiert ist, welche konkreten Stellen welche Angaben wem gegenüber zur Verfügung zu stellen haben.

Auf meine Intervention hin hat das betreffende Sozialamt ein Auskunftsbegehren auf die Kreditinstitute beschränkt, bei denen nach den Umständen des Falles überhaupt ein Guthaben zu vermuten war. Zugesagt wurde auch, den Antragstellern in Zukunft keine Blanko-Vordrucke zur Unterschrift vorzulegen.

18.5 Die Adresse des Geschädigten

Das OLG Schleswig hat eine Entscheidung getroffen, die aus der Sicht des Datenschutzes auf Bedenken stößt. Der Entscheidung lag folgender Sachverhalt zugrunde: Die Krankenkasse hatte nach der Körperverletzung eines Mitglieds den wegen der übernommenen Behandlungskosten auf sie übergegangenen Schadenersatzanspruch beim Schädiger geltend gemacht. Darin hatte sie u.a. Namen, Anschrift und Geburtsdatum des geschädigten Mitglieds als Zeugen angegeben. Dies nahm der Schädiger nach eigenen Angaben zum Anlaß, das ihm bis dahin nicht näher bekannte Opfer in der Wohnung aufzusuchen und erneut zu verprügeln. Das Gericht hielt die Mitteilung der genauen Adresse an den Schädiger für zulässig. Der Schädiger habe ein Recht darauf, die Anschrift, die neben dem Geburtsdatum zu den elementaren Identifikationsdaten gehöre, zu erfahren.

Nach den Vorschriften des Sozialgesetzbuches (§ 69 Abs. 1 SGB X) ist eine solche Datenübermittlung nur zulässig, wenn sie im Einzelfall zur Aufgabenerfüllung der Krankenkasse erforderlich ist. Regelmäßig dürften Angaben zum Ort, zum Zeitpunkt sowie zu den näheren Umständen des Vorfalls genügen. Nur in Ausnahmefällen, etwa wenn der Täter innerhalb kurzer Zeit mehrere Personen geschädigt hat und den Ersatzanspruch

nicht einem bestimmten Opfer zuordnen kann, sollten zusätzliche Angaben zur Identifizierung des Geschädigten nachgeliefert werden.

Die Krankenkassen in meinem Zuständigkeitsbereich, mit denen ich korrespondiert habe, wollen in diesem Sinne verfahren.

18.6 Projekt Arbeitstraining für psychisch Behinderte

Ein gemeinnütziger Träger hat mich um Überprüfung der Unterlagen gebeten, die der Hauptfürsorgestelle für die Förderung des Projekts Arbeitstraining für psychisch Behinderte vorzulegen waren. Bei Beginn der Trainingsmaßnahme, nach 6 Monaten und beim Abschluß sollte der Träger über die betreute Person berichten, u. a. welcher Art die psychische Behinderung ist (schizophren, manisch-depressiv, sonstige endogene Psychose), ob die betreute Person allein lebt, in einer Partnerschaft, in einer Familie oder einer Einrichtung, über welches Einkommen sie im einzelnen monatlich verfügt. Die Teilnehmer an dem Projekt sollten außerdem eine Einverständniserklärung unterschreiben. Vor allem die Formulierungen dieser Erklärung haben Ängste bei den Betroffenen geweckt, was mit ihren Daten geschieht:

- Der Betreuer beim Träger wurde u. a. ermächtigt, Einsicht in die Krankenakten zu nehmen; ihm konnten personenbezogene Daten, Berichte, Gutachten u.ä. ausgehändigt werden, ohne daß näher bestimmt war, bei welchen Ärzten und Stellen dies möglich sein sollte. Die Einsichtnahme in die Krankenakte durch einen Nichtmediziner halte ich gerade bei psychisch Kranken für einen unangemessenen, schwerwiegenden Eingriff in die Intimsphäre der Betreuten. Die Erteilung erforderlicher Auskünfte dürfte ausreichen. Die nicht abschließende Aufzählung („u. ä.") mußte außerdem den Eindruck entstehen lassen, als könnten beliebige Unterlagen zur Verfügung gestellt werden.

- Die betreute Person hatte ferner darin einzuwilligen, daß „die Daten, die als Nachweis zu führen sind, entsprechend an zuständige Ämter und Behörden zur Kenntnisnahme bzw. zum Verbleib weitergeleitet werden" können. Die Befürchtung der Behinderten war verständlich, daß dies eine Datenweitergabe an alle möglichen Stellen rechtfertigen könnte. Wenn die Daten regelmäßig (nur) an die Hauptfürsorgestelle

übermittelt werden, sollte - um unnötige Ängste zu vermeiden - auch nur diese Stelle in der Einwilligungserklärung als Datenempfänger genannt werden.

– Ebenso sollte in dem Vordruck „Fachärztliche Bescheinigung", in der der psychiatrische Krankheitsverlauf in den Fällen darzustellen ist, in denen keine amtlich anerkannte Schwerbehinderung vorliegt, aus Gründen der Transparenz für Arzt und Behinderten klar zum Ausdruck kommen, daß sie der Vorlage bei der Hauptfürsorgestelle dient.

Das Ministerium für Frauen, Arbeit, Gesundheit und Soziales hat die Antragsunterlagen inzwischen überarbeitet, den Umfang der Datenerhebung eingeschränkt und bei der Einverständniserklärung meinen Bedenken Rechnung getragen.

18.7 Neues Unfallversicherungsrecht

Mit dem „Gesetz zur Einordnung des Rechts der gesetzlichen Unfallversicherung in das Sozialgesetzbuch (Unfallversicherungs-Einordnungsgesetz UVEG)", das in seinen wesentlichen Teilen ab 1. Januar 1997 in Kraft getreten ist, wurde das Unfallversicherungsrecht als 7. Buch in das Sozialgesetzbuch eingegliedert.

Im Gesetzgebungsverfahren hatten die Datenschutzbeauftragten des Bundes und der Länder insbesondere kritisiert, daß die Aufgaben der Unfallversicherungsträger und ihrer Verbände soweit ihre Befugnisse zur Datenerhebung, -verarbeitung und -nutzung nicht in der verfassungsrechtlich gebotenen Klarheit geregelt waren (Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995, Anlage 16).

Als wichtige Neuregelungen sind folgende Punkte zu erwähnen:

– Vor Erteilung eines Gutachten-Auftrages soll der Unfallversicherungsträger dem Versicherten mehrere Gutachter zur Auswahl benennen (§ 200 Abs. 2 SGB VII).

- Neu ist die Regelung, wonach der Unfallversicherungsträger bei der Feststellung des Versicherungsfalles Auskünfte über Erkankungen und frühere Erkrankungen des Betroffenen von anderen Stellen oder Personen erst einholen soll, wenn hinreichende Anhaltspunkte für den ursächlichen Zusammenhang zwischen der versicherten Tätigkeit und dem schädigenden Ereignis vorliegen (§ 199 Abs. 3 SGB VII).

- Die Auskunftspflicht von Ärzten über die Behandlung und frühere Erkrankungen ist beschränkt worden. Der Unfallversicherungsträger soll seine Auskunftsverlangen zur Feststellung des Versicherungsfalles auf solche Erkrankungen oder auf solche Bereiche von Erkrankungen beschränken, die mit dem Versicherungsfall in einem ursächlichen Zusammenhang stehen können (203 Abs. 1 SGB VII). Das gleiche gilt für Auskunftsverlangen gegenüber den Krankenkassen (§ 188 SGB VII).

- Der Versicherte kann vom Unfallversicherungsträger verlangen, über die von den Ärzten und Krankenkassen übermittelten Daten unterrichtet zu werden (§ 201 Abs. 1 und § 188 SGB VII).

- Der Gesetzgeber hat festgelegt, für welche Zwecke eine Datei für mehrere Unfallversicherungsträger errichtet werden darf und welche Daten in diesen Dateien verarbeitet werden dürfen. Vor der erstmaligen Speicherung seiner Sozialdaten in einer solchen Datei ist der Versicherte über die Art der gespeicherten Daten, die speichernde Stelle und den Zweck der Datei durch den Unfallversicherungsträger schriftlich zu unterrichten.

18.8 Datenschutzprüfung bei der Innungskrankenkasse des Saarlandes (IKK)

Bei der IKK, einer kleineren Krankenkasse, die erst 1995 ihre Tätigkeit aufgenommen hat, wurden die Hauptverwaltung Saarbrücken und die ihr angeschlossene Geschäftsstelle geprüft.

Für die Abwicklung der Krankenkassenaufgaben wurde zum Zeitpunkt der Prüfung noch das System MOSAIK mit weitgehend zentraler Verarbeitung der Daten beim Verbandsrechenzentrum in Münster eingesetzt. Da 1997

auf das Dialogverarbeitungssystem IS-KV umgestellt werden soll, wurde das auslaufende Verfahren nicht näher untersucht. Das Sicherheitskonzept für den Einsatz von IS-KV wird im Rahmen der anstehenden Beteiligung nach § 8 Abs. 2 SDSG überprüft. Bei der Umstellung auf das neue Verfahren wird auch der Vertrag mit dem Verbandsrechenzentrum über die Auftragsdatenverarbeitung zu überarbeiten sein. Der jetzige Vertrag enthält - obwohl umfangreiche IT-Dienstleistungen erbracht werden - außer einem allgemeinen Hinweis, daß „die Bestimmungen für Datenschutz und Datensicherung zu berücksichtigen" sind, keine konkreten Regelungen über die zu treffenden Datensicherungsmaßnahmen. Die Kenntnisse der Systemverwaltung vor Ort sind zu verbessern, damit grundlegende Funktionen (z. B. die Kontrolle der Protokolldateien) bei der IKK wahrgenommen werden können.

Weitere Prüfungsfeststellungen:

- Nach § 286 SGB V haben die Krankenkassen u. a. die Verfahren zur Verarbeitung der Daten, die Abgrenzung der Verantwortungsbereiche bei der Datenverarbeitung und die Datensicherungsmaßnahmen in einer Dienstanweisung zu regeln. Bei der IKK lag zwar ein Muster einer Dienstanweisung eines anderen Landesverbandes vor, allerdings war sie noch nicht auf die hiesigen Verhältnisse umgearbeitet und in Kraft gesetzt. Dies ist inzwischen erfolgt.

- Dateibeschreibungen für die Aufnahme in das Dateienregister sind nicht erstellt.

- Der Zugriff auf die Versichertendaten ist über die Zuständigkeit einer Geschäftsstelle hinaus möglich. Mitarbeiter der Geschäftsstelle Saarbrücken und der Hauptverwaltung konnten ebenso auf Daten der der Geschäftsstelle in einer anderen Stadt zugeordneten Versicherten zugreifen wie umgekehrt (vgl. hierzu auch unten TZ 18.12). Die IKK will bei der Einführung des Systems IS-KV die Zugriffsbefugnisse auf den Versichertenbestand der jeweiligen Geschäftsstelle beschränken.

- Im automatisierten System werden sämtliche an die Versicherten gewährten Leistungen mit Ausnahme der Arztleistungen und Arzneimittel gespeichert. Angaben über Leistungen dürfen jedoch nur dann gespeichert werden, wenn sie zur Prüfung der Voraussetzungen späterer

Leistungsgewährung erforderlich sind (§ 292 SGB V). Die IKK hat zugesichert, bei Einführung des neuen Systems die hierfür benötigten Datenarten zu bestimmen. Dabei sind auch Löschungsfristen für die einzelnen Datenarten festzulegen.

- Für die bei der Kasse aufbewahrten Abrechnungsunterlagen der Ärzte, Apotheker und Leistungserbringern von Heil- und Hilfsmitteln sind Löschungsfristen festzulegen (§ 304 SGB V in Verbindung mit § 84 SGB X). Die IKK ist dieser Forderung inzwischen nachgekommen; sie wird die Unterlagen nach 2 Jahren vernichten.

18.9 Automatisierte Übermittlung von Abrechnungsdaten durch Kassenzahnärztliche Vereinigungen an gesetzliche Krankenkassen

Durch das Gesundheitsreformgesetz und das Gesundheitsstrukturgesetz ist den Kassenärztlichen und Kassenzahnärztlichen Vereinigungen aufgegeben worden, die Abrechnung der ärztlichen Leistungen mit den gesetzlichen Krankenkassen automatisiert durchzuführen. Zum Ausgleich des damit verbundenen Risikos einer völligen Durchleuchtung der gesundheitlichen Verhältnisse der Patienten durch automatisierte Datenauswertungen hat der Gesetzgeber gleichzeitig festgelegt, daß die Angaben über die abgerechneten ärztlichen Leistungen und Diagnosen den Krankenkassen nur in dem für diese Abrechnung erforderlichen Umfang und „nicht versichertenbezogen" zu übermitteln sind.

Der in dem Schiedsspruch vom 20. Februar 1995 festgelegte Umfang der Datenübermittlung zwischen Kassenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen erfüllt diese Anforderungen des Sozialgesetzbuches an den Datenaustausch nicht, weil das Risiko der Identifizierbarkeit des Versicherten besteht.

Unter anderem auf das Drängen der Datenschutzbeauftragten ist es zurückzuführen, daß der größte Teil der gesetzlichen Krankenkassen mittlerweile den Umfang der zu übermittelnden Daten reduziert hat. Auf ihrer Konferenz am 22./23. Oktober 1996 haben die Datenschutzbeauftragten des Bundes und der Länder den Verband der Angestellten-Ersatzkassen, der bisher als einziger Spitzenverband der gesetzlichen Krankenkassen

diese Datenreduzierungen nicht mitgetragen hat, aufgefordert, sich der einheitlichen Linie anzuschließen (Anlage 17).

18.10 Abrechnung mit Krankenkassen über eine Vermittlungsstelle

Im Berichtszeitraum ist die Absicht bekannt geworden, die Übermittlung personenbezogener Daten zwischen Kassenärztlichen und Kassenzahnärztlichen Vereinigungen, Krankenhäusern, Apotheken und sonstigen Leistungserbringern mit der gesetzlichen Krankenversicherung maschinenlesbar über öffentliche Leitungswege bzw. durch Übersendung maschinenlesbarer Datenträger (Disketten, Magnetbänder oder Magnetband-Kassetten) durchzuführen. Von verschiedenen Kassenverbänden ist vorgesehen, diesen Datenaustausch zur gesetzlichen Krankenversicherung über eine Vermittlungsstelle, ein privates Telekommunikationsunternehmen, zu leiten. Es stellt sich damit die Frage der ausreichenden Sicherung der zu übermittelnden Daten gegen unbefugte Kenntnisnahme, auch durch die Vermittlungsstelle.

Ich habe die meiner Kontrolle unterliegenden saarländischen Krankenkassen, die Saarländische Krankenhausgesellschaft sowie die Kassenärztliche und die Kassenzahnärztliche Vereinigung darauf aufmerksam gemacht, daß ich innerhalb meines Zuständigkeitsbereichs folgende Datensicherungsmaßnahmen für erforderlich halte:

- Die Verschlüsselung der personenbezogenen Daten für die Übertragung über Leitungen oder mit Hilfe von Datenträgern unverzüglich ab Betriebsaufnahme

- soweit möglich, elektronische Signatur der verschlüsselten Daten, um die Authentizität des Absenders sicherzustellen, und

- maschinelle Sicherungsprozeduren bei Wählverbindungen zur Sicherung der richtigen Zustellung.

Im Hinblick auf die Sensibilität der medizinischen Daten, die leichte Auswertbarkeit maschinell verfügbarer Daten, die Nutzung allgemeiner Übertragungswege und die Leitung der Daten über eine zentrale Annahme-

und Verteilstelle habe ich auf eine Verschlüsselung mit Beginn der Betriebsaufnahme Wert gelegt.

18.11 Gemeinsames AOK-Rechenzentrum

Die AOK für das Saarland hat mich über ihre Absicht unterrichtet, zusammen mit der AOK Rheinland-Pfalz und der AOK Hessen ein gemeinsames Rechenzentrum zu betreiben. Ziel ist es, die Rechenzentrumsleistungen künftig zu geringeren Kosten erbringen zu können.

Bei dieser Zusammenarbeit muß gewährleistet sein, daß die Zugriffe auf die Datenbestände und die Ausdrucke der Ergebnisse bei der jeweils zuständigen AOK verbleiben. Die zur Umsetzung geeigneten und erforderlichen technisch-organisatorischen Datensicherungsmaßnahmen werden derzeit zwischen den beteiligten Krankenkassen und Landesbeauftragten für den Datenschutz erörtert.

18.12 Geschäftsstellenübergreifender Zugriff auf Versichertendaten bei Krankenkassen

Die meisten Krankenkassen haben mehrere Geschäftsstellen eingerichtet, in denen ihre Versicherten betreut werden. Im Regelfall können die Sachbearbeiter in den einzelnen Geschäftsstellen auf sämtliche im automatisierten Bestand gespeicherten Leistungsdaten, dazu gehören auch Diagnosen, aller Versicherten der jeweiligen Krankenkasse zugreifen. Wie ich bereits in meinem 13. Tätigkeitsbericht (TZ. 6.1) ausgeführt habe, ist ein solch umfassender Zugriff im Hinblick auf die schutzwürdigen Belange der Betroffenen nicht zuzulassen; er ist auch zur ordnungsgemäßen Aufgabenerfüllung nicht geboten. Es reicht aus, wenn nur den von dem Mitglied ausdrücklich gewählten Geschäftsstellen der Zugriff eröffnet wird. Dies kann die Geschäftsstelle am Wohnort, am Arbeitsplatz oder auch, wenn dies ausdrücklich gewünscht wird, auch sämtliche Geschäftsstellen einer Krankenkasse sein.

Die Problematik ist mittlerweile von den Datenschutzbeauftragten des Bundes und der Länder aufgegriffen worden. In ihrer Entschließung vom

9./10. März 1995 (Anlage 18) haben sich die Datenschutzbeauftragten dazu geäußert, wie ein dem Kundenservice und dem informationellen Selbstbestimmungsrecht der Versicherten gerecht werdender Datenzugriff organisiert werden muß.

18.13 Verschlüsselung der Diagnosen mit ICD-10-Code

Seit dem 1.1.1995 sind die an der vertragsärztlichen Versorgung teilnehmenden Ärzte verpflichtet, in den Abrechnungsunterlagen und in den Arbeitsunfähigkeitsbescheinigungen für die Krankenkasse die Diagnosen einzutragen (§ 295 Abs. 1 SGB V). Die Diagnosen sind nach dem vierstelligen Schlüssel der internationalen Klassifikation der Krankheiten (ICD-10), in der jeweiligen vom Deutschen Institut für Medizinische Dokumentation und Information im Auftrag des Bundesministeriums für Gesundheit herausgegebenen deutschen Fassung, zu verschlüsseln.

Die Entscheidung des Gesetzgebers führte zu erheblicher Kritik, die auch auf Datenschutzbedenken gründete. Zunächst erscheint fraglich, ob die vorgegebenen Schlüssel, die ursprünglich zu einem gänzlich anderen Zweck entwickelt worden waren, überhaupt geeignet sind, die angestrebten Zwecke zu erreichen, nämlich Falschabrechnungen der Ärzte zu verhindern, Angaben über vom Arzt veranlaßte Maßnahmen bei bestimmten Krankheiten zu erhalten und damit Datengrundlagen für wissenschaftliche Fragestellungen zu gewinnen. So wird gegen den ICD-10-Code von ärztlicher Seite unter anderem eingewandt, daß viele in der Praxis relevante Diagnosen fehlen oder daß aus dem Code nicht erkennbar ist, ob es sich um bestätigte oder Verdachtsfälle handelt.

Ein weiterer wesentlicher Kritikpunkt ist, daß der ICD-10-Code Schlüssel enthält, die keine Diagnosen, d.h. die Bezeichnung für eine Krankheit, darstellen, sondern Ursachen oder Begleitumstände von Krankheiten. Schließlich enthält der ICD-10-Code Diagnosen, die wegen der Art ihrer Formulierung geeignet sind, die Persönlichkeitsrechte der Patienten zu beeinträchtigen (z.B. F 520 Mangel oder Verlust von sexuellem Verlangen, F 632 pathologisches Stehlen, F 72 schwere Intelligenzminderung).

Inzwischen hat der Bundesgesundheitsminister bekannt gegeben, daß die Anwendung des ICD-10-Codes für die Dauer von 2 Jahren, in denen eine Überarbeitung stattfinden soll, ausgesetzt wird.

18.14 Chipkarten im Gesundheitswesen

Seit dem 1. Januar 1995 gibt es keine Krankenscheine mehr; statt dessen erhält jeder gesetzlich Krankenversicherte eine Krankenversichertenkarte. Mit der Karte weist der Versicherte seine Anspruchsberechtigung nach; sie dient außerdem dazu, die automatische Abrechnung unter Einsatz maschinenlesbarer Formulare durchzuführen. Medizinische Daten dürfen auf dieser vom Gesetzgeber vorgegebenen Krankenversichertenkarte nicht gespeichert werden.

Daneben sind Bestrebungen zur Einführung von Karten auf freiwilliger Basis festzustellen, auf denen vielfältige medizinische Patientendaten (wie etwa Anamnesedaten, Impfungen, Röntgenstatus) gespeichert werden. Der Vorteil solcher Karten soll in der schnellen und zuverlässigen Information der Ärzte untereinander liegen; bei Kartentypen mit Speicherung verordneter Medikamente werden auch die Apotheken in den Informationsfluß einbezogen. Es ist allerdings nicht zu übersehen, daß die Nutzung solcher Karten vielfältige Gefahren für das informationelle Selbstbestimmungsrecht der Betroffenen mit sich bringt (siehe auch TZ 4.2). So liegt die Gefahr einer pauschalen Offenbarung von medizinischen Daten nahe. Ein Problem ist auch, daß dem Patienten die Last aufgebürdet wird, für die Sicherheit seiner medizinischen Daten selbst zu sorgen.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich intensiv mit der Problematik befaßt und die datenschutzrechtlichen Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen in einer gemeinsamen Entschließung formuliert (siehe Anlage 19). Da die Kartenanbieter naturgemäß lediglich die Vorteile der neuen Karten herausstellen, halte ich es für wichtig, daß die potentiellen Kartennutzer im Sinne einer vollständigen Information auch über die möglichen Gefährdungen unterrichtet werden. Zusammen mit anderen Landesbeauftragten für den Datenschutz, Verbraucherzentralen und Patienteninitiativen habe ich deshalb eine Informationsbroschüre herausgegeben, die die Risiken von

Gesundheitschipkarten aufzeigt. Der Text der Broschüre ist auch in meinem Internet-Angebot (TZ 22.2) enthalten.

19 Schulen und Hochschulen

19.1 Datenschutzprüfung bei einem Gymnasium

Die bei der Prüfung der Datenverarbeitung eines Gymnasiums im Saarpfalz-Kreis festgestellten Mängel beruhen nicht auf einem besonders nachlässigen Umgang mit personenbezogenen Daten gerade an dieser Schule, sondern sind nach bisherigen Erfahrungen in ähnlicher Weise auch an anderen Schulen anzutreffen (vgl. meinen 15. Tätigkeitsbericht TZ 13.3):

- Schulverwaltungsprogramme und andere automatisierte Verfahren werden am PC ohne ausdrückliche Freigabe und ohne die erforderlichen technischen und organisatorischen Maßnahmen der Datensicherung eingesetzt. Dazu näheres im folgenden Punkt 19.2.

- Schulunterlagen werden länger aufbewahrt als in der Rechtsverordnung des Bildungsministeriums vom 03.11.86 vorgesehen. So sollen nach der Verordnung Schülerakten und Klassenbücher lediglich 5 Jahre aufbewahrt werden; in dem geprüften Gymnasium waren dagegen nahezu 30 Jahre alte Unterlagen vorzufinden. Unterlagen, deren Aufbewahrungsfrist abgelaufen ist und die demnach nicht mehr zur Aufgabenerfüllung benötigt werden, sind zu vernichten (§ 19 Abs. 3 SDSG). Das Ministerium will prüfen, ob die Aufbewahrungsfristen in der Verordnung geändert werden müssen.

- Die Personalnebenakten über die in der Schule eingesetzten Lehrer sind zu umfangreich. Sie sollen kein Spiegelbild der beim Ministerium geführten Personalakte sein, sondern sich auf das beschränken, was vor Ort zur Aufgabenerledigung erforderlich ist (§ 108 Abs. 2 SBG). Ich halte eine generelle Regelung durch das Ministerium für zweckmäßig.

19.2 Einsatz von Schulverwaltungsprogrammen

Durch Meldungen zum Dateienregister oder im Zusammenhang mit Prüfungen stelle ich immer wieder fest, daß in den saarländischen Schulen eine Vielzahl unterschiedlicher Computerprogramme für verschiedene Schulverwaltungszwecke eingesetzt werden. Generelle Empfehlungen von Seiten der Schulaufsichtsbehörden bestehen offensichtlich nicht, so daß es jeder Schule oder auch dem jeweiligen Schulträger überlassen bleibt, welche Software ausgewählt und beschafft wird. Datenschutzrechtliche Anforderungen, wie sie vor allem in der Rechtsverordnung über die Erhebung, Verarbeitung und sonstige Nutzung personenbezogener Daten in den Schulen vom 03.11.86 (Amtsbl. S. 990) oder im Erlaß des Bildungsministeriums vom 10.06.88 über die automatisierte Datenverarbeitung für Verwaltungszwecke in der Schule festgelegt sind, werden häufig nicht berücksichtigt. So sollte in einem Gymnasium aus dem Landkreis Merzig ein Programm eingesetzt werden, das die Erfassung von Daten vorsieht, deren Speicherung nach der genannten Verordnung nicht zulässig ist (z.B. Asylbewerber, Aussiedler, Beruf, textlich nicht festgelegte Bemerkungen über Schüler). Das Verfahren erlaubt nach dem Bedienerhandbuch ein „intuitives Manövrieren zwischen zusammenhängenden Datensätzen"; es kann „nahezu jede beliebige Liste ... aus den verwalteten Daten erstellt werden".

Dabei ist es Aufgabe der obersten Landesbehörde, für ihren Geschäftsbereich die Ausführung der Rechtsvorschriften über den Datenschutz sicherzustellen (§ 8 Abs. 1 SDSG). Ebenso hat das Ministerium automatisierte Verfahren, mit denen personenbezogene Daten verarbeitet werden, vor ihrem Einsatz in der jeweiligen Schule schriftlich freizugeben (§ 8 Abs. 2 SDSG).

Die Einsatzbedingungen des Schulverwaltungsprogramms, die technischen und organisatorischen Maßnahmen der Datensicherung und die dabei von den beteiligten Bediensteten wahrzunehmenden Pflichten sind in jeder Schule durch eine Dienstanweisung zu regeln. Unter Mitwirkung meiner Dienststelle wurde für ein Berufsbildungszentrum eine Dienstanweisung mit Dateibeschreibungen für die Meldung zum Dateienregister entworfen, die als Muster auch in anderen Schulformen verwendet werden können (siehe auch TZ 4.11).

19.3 Einsicht in Schulchronik

Es wurde die Frage an mich herangetragen, ob im Rahmen heimatgeschichtlicher Forschung Einsicht in eine Schulchronik durch schulfremde Personen genommen werden darf. In dem speziellen Fall enthielt die Chronik auch Bemerkungen über Erkrankungen von Schülern und Lehrern.

Ich halte es für sachgerecht, die Zulässigkeit der Nutzung der in der Schulchronik enthaltenen personenbezogenen Daten unter Zugrundelegung der Vorschriften des Saarländischen Archivgesetzes zu beantworten (die schulrechtlichen Vorschriften enthalten keine Aussagen zu dem nutzungsberechtigten Personenkreis einer Schulchronik). Auch bei den in der Schulchronik enthaltenen personenbezogenen Daten handelt es sich um solche, die für die aktuelle Aufgabenerfüllung der Schule nicht mehr erforderlich, aus kulturellen Gründen aber noch von Bedeutung sind.

Die Einsicht in Archivgut, das sich auf natürliche Personen bezieht, ist im Saarländischen Archivgesetz wie folgt geregelt: Für die Einsichtnahme in Archivunterlagen gelten bestimmte Schutzfristen. Diese endet 30 Jahre nach dem Tod des Betroffenen. Wenn der Todestag nicht feststellbar ist, endet die Schutzfrist 110 Jahre nach der Geburt. Über diese Schutzfristen hinaus kann die Benutzung des Archivgutes eingeschränkt oder versagt werden, soweit schutzwürdige Belange Dritter entgegenstehen (§ 11 Abs. 7 Nr. 3 SArchG).

Es muß also in jedem Einzelfall vor der Entscheidung über die Einsichtsgewährung festgestellt werden, welche personenbezogenen Daten in der Schulchronik enthalten sind. Falls dort Krankheiten von Schülern und Lehrern vermerkt sind, würde ich von einer Einsichtnahme abraten.

Ergänzend habe ich noch ausgeführt, daß ich gegen eine Einsichtnahme dann keine Bedenken hätte, wenn die Schulchronik nur folgende Daten enthielte: Name, Vorname, Jahrgangsstufe und Klasse der Schüler; Name, Vorname, Amts- bzw. Dienstbezeichnung, Fächerverbindung und Verwendung der einzelnen Lehrer, „Angaben über besondere schulische Tätigkeiten und Funktionen einzelner Lehrer, Schüler und Erziehungsberechtigter". Denn dies ist der Datenkatalog, der in einem Bericht der Schule für ein Schuljahr oder mehrere Schuljahre enthalten sein darf (§ 8

Abs. 2 der Verordnung über die Erhebung, Verarbeitung und sonstige Nutzung personenbezogener Daten in den Schulen).

19.4 Studentendaten-Verordnung

In einem weiteren Bereich, in dem in erheblichem Umfang mit personenbezogenen Daten umgegangen wird, wurde ein bisher bestehendes Regelungsdefizit ausgeglichen. Am 1. September 1995 ist die Verordnung über die Erhebung, Verarbeitung und Aufbewahrungsdauer personenbezogener Daten an den Hochschulen des Saarlandes in Kraft getreten (Amtsblatt Seite 846). In dieser Verordnung hat das Ministerium für Bildung, Kultur und Wissenschaft im einzelnen die Daten festgelegt, die von den Studienbewerbern und den Studenten an den Hochschulen des Saarlandes gespeichert werden dürfen. In der Verordnung ist darüber hinaus festgelegt, wie lange die einzelnen Daten gespeichert bleiben dürfen.

Im Rahmen des Anhörverfahrens habe ich das Ministerium darauf hingewiesen, daß die Verordnungsermächtigung im Universitätsgesetz und den anderen Hochschulgesetzen lediglich eine Datenerhebung für Verwaltungszwecke erlaubt und daß die entsprechenden Vorschriften keine Ermächtigungsgrundlage für die Erhebung statistischer Angaben bieten.

Ich habe das Ministerium gebeten, den Datenkatalog daraufhin zu überprüfen, ob sämtliche Angaben des Katalogs von allen Studienbewerbern erhoben werden dürfen oder ob in dem Katalog Daten enthalten sind, die nur von den Bewerbern für bestimmte Studiengänge erhoben werden dürfen.

Es war vorgesehen, daß die Studienbewerber unter dem Gesichtspunkt „Umstände, die einer Immatrikulation entgegenstehen können" Straftaten und die Aberkennung der Fähigkeit zur Begleitung öffentlicher Ämter angeben mußten. Ich habe darauf hingewiesen, daß weder im Universitätsgesetz noch in den anderen Hochschulgesetzen entsprechende Versagungsgründe genannt sind. Das Ministerium ist meiner Argumentation gefolgt und hat die entsprechenden Angaben in der Verordnung gestrichen.

Bedenken hatte ich auch gegen die geforderte Angabe „Krankheiten, die die Gesundheit anderer Studenten gefährden oder den Studienbetrieb ernstlich beeinträchtigen können" geltend gemacht. Zwar ist nach dem Universitätsgesetz und den entsprechenden Vorschriften in den anderen Hochschulgesetzen die Einschreibung zu versagen, wenn der Studienbewerber an einer Krankheit leidet, welche die Gesundheit anderer Studenten ernstlich gefährdet. Ich frage mich allerdings, wie der einzelne Studienbewerber, von dem eine Beantwortung dieser Frage verlangt wird, beurteilen soll, ob er an einer solchen Krankheit leidet. Ich sehe die Gefahr, daß Studienbewerber sich in einem über das Erforderliche hinausgehende Maß offenbaren. Die entsprechende Abfrage ist in der Verordnung nicht mehr enthalten.

19.5 Private PC der Lehrer

Mehrere Eltern von Schülern einer Schule haben sich bei mir über die Speicherung von Schüler- und Elterndaten durch eine Lehrkraft auf deren privatem Laptop beschwert. Auf Nachfrage hat mir die Schulleitung bestätigt, daß der betreffende Lehrer Notizen über Leistungen und Verhalten seiner Schülerinnen und Schüler auf einem privaten Laptop festhalte.

Eine Überprüfung der Rechtslage hat ergeben, daß die Nutzung privater Datenverarbeitungsgeräte, wie etwa PC oder Laptop, mit den im Saarland derzeit geltenden Vorschriften über die Verarbeitung von Schülerdaten nicht vereinbar ist. Schülerdaten dürfen nur auf in der Schule befindlichen oder anderen automatischen Datenverarbeitungsanlagen des Schulträgers verarbeitet werden (§ 5 Abs. 1 der Verordnung über die Erhebung, Verarbeitung und sonstige Nutzung personenbezogener Daten in den Schulen). Aber nicht nur die Tatsache der Nutzung eines privaten Laptop gab Anlaß zur Kritik, sondern auch die Art der gespeicherten Daten. Nach einem Erlaß des ehemaligen Ministeriums für Kultus, Bildung und Wissenschaft dürfen Leistungsdaten nur ausnahmsweise automatisiert verarbeitet werden, nämlich nur soweit dies zur Ermittlung von Qualifikationen des einzelnen Schülers dient, die aufgrund bestehender Vorschriften ausschließlich auf der Grundlage der Anwendung mathematischer Algorithmen gefunden werden und auch nur für Schüler der Gesamtschulen und der Jahrgangsstufen 12 und 13 des Gymnasiums. Sonstige Schülerdaten, die nicht Leistungsdaten sind, dürfen ebenfalls nicht uneingeschränkt ge-

speichert werden. So dürfen personenbezogene Daten, deren Kenntnis schutzwürdige Belange der Betroffenen beeinträchtigen könnte, nicht in automatischen Datenverarbeitungsanlagen verarbeitet werden.

Der Leiter der betroffenen Schule hat daraufhin alle Lehrer seiner Schule schriftlich darauf hingewiesen, daß die Speicherung personenbezogener Leistungs- und Verhaltensdaten von Schülern auf privaten Datenverarbeitungsgeräten unterbleiben muß und daß bereits vorhandene Daten umgehend zu löschen sind.

Ich gehe davon aus, daß der von den Eltern an mich herangetragene Fall kein Einzelfall ist. Der Einsatz privater Datenverarbeitungsgeräte ist bei Lehrern durchaus üblich, und es ist zu vermuten, daß hierbei auch personenbezogene Daten von Schülern verarbeitet werden. Ich habe deshalb das zuständige Ministerium für Bildung, Kultur und Wissenschaft aufgefordert darauf hinzuwirken, daß die von ihm gegebenen Regelungen über den Umgang mit automatischer Datenverarbeitung in den Schulen eingehalten werden. Wegen der vielfältigen Gefahren, die die Nutzung privateigener Datenverarbeitungsgeräte durch Lehrer mit sich bringt und denen bisher nicht ausreichend entgegengewirkt wird, etwa technisch-organisatorische Datensicherungsmaßnahmen, Kontrolle der Datenschutzbestimmungen durch die Schulleitung und den Landesbeauftragten für Datenschutz, Einsatz nicht genehmigter Programme, muß ich auf dem Verzicht privater Geräte bestehen. Dies gilt jedenfalls solange, als die Bedingungen für die Nutzung privater Geräte nicht im einzelnen geregelt sind.

20 Öffentlicher Dienst

20.1 Neue Regelungen für Personalakten

Das Gesetz zur Änderung dienstrechtlicher Vorschriften vom 21.06.1995 (Amtsblatt S. 794) hat in das Saarländische Beamtengesetz neue Regelungen für die Verwaltung von Personalakten eingefügt (§§ 108 ff SBG). Mit dieser Anpassung an das bereits 1992 verabschiedete Rahmenrecht des Bundes werden die Persönlichkeitsrechte der Betroffenen gestärkt

und wichtige Klarstellungen für die Verarbeitung von Personaldaten getroffen. Folgende Punkte sind besonders herauszustellen:

- Es ist festgelegt, welche Unterlagen in die Personalakten gehören und welche getrennt davon als Sachakten zu führen sind.

- Die Personalakten sind vertraulich zu behandeln. Zugang zu Personalakten und - im automatisierten Verfahren - Zugriff auf Personalaktendaten dürfen nur Beschäftigte erhalten, die mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist. Fachvorgesetzte dürfen nicht in die Personalakten Einsicht nehmen.

- Die Beihilfe soll in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden. Die bisher übliche Bearbeitung in der Personalabteilung oder im Personalamt ist somit grundsätzlich nicht mehr erlaubt (vgl. auch unten TZ 20.6).

- Das Einsichtsrecht der Betroffenen beschränkt sich nicht nur auf die eigentlichen Personalakten, sondern auf alle Unterlagen (ausgenommen Sicherheitsakten) mit Personaldaten.

- Die Rechte auf Entfernen von Unterlagen aus Personalakten wurden verbessert. So sind z.B. nunmehr auch Vorgänge mit Beschwerden oder Behauptungen, die für den Beamten nachteilig werden können, auf seinen Antrag nach 3 Jahren aus den Personalakten zu entfernen und zu vernichten; dies gilt nicht für Beurteilungen.

- Personalakten sind nach Ablauf der im einzelnen festgelegten Fristen - sofern sie nicht vom zuständigen öffentlichen Archiv übernommen werden - zu vernichten. So sind Beihilfeunterlagen bereits 3 Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, zu vernichten.

- Sollen Personalaktendaten in Dateien verarbeitet werden, sind besondere Zulässigkeitsvoraussetzungen zu beachten. Vor allem die Transparenz der Verarbeitung gegenüber den Betroffenen wird verbessert: bei der erstmaligen Speicherung und bei wesentlichen Änderungen sind sie über die Art der Daten zu informieren. Ferner sind u.a. die

Verarbeitungsformen automatisierter Personalverwaltungsverfahren einschließlich des Verwendungszweckes den Betroffenen allgemein bekanntzugeben.

Ich habe beim Ministerium des Innern angeregt, die aus dem Jahre 1968 stammenden Verwaltungsvorschriften über die Führung der Personalakten zu überarbeiten, um die praktische Umsetzung der neuen Regelungen in den Personalverwaltungen sicherzustellen.

20.2 Unnötige Bekanntgabe von Personalinformationen in einer Organisationsverfügung

Ein bei einer saarländischen Stadt beschäftigter Beamter hatte in einem Rechtsstreit gegen seinen Dienstherrn teilweise obsiegt, so daß der Bürgermeister Verwaltungsgliederung und Geschäftsverteilung ändern mußte. In der Organisationsverfügung wurde der Prozeßverlauf im einzelnen beschrieben, z.B. in welchen Punkten der namentlich bezeichnete Beamte unterlegen ist, welchem Antrag stattgegeben wurde und welche organisatorischen und personellen Konsequenzen aus der Entscheidung zu ziehen sind. Der Beamte beschwerte sich bei mir darüber, daß diese Personaldetails in einer Verfügung dargestellt wurden, die innerhalb der Stadtverwaltung einem größeren Kreis von Mitarbeitern bekanntgegeben wurde.

Ich habe diese Weitergabe von Personaldaten beanstandet. Es war nicht erforderlich, in der Organisationsverfügung auf Einzelheiten aus dem Beamtenrechtsstreit in personenbezogener Form einzugehen. Vielmehr hätte es ausgereicht, die organisatorischen Maßnahmen und die sich daraus ergebenden personellen Umsetzungen darzustellen. Die Gründe, die zu der Organisationsentscheidung geführt haben, hätten in einem internen Vermerk beschrieben werden können.

20.3 Automatisierte Verarbeitung von Fehlzeiten

Der Personalrat hatte mich darüber informiert, daß bei einem Ministerium Daten über die Fehlzeiten der Beschäftigten ohne seine Zustimmung au-

tomatisiert verarbeitet werden. Bei einem Besuch der Personalabteilung habe ich festgestellt, daß seit etwa einem Jahr an einem PC unter Einsatz eines Tabellenkalkulationsprogrammes die nicht urlaubsbedingten Abwesenheitstage der Mitarbeiter - auch für die zurückliegenden Jahre - erfaßt wurden. Das Ministerium sah in dieser Verarbeitung eine bloße Fortführung der bisherigen manuellen Kartei.

Die Erfassung von Fehlzeiten ist für Zwecke der Personalverwaltung erforderlich; sie ist daher auch datenschutzrechtlich grundsätzlich zulässig. Bei Einsatz eines automatisierten Verfahrens sind jedoch bestimmte Regeln einzuhalten:

- Das Mitbestimmungsrecht des Personalrates ist zu wahren (§ 84 SPersVG). Bei Nichtbeteiligung ist auch aus der Sicht des Datenschutzes eine Zulässigkeitsvoraussetzung nicht erfüllt.

- Formelle Freigabe des Verfahrens nach Beteiligung des Landesbeauftragten für Datenschutz (§ 8 SDSG).

- Information der betroffenen Mitarbeiter (§ 108 g SBG).

Geteilt habe ich die Bedenken des Personalrates dagegen, daß in einer Liste die Abwesenheitszeiten von 4 Jahren zusammengestellt und den jeweiligen Abteilungen zugeleitet wurden. Die Abteilungsleiter sollten „in den Fällen, in denen Bedienstete besonders viele Krankheitstage aufweisen, der Sache nachgehen und mit den Bediensteten ein persönliches Gespräch hinsichtlich der vielen Fehlzeiten führen". Wenn solche Personalgespräche als geeignetes Mittel zur Senkung des Krankenstandes angesehen werden, sollten sie von der „neutraleren", für Personalentscheidungen zuständigen Personalverwaltung und nicht vom Fachvorgesetzten geführt werden.

Überdies war es nicht notwendig, die Daten sämtlicher Mitarbeiter weiterzugeben, wenn nur bei denen mit „besonders vielen Krankheitstagen" etwas veranlaßt werden sollte.

Das Ministerium hat von der automatisierten Verarbeitung Abstand genommen. Hinsichtlich der Führung der Personalgespräche ist es meiner Empfehlung gefolgt.

20.4 Veröffentlichung der Ungültigkeitserklärung von Dienstausweisen

Häufig waren im Amtsblatt des Saarlandes folgende Veröffentlichungen zu lesen: „Der Dienstausweis des (Dienstbezeichnung, Name, Vorname, Geburtsdatum) ist verlorengegangen; er wird hiermit für ungültig erklärt."

Was sollte mit dieser Bekanntgabe personenbezogener Daten bezweckt werden? Es ist nicht bekannt, ob jemals aufgrund der Veröffentlichung im Amtsblatt die mißbräuchliche Benutzung eines gestohlenen oder verlorengegangenen Dienstausweises verhindert wurde.

Das Ministerium des Innern und die meisten anderen Ressorts haben bereits seit längerem die Veröffentlichungen eingestellt, weil keinerlei Resonanz festzustellen war. Das Ministerium der Justiz hat auf meine Veranlassung hin inzwischen ebenfalls zugestimmt, auf die Bekanntgabe personenbezogener Daten zu verzichten.

20.5 Meldung von Behinderungen beim Dienstherrn

Die Schwerbehinderung wird gegenüber dem Arbeitgeber oder Dienstherrn durch die Vorlage des Schwerbehindertenausweises nachgewiesen (§ 4 Abs. 5 SchwbG). Der Bescheid des Landesamtes für Soziales und Versorgung, in dem die Behinderungen im einzelnen aufgeführt sind, ist nicht vorzulegen. Personen, deren Behinderungsgrad weniger als 50% beträgt und die daher keinen Ausweis erhalten, legen für die Gewährung des Zusatzurlaubs eine Bescheidkopie vor, in der Angaben über die Art der Erkrankungen geschwärzt oder beim Fotokopieren abgedeckt werden.

Die Schwerbehindertenvertretung bei der Polizei hat mich darüber informiert, daß dort durch eine Verfügung vom Juni 1994 angeordnet wurde, dem Polizeiärztlichen Dienst eine „ungeschwärzte Ausfertigung" der Bescheide zur „Überprüfung der Verwendungsfähigkeit des Beamten" zu übersenden. Die Schwerbehindertenvertretung sah darin eine Selbstanzeige zur Prüfung der Polizeidienstunfähigkeit.

Das Ministerium des Innern hat aufgrund meiner Intervention die entsprechende Passage der Verfügung aufgehoben.

20.6 Beihilfeberechnung durch die Ruhegehalts- und Zusatzversorgungskasse des Saarlandes (RZVK)

Der Landesbeauftragte für Datenschutz unterstützt seit Jahren Bestrebungen, die Beihilfebearbeitung von der Personalsachbearbeitung zu trennen, um sicherzustellen, daß keine Informationen aus Beihilfeanträgen (Arzt- und Heilmittelrechnungen mit Diagnosen, Arzneimittelverordnungen) in Personalentscheidungen einfließen. Mit einer Verlagerung der Beihilfebearbeitung auf eine externe, öffentliche Stelle soll ein Zustand erreicht werden, der in etwa vergleichbar ist dem Verhältnis zwischen Arbeitgeber und Krankenkasse. Dem Arbeitgeber wird nicht bekannt, wegen welcher Krankheiten der Arbeitnehmer welche ärztlichen Leistungen in Anspruch nimmt.

Für den Bereich der Landesverwaltung wurde bereits 1990 eine zentrale Beihilfestelle bei der Oberfinanzdirektion eingerichtet. Seit Anfang 1996 kann nunmehr die RZVK ebenfalls die Beihilfeberechnung für andere öffentliche Stellen übernehmen. Damit wird insbesondere den Gemeinden eine Alternative geboten, die das in dem neuen § 108 a SGB aufgenommene Trennungsgebot der Beihilfe- von der Personalbearbeitung nicht realisieren können (vgl. auch oben TZ 20.1).

Mit der Verlagerung der Berechnung auf Dritte sind jedoch nicht alle Probleme gelöst. Auch für die Bearbeitung der Widersprüche und Klagen gegen Beihilfebescheide ist beim Dienstherrn eine Zuständigkeitsregelung zu finden, die den Anforderungen des § 108 a SBG Rechnung trägt.

21 Kommunikation und Medien

Weiterentwickelte technische Möglichkeiten in Kommunikation und Medienwelt gaben im Zeitraum dieses Berichts erneut Anlaß zu Überlegungen, technische und rechtliche Bedingungen für eine datenschutzgerechte Ausgestaltung zu setzen. Auch umgekehrt führten uns Bestrebungen, den rechtlichen Rahmen - etwa bei der Liberalisierung der Post- und Telekommunikationsdienste - zu ändern, zu der Sorge, jedenfalls den bestehenden Datenschutzstandard zu erhalten. Denn mit veränderter Technik wandelt sich auch das Nutzungsverhalten der Bürger, die sich der neuen

Kommunikationsmedien zuwenden und dabei eine Vielzahl zusätzlicher Datenspuren hinterlassen.

Ich habe mich damit überwiegend gemeinsam mit den übrigen Datenschutzbeauftragten befaßt. Die gemeinsame Beurteilung liegt schon deswegen nahe, weil es sich großenteils um allgemeine Entwicklungen oder Regelungsbemühen auf Bundes- oder auf europäischer Ebene handelt, in deren Bewertung die Landesbeauftragten im Rahmen ihrer gegenseitigen Zusammenarbeit eingeschaltet werden. Sie können so ihre Kenntnisse sowie Erfahrungen bei den örtlichen Stellen einbringen, für deren Kontrolle sie zuständig sind.

Für den Bereich der Telekommunikation war schon in früheren Berichten auf die Absicht verwiesen worden, mit einer sog. ISDN-Richtlinie auf europäischer Ebene bereichsspezifische Regelungen für den Datenschutz in Telekommunikationsnetzen (einschließlich Mobilfunk) zu erreichen (zuletzt 15. TB TZ 16.9). Mit Verabschiedung des gemeinsamen Standpunkts im Ministerrat der Union ist dieses Vorhaben weiter vorangetrieben; angestrebt wird, nach Stellungnahme des Europäischen Parlaments auf eine Umsetzung der Richtlinie zeitgleich mit der allgemeinen Datenschutzrichtlinie hinzuwirken, also bis Herbst 1998.

21.1 Telekommunikationsgesetz

Innerstaatlich ist vor allem auf die Liberalisierung der Telekommunikation zu verweisen, die über die Privatisierung (Postreform II) auch auf den Wegfall der Monopolstellung in wichtigen Bereichen zielt (Postreform III). Kernstück des rechtlichen Rahmens hierfür ist das Telekommunikationsgesetz (TKG), das im Sommer 1996 in Kraft getreten ist.

Mit einer Entschließung (Anlage 20) vom 9./10. 11. 1995 hatten die Datenschutzbeauftragten im Vorfeld zum damaligen Entwurf eingefordert, bei der Neugestaltung des Telekommunikationssektors Datenschutz als gleichberechtigtes Regelungsziel festzuschreiben. Die Empfehlung drängt darauf, die Prinzipien Datenvermeidung und strikte Begrenzung auf das erforderliche Ausmaß der Datenverarbeitung zu beachten und grundsätzlich - mindestens alternativ - anonymen Zugang zu eröffnen. Abrech-

nungs- und Verbindungsdaten müssen eng an ihre Zweckbestimmung gebunden bleiben.

Das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis müssen für alle Netzbetreiber und Diensteanbieter ungeachtet ihrer Rechtsform und ihrer Kundenstruktur (z.B. sog. Corporate Networks) einheitlich auf einem hohen Niveau gesichert sein.

Kunden bzw. Teilnehmer müssen die Verarbeitungsvorgänge im TK-Bereich überschauen und Nutzungsrisiken erkennen können; über Widerspruchsmöglichkeiten sind sie eingehend aufzuklären. (Verschiedene Aktionen der Telekom AG, für deren Kontrolle allerdings der Bundesbeauftragte für den Datenschutz zuständig ist, haben gerade insoweit im Berichtszeitraum zu verärgerten Eingaben geführt.)

Nur ein Teil der umfangreichen Vorschläge ist im Gesetzgebungsverfahren aufgegriffen worden. Immerhin ist mit dem verabschiedeten Telekommunikationsgesetz ein beachtlicher Grundrahmen für den Datenschutz gesetzt, der noch näherer Ausformung bedarf. Mit dem TKG gilt auch das Fernmeldegeheimnis nicht mehr allein für den öffentlichen Fernmeldeverkehr.

Nicht unproblematisch erscheint als Einzelvorschrift, daß die Telekommunikationsdienst-Anbieter Strafverfolgungs- und Sicherheitsbehörden in automatisch abrufbarer Form die Bestandsdaten der Teilnehmer verfügbar zu machen haben, ohne daß näher begrenzt wird, unter welchen Bedingungen diese Adreßdaten genutzt werden können. Mit vergleichbaren Verpflichtungen, wie sie gegenwärtig auch in weiteren (Bundes)-Gesetzgebungsverfahren vorgesehen sind, können diese Behörden weit mehr als nur die Adreßdaten der Teilnehmer erhalten, ohne daß diese oder die Dienstanbieter davon erfahren. Auf die Entschließung der Datenschutzbeauftragten zu neuen Eingriffsbefugnissen zur Strafverfolgung im Informations- und Telekommunikationsbereich wurde bereits hingewiesen (TZ 12.8).

21.2 Telekommunikationsdienstunternehmen - Datenschutzverordnung (TDSV)

Fast zeitgleich, aber noch auf Basis der ehemaligen rechtlichen Grundlage vor dem TKG und deshalb ohne Geltung für interne Netze (Corporate Networks), hat die Bundesregierung in der Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (TDSV), Einzelheiten für die Beachtung des informationellen Selbstbestimmungsrechts im Fernmeldeverkehr bestimmt. Auch hierzu hatten die Datenschutzbeauftragten im Rechtsetzungsverfahren eingehend Stellung genommen und die Grundpositionen in einer Entschließung deutlich gemacht, die nur zum Teil in die endgültige Fassung der Verordnung eingeflossen ist (Anlage 21). Gleichwohl erschien aus Datenschutzsicht sinnvoller, zunächst mit der TDSV verbindliche Detailregelungen zu schaffen als zuzuwarten, bis sie aufgrund des TKG getroffen werden können.

21.3 Datenschutz bei Online-Diensten

Für viele wird immer selbstverständlicher, die vielfältigen und weiter zunehmenden Angebote zu nutzen, die meist mit der „normalen" Telekommunikation verbunden sind, aber hierüber hinausgehen; die Anwendungsspanne reicht von elektronischen Unterhaltungs- und Bildungsangeboten bis zur Erledigung von Einkäufen, Bankgeschäften und Tele-Arbeit. Gemeinsam ist allen, daß in großer Zahl Einzeldaten anfallen, die über das Mediennutzungsverhalten Aufschluß über intimste Daten geben können.

Daß bei einem neuen rechtlichen Rahmen für diese Dienste Datenschutz eine unverzichtbare Forderung sein muß, liegt auf der Hand. Dies war im Grundsatz auch unbestritten bei Bund und Ländern, die beide für einander teilweise überschneidende Regelungsbereiche über die Gesetzgebungskompetenz verfügen. Auf Länderseite konnte mit dem Bildschirmtext-Staatsvertrag bereits an eine Vorläufer-Regelung angeknüpft werden.

In einer Entschließung vom 29. 4. 1996 (Anlage 22) haben die Datenschutzbeauftragten noch einmal die Forderungen zusammengefaßt und

präzisiert, die den Regelungen auf der jeweils zutreffenden Normebene zugrunde gelegt werden sollten.

21.4 Teledienstegesetz (TDG); Teledienstedatenschutzgesetz (TDDSG)

Auf Bundesseite besteht die Absicht, in einem Artikelgesetz umfassend einen Ordnungsrahmen für die neuen Medien zu setzen; hierzu gehören auch Vorschriften über elektronische Signatur (vgl. TZ 4.4). Nach einer Verständigung mit den Ländern wird sich der Datenschutz vor allem im Bereich der Individualkommunikation (z.B. electronic Mail; Buchungsdienste; Datendienste; Videokonferenzen; Telespiele; Telebanking; Tele-Arbeit; Tele-Medizin) nach bundesrechtlicher Vorgabe richten, die neben der Ordnung der übrigen Rechtsbereiche in einem spezifischen „Teledienstedatenschutzgesetz" niedergelegt werden soll. Inhaltlich wird aber eine Abstimmung mit der Länderregelung angestrebt.

Ich hatte schon auf den - leider aufgegebenen - Ansatz in einer früheren Entwurfsfassung hingewiesen (TZ 3), durch Festlegen von bestimmten Datenschutzstandards und Prämierung ihres Konzepts Möglichkeiten für die Anbieter zu schaffen, für ihre Angebote, die sie erfüllen, um größere Akzeptanz zu werben.

21.5 Mediendienste-Staatsvertrag

Für den den Ländern zur Gesetzgebung vorbehaltenen Regelungsbereich, der sich im wesentlichen auf die Massenkommunikation und vergleichbare Verteildienste bezieht, soll in einem Staatsvertrag ländereinheitlich ein Rechtsrahmen gesetzt werden.

Die grundsätzlichen Forderungen der Entschließung zu den Online-Diensten (TZ 21.3) gelten auch hier; ich habe sie dem Landtag und der Staatskanzlei zugeleitet. Die angestrebte Übereinstimmung mit der bundesrechtlichen Regelung (Teledienstedatenschutzgesetz) ist sinnvoll. Zweifel ergeben sich allerdings, soweit auch für diesen Bereich eine bundesrechtliche Datenschutzkontrolle bestimmt werden soll.

21.6 Landesrundfunkgesetz

Im Vorgriff hierauf und zur Sicherung von Standortinteressen wurde auch das saarländische Landesrundfunkgesetz um Vorschriften über Modellversuche erweitert. Bereits zuvor hatte die Landesanstalt für das Rundfunkwesen, die über die Nutzung von Fernseh- und Hörfunkfrequenzen sowie Kabelnetzen zu entscheiden hat, mit der Staatskanzlei und der Deutschen Telekom AG die Durchführung eines „Multimedia-Pilotprojekts Saarland" vereinbart, das sich auf die digitale (Weiter-)Verbreitung von Hörfunkprogrammen, neuen programmbegleitenden Rundfunkdiensten und sonstigen programmunabhängigen Datendiensten über digitale terrestrische Hörfunkfrequenzen (Digital Audio Broadcasting System, DAB) bezieht. Nach Ausschreibung befand die LAR im November 1996 über die Verteilung der Übertragungsmöglichkeiten für die zunächst bis Ende 1998 befristete Nutzung.

Die gesetzliche Regelung im Landesrundfunkgesetz läßt indes über diese Nutzung terrestrischer (Hörfunk-)Frequenzen hinaus weitere Dienste in Modellvorhaben zu, ohne deren Inhalt näher zu bestimmen. Deshalb ist auch nicht vorab zu erkennen, ob und inwieweit für die Teilnehmer an den Versuchen Gefährdungen ihres informationellen Selbstbestimmungsrechtes etwa dadurch entstehen, daß die Nutzung über den erforderlichen Umfang hinaus „Datenspuren" legt oder die Verarbeitung unzureichend gesichert wird. Bei meiner Beteiligung am Gesetzgebungsverfahren konnte ich nur - aber immerhin - erreichen, daß die für Rundfunkdienste geltenden Datenschutzvorschriften auch auf rundfunkähnliche (an die Allgemeinheit gerichtete) Dienste erstreckt werden. Spezielle Regelungen im übrigen fehlen; für die Beteiligung des Saarländischen Rundfunks an Modellvorhaben verzichtet der Gesetzgeber auf jegliche normativen Vorgaben und verläßt sich auf eine „Vereinbarung" mit der LAR.

Es ist zu hoffen, daß mit Inkrafttreten des vorgesehenen Länderstaatsvertrags sowie des künftigen Teledienstegesetzes des Bundes klarere Zielvorgaben und konkretere Schutzbestimmungen festgelegt werden, die dann auch für saarländische Modellvorhaben gelten.

21.7 Führt das digitale Fernsehen zum „gläsernen Zuschauer"?

1996 war in Deutschland das Startjahr für das „digitale Fernsehen". Bürger können sich unabhängig von festgelegten Sendeterminen der Rundfunkveranstalter gewünschte Angebote ins Wohnzimmer holen. Mehr noch als beim Abonnementfernsehen, bei dem in der Regel dem Anbieter nur die Kundenbeziehung als solche bekannt wird, fallen für Nutzung und Abrechnung eine Vielzahl neuer Daten an. Bei Systemen, bei denen Kunden für die einzelnen empfangenen Sendungen bezahlen müssen, lassen sich individuelle Vorliebe, Interessen und Sehgewohnheiten registrieren und zu Mediennutzungsprofilen einzelner Zuschauer verdichten.

Auf die Gefahren weist eine Entschließung vom 22./23. 10. 1996 (Anlage 23) hin und fordert, jedenfalls alternativ Möglichkeiten eines anonymen Zugangs einzurichten.

22 Situation der Dienststelle

22.1 Personelle Situation

Nach wie vor unzureichend ist die personelle Ausstattung der Dienststelle; bereits im letzten Tätigkeitsbericht ist hierauf eingehend hingewiesen worden (15. TB TZ 1.2).

Unverändert fehlt es am gesicherten Ersatz für eine langfristig erkrankte Mitarbeiterin und der notwendigen Unterstützung im Geschäftsstellen-, Querschnitts- und Technikbereich. Die eigentliche Aufgabe kommt damit zu kurz. Die öffentlichen Stellen in der Kommunikationstechnik datenschutzrechtlich zu beraten und zu prüfen, wird immer wichtiger, ohne zusätzliche personelle Hilfe aber immer schwieriger.

Im gebotenen Maß ist die Absicherung des informationellen Selbstbestimmungsrechtes durch unabhängige Kontrolleinrichtungen, die das Bundesverfassungsgericht für zwingend erforderlich bezeichnet, mit dem vorhandenen Personalbestand nicht möglich, weil dies ein zu hohes Maß an Selbstbeschränkung in der Prüfung erzwingt. Den Mitarbeitern muß ich ein großes Arbeitspensum auferlegen, ohne ihre Motivation mit einer an-

gemessenen Bewertung stützen zu können. An der hilfreichen, weitgehend zwingend notwendigen Zusammenarbeit mit den Kollegen der übrigen Länder und dem Bundesbeauftragten kann ich vielfach nur passiv teilnehmen.

Selbstverständlich erkenne ich an, daß das notwendige Sparbemühen im Landeshaushalt auch den Personalbereich nicht ausnehmen darf. Aber nur von einer ausreichenden Basis her sind Einschnitte vertretbar. Rückläufige Personalstärken bei anderen Landesbehörden können kein Maßstab sein, im Gegenteil: das Verlagern von Tätigkeiten auf (oft nur formal) privatisierte Stellen und zunehmende Auftragsdatenverarbeitung vermindern den Kontroll- und Beratungsbedarf beim LfD nicht; neue automatisierte Verfahren, die menschliche Arbeitskraft unterstützen und teilweise ersetzen, vergrößern ihn. Allein die Beteiligung vor Freigabe eines jeden Verfahrens (§ 8 Abs. 2 SDSG) bindet wesentliche Kapazitäten.

Das Bemühen des Landtagspräsidiums, hier eine Verbesserung zu erreichen, will ich gern betonen. Leider ist aber der Haushaltsgesetzgeber erneut dem Vorschlag der Landesregierung gefolgt, die diesen drängenden Bedarf nicht anerkennt.

22.2 Technische Ausstattung; Internet-Angebot

Sachlich wird es darauf ankommen, vor allem in der Kommunikationstechnologie Anschluß an die Entwicklung in den öffentlichen Stellen zu halten, um kompetent Kontrolle und Beratung durchführen zu können. Daß gerade hier künftig ein Schwerpunkt der Arbeit liegen muß, hatte ich bereits dargestellt (TZ 3.2 und 4).

Dem dienen der Aufbau eines lokalen Netzes in der Dienststelle, die aktive Mitwirkung an Planung und Einrichtung eines entsprechenden Netzwerkes im Bereich der Landesverwaltung und auch die eigene Nutzung von Möglichkeiten, mit anderen Stellen über elektronische Netze zu kommunizieren.

So können wir inzwischen auch das Internet als Transport- und Publikationsmedium nutzen. Hierfür hat mir die Landesregierung auf ihrem Rechner, auf dem sie ihre eigenen Informationen anbietet, einen Speicherbe-

reich zur Verfügung gestellt. In meinem Angebot sind derzeit das Saarländische Datenschutzgesetz und spezifische Datenschutzregelungen aus anderen landesrechtlichen Rechtsvorschriften im Wortlaut verfügbar. Weiter enthalten sind Materialien zum Datenschutz wie Dienstanweisungen, Orientierungshilfen und Checklisten, die für die Arbeit der öffentlichen Stellen von Interesse sind, ferner Verweise auf andere Datenschutzangebote. Die im Bericht genannten Entschließungen, Orientierungshilfen usw. sind auf diesem Weg abrufbar.

Nicht allein im Verkehr mit öffentlichen Stellen kann dieser Kommunikationsweg genutzt werden. Informationen von allgemeinem Interesse, deren Angebot schrittweise weiter ausgebaut wird, stehen auf diesem Weg auch Privaten offen. Viele Dokumente liegen in einem Textsystemformat vor, so daß sie unmittelbar im eigenen Textsystem weiterverwendet werden können. Dadurch wird auch der Versand umfangreicher Kopien oder von Disketten entbehrlich.

Das Internet-Angebot ist erreichbar über:

www.saarland.de/dschutz/ LfD.html

Zur Nutzung moderner Kommunikationsformen habe ich auch eine e-Mail-Adresse eröffnet, über die Bürger und Behörden in einfachen Fällen Kontakt aufnehmen können. Auch in diesem Zusammenhang weise ich allerdings darauf hin, daß der e-Mail - Versand dem Versenden von Postkarten entspricht, Vertraulichkeit demgemäß nicht gesichert ist. Mitteilungen vertraulichen Charakters sollten verschlüsselt oder per Briefpost zugeleitet werden.

Die e-Mail-Adresse des LfD-Saarland lautet:

lfd-saar@t-online.de

Anlage 1

52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996

Kurzbericht zum TOP „Datenschutz durch Technik“

Datensparsamkeit durch moderne Informationstechnik (Datenvermeidung, Anonymisierung und Pseudonymisierung)

Die zunehmende Verbreitung, Nutzung und Verknüpfbarkeit von Informations- und Kommunikationstechnik bringt mit sich, daß jeder Benutzer immer mehr elektronische Spuren hinterläßt. Das wird dazu führen, daß er über Art, Umfang, Speicherort, Speicherdauer und Verwendungszweck der vielen über ihn gespeicherten Daten keine Kontrolle mehr hat, so daß die Gefahr des Mißbrauchs und der Zusammenführung zu komplexen Persönlichkeitsprofilen ständig zunimmt.

Dieser Gefahr kann dann begegnet werden, wenn in Zukunft die Frage nach der Erforderlichkeit personenbezogener Daten im Vordergrund steht, wobei Datensparsamkeit bis hin zur Datenvermeidung angestrebt werden muß. Durch die Nutzung neuer Möglichkeiten der modernen Informations- und Kommunikationstechnik (IuK-Technik) ist es in vielen Anwendungsfällen möglich, den Umgang mit personenbezogenen Daten zu reduzieren bis hin zur vollständigen Vermeidung. Auf diese Weise kann das Prinzip **„Datenschutz durch Technik“** umgesetzt werden. Datensparsamkeit und Datenvermeidung werden sich dabei auch zunehmend als Wettbewerbsvorteil erweisen.

Ausgehend von einer Untersuchung des niederländischen und der kanadischen Datenschutzbeauftragten zum sogenannten **Identity Protector** beschäftigen sich derzeit die Datenschutzbeauftragten des Bundes und der Länder intensiv mit der Formulierung von Anforderungen zur datenschutzfreundlichen Ausgestaltung von IuK-Technik. Schon die Sommerakademie in Kiel zeigte unter dem Motto „Datenschutz durch Technik - Technik im Dienste der Grundrechte“ Wege zur Wahrung der Persönlichkeitsrechte der Bürger auf. Einige datenvermeidende Technologien wie die anonyme, vorausbezahlte Telefonkarte sind bereits seit längerer Zeit allgemein akzeptiert. Erste

Ansätze der Datenvermeidung auf gesetzgeberischer Ebene sind im Entwurf zum Teledienstegesetz und zum Mediendienstestaatsvertrag enthalten.

Der Arbeitskreis "Technische und organisatorische Datenschutzfragen" erarbeitet im Auftrag der Konferenz der Datenschutzbeauftragten des Bundes und der Länder einen Bericht mit Vorschlägen und Empfehlungen, wie unter Nutzung der modernen Datenschutztechnik das Prinzip der Datenvermeidung umgesetzt werden kann. Dabei werden Begriffe wie Anonymisierung und Pseudonymisierung eine zentrale Rolle spielen. Bei der Erarbeitung des Berichtes werden Experten aus Wissenschaft und Forschung hinzugezogen, um den aktuellen Stand der Technik berücksichtigen zu können. Auch Vertreter der Wirtschaft werden einbezogen, damit die Umsetzung der Vorschläge der Datenschutzbeauftragten als zukünftiger Wettbewerbsvorteil erkannt wird.

Während der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder wird vom Arbeitskreis "Technische und organisatorische Datenschutzfragen" ein Zwischenbericht zum Thema vorgelegt. Der umfassenden Darstellung des gesamten Problemkreises wird eine so große Bedeutung beigemessen, daß noch weitere Recherchen und die intensive Einbeziehung externer Fachleute erforderlich sind, um zukunftsweisende und realistische Empfehlungen geben zu können.

Anlage 2

Entschließung der Datenschutzbeauftragten
des Bundes und der Länder
vom 13. Oktober 1995

Datenschutz bei elektronischen Geldbörsen und anderen kartengestützten Zahlungssystemen

Die Datenschutzbeauftragten des Bundes und der Länder halten es für dringend erforderlich, daß bei kartengestützten Zahlungssystemen, die zunehmend in Konkurrenz zum Bargeld treten, datenschutzfreundliche Verfahren eingesetzt werden. Dabei bietet es sich an, vor allem Guthabenkarten zu verwenden. Es sollten nur solche Clearingverfahren eingesetzt werden, die weder eine individuelle Kartennummer benutzen noch einen anderen Bezug zum Karteninhaber herstellen.

Sowohl im öffentlichen Personennahverkehr als auch bei der Deutschen Bahn AG können Fahrscheine bargeldlos erworben werden. Auch Autofahrer können auf Bargeld verzichten: Beim Parken, beim Tanken, künftig auch bei der Benutzung von Autobahnen wird verstärkt auf elektronisches Bezahlen zurückgegriffen. Immer mehr Telefone und Warenautomaten werden auf bargeldlose Zahlungsverfahren umgestellt, so daß viele Artikel des täglichen Bedarfs elektronisch bezahlt werden können. Von Kreditinstituten wird die Kombination verschiedener Anwendungen auf einer Karte angestrebt, z.B. mit einer Kombination der Bezahlung für den öffentlichen Nahverkehr, Parkgebühren und Benutzungsentgelte für öffentliche Einrichtungen.

Zum elektronischen Bezahlen werden entweder Kreditkarten, Debitkarten oder Guthabenkarten eingesetzt. Bei Kredit- und Debitkarten werden sämtliche Zahlungsbeträge verbucht, dem Käufer in Rechnung gestellt, auf den Kontoauszügen ausgedruckt und für mindestens 6 Jahre gespeichert. Dagegen wird bei Guthabenkarten im voraus ein Guthaben eingezahlt und bei jeder einzelnen Zahlung das Guthaben entsprechend herabgesetzt; die Zahlungsbeträge müssen keinem Käufer zugeordnet werden.

Beim elektronischen Bezahlen entstehen sehr unterschiedliche Datenschutzrisiken. Bei Kredit- und Debitkarten besteht die Gefahr, daß die aus Abrechnungsgründen gespeicherten personenbezogenen Daten ausgewertet und zweckentfremdet genutzt werden: Informationen über den Kauf von Fahrscheinen oder über die Nutzung von Autobahnen können zu Bewegungsprofilen verdichtet werden. Das Konsumverhalten

des Einzelnen wird bis ins Detail nachvollziehbar, falls auch Kleineinkäufe am Kiosk nachträglich abgerechnet werden. Durch den Datenverkauf für Werbung und Marketing können sich weitere Risiken ergeben. Demgegenüber kann bei der Verwendung von Guthabenkarten auf das Speichern personen- oder kartenbezogener Daten aus erfolgten Zahlungen verzichtet werden.

Vor allem im Kleingeldbereich ist die Nutzung von Debit- und Kreditkarten entbehrlich, da fälschungssichere Guthabenkarten auf der Basis von Chipkarten mit integriertem Verschlüsselungsbaustein zur Verfügung stehen. Falls größere Geldbeträge nachträglich per Kredit- oder Debitkarte bezahlt werden, ist darauf zu achten, daß die Abrechnung zunächst über Konten erfolgt, deren Inhaber dem Zahlungsempfänger nicht namhaft gemacht wird. Erst bei Zahlungsunregelmäßigkeiten ist es notwendig, den Bezug zum Kontoinhaber herzustellen.

Angesichts der Risiken, aber auch der von Chipkarten ausgehenden Chancen, fordern die Datenschutzbeauftragten die Kartenherausgeber und die Kreditwirtschaft dazu auf, kartengestützte Zahlungssysteme zu entwickeln, die möglichst ohne personenbezogene Daten auskommen, und deren Anwendung so zu gestalten, daß ein karten- und damit personenbezogenes Clearing nicht erfolgt. Der Gesetzgeber muß sicherstellen, daß auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher anonym zu bleiben.

Anlage 3

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 9. Mai 1996

Forderungen zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten

Der Schutz personenbezogener Daten ist während der Übertragung oder anderer Formen des Transportes nicht immer gewährleistet. Elektronisch gespeicherte, personenbezogene Daten können sowohl auf leitungsgebundenen oder drahtlosen Übertragungswegen als auch auf maschinell lesbaren Datenträgern weitergegeben werden. Oft sind die Eigenschaften des Transportweges dem Absender und dem Empfänger weder bekannt noch durch sie beeinflußbar. Vor allem die Vertraulichkeit, die Integrität (Unversehrtheit) und die Zurechenbarkeit der Daten (Authentizität) sind nicht sichergestellt, solange Manipulationen, unbefugte Kenntnisnahme und Fehler während des Transportes nicht ausgeschlossen werden können. Die Verletzung der Vertraulichkeit ist möglich, ohne daß Spuren hinterlassen werden.

Zahlreiche Rechtsvorschriften gebieten, das Grundrecht des Bürgers auf informationelle Selbstbestimmung auch während der automatisierten Verarbeitung personenbezogener Daten zu sichern (z. B. § 78a SGB X mit Anlage, § 10 Abs. 8 Btx-Staatsvertrag, § 9 BDSG nebst Anlage und entsprechende landesgesetzliche Regelungen).

Kryptographische Verfahren (z. B. symmetrische und asymmetrische Verschlüsselung, digitale Signatur) sind besonders geeignet, um Verletzungen des Datenschutzes beim Transport schutzwürdiger elektronisch gespeicherter Daten zu verhindern. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler nachweisen und die unberechtigte Kenntnisnahme verhindern. Derartige Verfahren sind heute Stand der Technik und können in vielen Anwendungsfällen mit vertretbarem Aufwand eingesetzt werden.

Angesichts der beschriebenen Situation und der vorhandenen technischen Möglichkeiten fordern die Datenschutzbeauftragten des Bundes und der Länder, geeignete, sichere kryptographische Verfahren beim Transport elektronisch gespeicherter personenbezogener Daten unter Berücksichtigung ihrer Schutzwürdigkeit anzuwenden.

Anlage 4

Datenschutz und Telefax

I. Konventionelle Telefaxgeräte

Telefaxgeräte sind datenverarbeitende Geräte, mit denen auch personenbezogene Daten automatisiert übertragen werden können. Sie werden eingesetzt, um bei einfacher Handhabung schnell Informationen zu übermitteln. Das Telefax ist nach dem Telefon inzwischen zum wichtigsten Kommunikationsverfahren geworden. Nicht alle Nutzer von Telefaxgeräten sind sich darüber im klaren, welche Risiken für die Vertraulichkeit der per Telefax übermittelten Informationen bestehen.

Die besonderen Gefahren sind:

- Die Informationen werden grundsätzlich „offen" (unverschlüsselt) übertragen, und der Empfänger erhält sie - vergleichbar mit einer Postkarte - in unverschlossener Form.

- Der Telefaxverkehr ist wie ein Telefongespräch abhörbar.

- Die Adressierung erfolgt durch eine Zahlenfolge (Telefaxnummer) und nicht durch eine mehrgliedrige Anschrift. Dadurch sind Adressierungsfehler wahrscheinlicher, und Übertragungen an den falschen Adressaten werden nicht oder erst nachträglich bemerkt.

- Bei Telefaxgeräten neueren Typs kann der Hersteller Fernwartungen durchführen, ohne daß der Besitzer diesen Zugriff wahrnimmt. Unter bestimmten Umständen kann er dabei auf die im Telefaxgerät gespeicherten Daten zugreifen (z.B. Lesen der Seitenspeicher sowie Lesen und Beschreiben der Rufnummern- und Parameterspeicher).

Diese Gefahren werden von Anbietern der Telekommunikationsnetze und -dienste nicht abgefangen. Deshalb ist insbesondere die absendende Stelle für die ordnungsgemäße Übertragung und die richtige Einstellung der technischen Parameter am Telefaxgerät verantwortlich.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich mit den Risiken vertraulicher Kommunikation beim Einsatz von Telefaxgeräten befaßt. Sie geben die

folgenden Empfehlungen, um den datenschutzgerechten Umgang mit Telefaxgeräten weitgehend zu gewährleisten:

1. Aufgrund der gegebenen Gefährdungen darf die Übertragung sensibler personenbezogener Daten per Telefax nicht zum Regelfall werden, sondern darf nur im Ausnahmefall unter Einhaltung zusätzlicher Sicherheitsvorkehrungen erfolgen.

2. Was am Telefon aus Gründen der Geheimhaltung nicht gesagt wird, darf auch nicht ohne besondere Sicherheitsvorkehrungen (z.B. Verschlüsselungsgeräte) gefaxt werden. Das gilt insbesondere für sensible, personenbezogene Daten, beispielsweise solche, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen (Sozial-, Steuer-, Personal- und medizinische Daten).

3. Bei der Übertragung sensibler personenbezogener Daten ist zusätzlich zu hier genannten Maßnahmen mit dem Empfänger ein Sendezeitpunkt abzustimmen, damit Unbefugte keinen Einblick nehmen können. So kann auch eine Fehlleitung durch z.B. veraltete Anschlußnummern oder beim Empfänger aktivierte Anrufumleitungen bzw. -weiterleitungen vermieden werden.

4. Telefaxgeräte sollten nur auf der Grundlage schriftlicher Dienstanweisungen eingesetzt werden. Die Bedienung darf nur durch eingewiesenes Personal erfolgen.

5. Das Telefaxgerät ist so aufzustellen, daß Unbefugte keine Kenntnis vom Inhalt eingehender oder übertragener Schreiben erhalten können.

6. Alle vom Gerät angebotenen Sicherheitsmaßnahmen (z.B. Anzeige der störungsfreien Übertragung, gesicherte Zwischenspeicherung, Abruf nach Paßwort, Fernwartungsmöglichkeit sperren) sollten genutzt werden.

7. Die vom Gerät auf der Gegenseite vor dem eigentlichen Sendevorgang abgegebene Kennung ist sofort zu überprüfen, damit bei eventuellen Wählfehlern die Übertragung unverzüglich abgebrochen werden kann.

8. Bei Telefaxgeräten, die an Nebenstellenanlagen angeschlossen sind, ist das Risiko einer Fehladressierung besonders groß, da vor der Nummer des Teilnehmers zusätzlich Zeichen zur Steuerung der Anlage eingegeben werden müssen. Beim Umgang mit derartigen Geräten ist deshalb besondere Sorgfalt geboten.

9. Die Dokumentationspflichten müssen eingehalten werden (z.B. Vorblatt oder entsprechend aussagekräftige Aufkleber verwenden, Zahl der Seiten angeben, Protokolle aufbewahren). Sende- und Empfangsprotokolle sind vertraulich abzulegen, da sie dem Fernmeldegeheimnis unterliegen.

10. Vor Verkauf, Weitergabe oder Aussortieren von Telefaxgeräten ist zu beachten, daß alle im Gerät gespeicherten Daten (Textinhalte, Verbindungsdaten, Kurzwahlziele usw.) gelöscht werden.

11. Die am Telefaxgerät eingestellten technischen Parameter und Speicherinhalte sind regelmäßig zu überprüfen, damit beispielsweise Manipulationsversuche frühzeitig erkannt und verhindert werden können.

12. Verfügt das Telefaxgerät über eine Fernwartungsfunktion, sollte sie grundsätzlich durch den Nutzer deaktiviert werden. Nur für notwendige Wartungsarbeiten sind diese Funktionen freizugeben. Nach Abschluß der Wartungsarbeiten sollten die eingestellten Parameter und Speicherinhalte kontrolliert werden.

II. Telefax in Bürokommunikationssystemen

Rechner mit Standard- oder Bürokommunikationssoftware können um Hard- und Softwarekomponenten erweitert werden, mit deren Hilfe Telefaxe gesendet und empfangen werden können (integrierte Telefaxlösungen). Lösungen für den Faxbetrieb werden sowohl für Einplatzrechner als auch für Rechnernetze angeboten.

Der Betrieb (Installation, Konfiguration, Bedienung und Wartung) integrierter Telefaxlösungen birgt gegenüber dem konventionellen Telefaxgerät zusätzliche Gefahren, da beispielsweise die verwendeten Faxmodems bzw. -karten oft nicht nur für Telefaxsendung und -empfgang geeignet sind, sondern auch andere Formen der Datenübertragung und des Zugriffs ermöglichen.

Daher sollten die folgenden Empfehlungen beim Umgang mit integrierten Telefaxlösungen zusätzlich zu den bereits genannten beachtet werden.

1. Das verwendete Rechnersystem muß sorgfältig konfiguriert und gesichert sein. Die IT-Sicherheit des verwendeten Rechners bzw. Netzes ist Voraussetzung für einen datenschutzgerechten Betrieb der Faxlösung. Dazu gehört unter anderem, daß

kein Unbefugter Zugang oder Zugriff zu den benutzten Rechnern und Netzwerken hat.

2. Beim Absenden ist auf die korrekte Angabe der Empfänger zu achten. Dazu sind die durch die Faxsoftware bereitgestellten Hilfsmittel wie Faxanschlußlisten, in denen Empfänger und Verteiler mit aussagekräftigen Bezeichnungen versehen werden können, zu benutzen.

3. Die vielfältigen Nutzungsmöglichkeiten integrierter Faxlösungen erfordern die regelmäßige und besonders sorgfältige Überprüfung der in der Faxsoftware gespeicherten technischen Parameter, Anschlußlisten und Protokolle.

4. Der Einsatz kryptographischer Verfahren ist bei integrierten Faxlösungen unkompliziert und kostengünstig möglich, sofern beide Seiten kompatible Produkte einsetzen. Deshalb sollten personenbezogene Daten immer verschlüsselt und digital signiert übertragen werden, um das Abhören zu verhindern und um den Absender sicher ermitteln und Manipulationen erkennen zu können.

5. Schon bei der Beschaffung integrierter Telefaxlösungen sollte darauf geachtet werden, daß ausreichende Konfigurationsmöglichkeiten vorhanden sind, um die dringend notwendige Anpassung an die datenschutzrechtlichen Erfordernisse des Nutzers zu gewährleisten.

Anlage 5

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 09./10. November 1995

Weiterentwicklung des Datenschutzes in der Europäischen Union

Die Konferenz der Datenschutzbeauftragten der Europäischen Union hat am 8.9.1995 in Kopenhagen in einer Resolution im Hinblick auf die für 1996 geplante Regierungskonferenz dafür plädiert, anläßlich der Überarbeitung der Unions- und Gemeinschaftsverträge in einen verbindlichen Grundrechtskatalog ein einklagbares europäisches Grundrecht auf Datenschutz aufzunehmen. Die Schaffung rechtsverbindlicher Datenschutzregelungen für die Organe und Einrichtungen der Union sowie die Schaffung einer unabhängigen und effektiven Datenschutzkontrollinstanz der EU werden angemahnt. Dieser Resolution schließt sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an. Sie hält angesichts der fortschreitenden Integration und des zunehmenden Einsatzes von Informations- und Kommunikationstechnologien in der EU eine Weiterentwicklung des Datenschutzes im Rahmen der EU für geboten.

Sie fordert die zuständigen Politiker und insbesondere die Bundesregierung auf, dafür einzutreten, daß im EU-Vertragsrecht ein Grundrecht auf Datenschutz aufgenommen wird, die materiellen Datenschutzregelungen in der EU verbessert werden, das Amt eines Europäischen Datenschutzbeauftragten geschaffen wird sowie eine parlamentarische und richterliche Kontrolle der Datenverarbeitung der im EU-Vertrag vorgesehen Instanzen sichergestellt wird.

Grundrecht auf Datenschutz

Bei einer Weiterentwicklung der Europäischen Union ist es unabdingbar, daß dem Grundrechtsschutz eine angemessene Bedeutung beigemessen wird. Dies sollte dadurch geschehen, daß die Verträge zur Europäischen Union mit einem Grundrechtskatalog ergänzt werden. Mit einer Entschließung vom 10.2.1994 hat das Europäische Parlament einen Entwurf zur Verfassung der Europäischen Union zur Erörterung gestellt, der u.a. folgende Aussagen enthält: "Jeder hat das Recht auf Achtung und

Schutz seiner Identität. Die Achtung der Privatsphäre und des Familienlebens, des Ansehens (...) wird gewährleistet".

Die Konferenz der Datenschutzbeauftragten ist mit ihrer Entschließung vom 28.4.1992 dafür eingetreten, daß in das Grundgesetz nach dem Vorbild anderer europäischer Verfassungen ein Grundrecht auf Datenschutz aufgenommen wird. Sie hat hierfür einen Formulierungsvorschlag gemacht. Auf ihren Konferenzen am 16./17.2.1993 und 9./10.3.1994 bekräftigten die Datenschutzbeauftragten des Bundes und der Länder ihre Position. Diese Forderung wurde aber wegen des Nichterreichens der notwendigen qualifizierten Mehrheit durch den Gesetzgeber nicht umgesetzt.

In Wirtschaft, Verwaltung und Gesellschaft der Staaten der EU erhält der Dienstleistungs- und Informationssektor eine zunehmende Bedeutung. Dies hat zur Folge, daß mit hochentwickelten Informationstechnologien von privaten wie von öffentlichen Stellen verstärkt personenbezogene Daten verarbeitet und auch grenzüberschreitend ausgetauscht werden. Diese Entwicklung wird gefördert durch die Privatisierung und den rasanten Ausbau transeuropäischer elektronischer Telekommunikations-Netze. Dadurch gerät das Grundrecht auf informationelle Selbstbestimmung in besonderem Maße auf der überstaatlichen Ebene in Gefahr. Dieser Gefahr kann dadurch entgegengetreten werden, daß in einen in den überarbeiteten EU-Vertrag aufzunehmenden Grundrechtskatalog das Grundrecht auf Datenschutz und zu dessen Konkretisierung ein Recht auf unbeobachtete Telekommunikation aufgenommen werden. Dies hätte folgende positive Auswirkungen:

- Anhand einer ausdrücklichen gemeinsamen Rechtsnorm kann sich eine einheitliche Rechtsprechung zum Datenschutz entwickeln, an die sowohl die EU-Organe wie auch die nationalen Stellen gebunden werden.
- Ein solches Grundrecht wäre die Basis für eine Vereinheitlichung des derzeit noch sehr unterschiedlichen nationalen Datenschutzrechts auf einem hohen Niveau.
- Den Bürgerinnen und Bürgern wird deutlich erkennbar, daß ihnen in einklagbarer Form der Datenschutz in gleicher Weise garantiert wird wie die traditionellen Grundrechte.
- Das grundlegende rechtsstaatliche Prinzip des Datenschutzes wird dauerhaft, auch bei Erweiterung der EU, gesichert.
- Mit der rechtlichen Konkretisierung eines Rechts auf unbeobachtete Telekommunikation würde der zunehmenden Registrierung des Verhaltens der Bürgerinnen und Bürger in der multimedialen Informationsgesellschaft entge-

gengewirkt und der Schutz des Fernmeldegeheimnisses auch nach dem Abbau der staatlichen Monopole im Sprachtelefondienst sichergestellt.

Materielle Datenschutzregelungen

Mit der kürzlich verabschiedeten EU-Datenschutzrichtlinie wird ein großer Fortschritt für den Datenschutz auf europäischer Ebene erreicht. Dies darf aber nicht den Blick dafür verstellen, daß in einzelnen Bereichen spezifische, dringend nötige Datenschutzregelungen fehlen. Insbesondere sind folgende Bereiche regelungsbedürftig:

- Es bedarf eines für die EU-Institutionen verbindlichen eigenen Datenschutzrechts. Die datenschutzrechtliche Verantwortung der Mitgliedstaaten einschließlich ihrer Datenschutzkontrolle der Übermittlung von Daten an EU-Institutionen bleibt dabei unberührt.
- Die geplante ISDN-Datenschutzrichtlinie darf weder einer völlig falsch verstandenen Subsidiarität zum Opfer fallen noch in unzureichender Form verabschiedet werden.
- Die im Bereich der Statistik bestehenden datenschutzrechtlichen Defizite sind abzubauen.
- Es soll eine Technikfolgenabschätzung bei der Förderung und Einführung neuer Informationstechniken mit Personenbezug durch die EU obligatorisch eingeführt werden.
- In den Bereichen Inneres und Justiz sind aufeinander abgestimmte verbindliche Regelungen mit hohem Datenschutzstandard, die die Datenverarbeitung in Akten und die Sicherung der Datenschutzkontrolle mit umfassen, zu schaffen.
- Es bedarf der Harmonisierung des Arbeitnehmerdatenschutzes auf hohem Niveau in den Staaten der EU.
- Für das Personal der EU-Organe ist der Arbeitnehmerdatenschutz sicherzustellen, was z.B. bei der Durchführung von Sicherheitsüberprüfungen insbesondere unter Beteiligung von Behörden der Heimatstaaten von großer Bedeutung ist.
- Es ist zu prüfen, inwieweit Informationszugangsrechte in weiteren Bereichen eingeführt werden sollen.

Europäischer Datenschutzbeauftragter

Die Konferenz der EU-Datenschutzkontrollinstanzen (25./26.5.1994, 8.9.1995) und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (25.8.1994) haben darauf hingewiesen, daß es an einer unabhängigen und effektiven Datenschutzkontrollinstanz fehlt, an die sich jeder wenden kann, wenn er der Ansicht ist, bei

der Verarbeitung seiner personenbezogenen Daten durch Stellen der EU in seinen Rechten verletzt zu sein. Aufgabe eines Europäischen Datenschutzbeauftragten sollte die Behandlung aller Datenschutzbelange der EU sein. Dazu gehört nicht nur die Bearbeitung von Betroffeneneingaben, sondern auch die datenschutzrechtliche Beratung der EU-Organe und -Einrichtungen sowie deren anlaßunabhängige Kontrolle, die Begleitung informationstechnischer EU-Projekte und der entsprechenden EU-Normsetzung sowie die Zusammenarbeit mit den nationalen Kontrollinstanzen. Wegen der teilweise anders gelagerten Aufgaben sollen die Funktionen des Europäischen Datenschutzbeauftragten und des Bürgerbeauftragten nach den EG-Verträgen nicht vermengt werden. Die Bundesregierung sollte im Rahmen der Vorbereitung der Regierungskonferenz 1996 darauf hinwirken, daß ein unabhängiger Europäischer Datenschutzbeauftragter in den Verträgen über die Europäische Union institutionell abgesichert wird.

Parlamentarische und richterliche Kontrolle

Bei der Zusammenarbeit der EU-Staaten in den Bereichen Justiz und Inneres muß mit Besorgnis festgestellt werden, daß eine ausreichende parlamentarische und richterliche Kontrolle im EUV derzeit nicht gewährleistet ist. Die geplante Europol-Konvention ist hierfür ein Beispiel. Mit unbestimmten Formulierungen werden einem fast völlig freischwebenden Europäischen Polizeiamt informationelle Befugnisse eingeräumt, einem Amt, das keiner parlamentarischen Verantwortlichkeit und nur einer unzureichenden (teils nur nationalen) Rechtskontrolle unterworfen wird. Zur Wahrung des Datenschutzes bei der Umsetzung gemeinsamer Maßnahmen in den Bereichen Justiz und Inneres muß daher - unbeschadet der Kontrolle durch die nationalen Datenschutzbehörden - auch eine im Rahmen ihrer jeweiligen Zuständigkeiten lückenlose Kontrolle durch die nationalen Parlamente und Gerichte sowie durch das Europäische Parlament und den Europäischen Gerichtshof sichergestellt werden.

Anlage 6

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 14./15. März 1996

Modernisierung und europäische Harmonisierung des Datenschutzrechts

Die Datenschutzrichtlinie der Europäischen Union vom Oktober 1995 verpflichtet alle Mitgliedstaaten, ihr Datenschutzrecht binnen drei Jahren auf europäischer Ebene zu harmonisieren. Die Richtlinie geht zu Recht von einem hohen Datenschutzniveau aus und stellt fest: "Die Datenverarbeitungssysteme stehen im Dienste des Menschen".

Die Datenschutzbeauftragten begrüßen diesen wichtigen Schritt zu einem auch international wirksamen Datenschutz. Sie appellieren an den Gesetzgeber in Bund und Ländern, die Umsetzung der Richtlinie nicht nur als Beitrag zur europäischen Integration zu verstehen, sondern als Aufforderung und Chance, den Datenschutz fortzuentwickeln. Die Datenschutzbeauftragten sprechen sich für eine umfassende Modernisierung des deutschen Datenschutzrechts aus, damit der einzelne in der sich rapide verändernden Welt der Datenverarbeitung, der Medien und der Telekommunikation über den Umlauf und die Verwendung seiner persönlichen Daten soweit wie möglich selbst bestimmen kann.

Die wichtigsten Ziele sind:

1. Weitgehende Vereinheitlichung der Vorschriften für den öffentlichen und privaten Bereich mit dem Ziel eines hohen, gleichwertigen Schutzes der Betroffenen, beispielsweise bei der Datenerhebung und bei der Zweckbindung bis hin zur Verarbeitung in Akten

2. Erweiterung der Rechte der Betroffenen auf Information durch die datenverarbeitenden Stellen über die Verwendung der Daten, auf Auskunft, auf Widerspruch und im Bereich der Einwilligung

3. Verpflichtung zu Risikoanalyse, Vorabkontrolle, Technikfolgenabschätzung und zur Beteiligung der Datenschutzbeauftragten bei der Vorbereitung von Regelungen mit Auswirkungen auf den Datenschutz

4. Verbesserung der Organisation und Stärkung der Befugnisse der Datenschutzkontrolle unter den Gesichtspunkten der Unabhängigkeit und der Effektivität

5. Einrichtung und effiziente Ausgestaltung des Amtes eines internen Datenschutzbeauftragten in öffentlichen Stellen

6. Weiterentwicklung der Vorschriften zur Datensicherheit, insbesondere im Hinblick auf Miniaturisierung und Vernetzung

Darüber hinaus machen die Datenschutzbeauftragten folgende Vorschläge:

1. Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen und Regelung der Video-Überwachung

2. Stärkere Einbeziehung von Presse und Rundfunk in den Datenschutz; Aufrechterhaltung von Sonderregelungen nur, soweit dies für die Sicherung der Meinungsfreiheit notwendig ist

3. Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren

4. Sicherstellung der informationellen Selbstbestimmung bei Multimedia-Diensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsformen anzubieten, durch den Schutz vor übereilter Einwilligung, z.B. durch ein Widerrufsrecht, und durch strenge Zweckbindung für die bei Verbindung, Aufbau und Nutzung anfallenden Daten

5. Besondere Regelungen für Chipkarten-Anwendungen, um die datenschutzrechtliche Verantwortung aller Beteiligten festzulegen und den einzelnen vor unfreiwilliger Preisgabe seiner Daten zu schützen

6. Schutz bei Persönlichkeitsbewertungen durch den Computer, insbesondere durch Beteiligung des Betroffenen und Nachvollziehbarkeit der Computerentscheidung

7. Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing

8. Verbesserung des Datenschutzes bei grenzüberschreitender Datenverarbeitung; Datenübermittlung ins Ausland nur bei angemessenem Datenschutzniveau.

Anlage 7

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 9./10. März 1995

Entwurf eines Gesetzes über das Bundeskriminalamt (BKA-Gesetz) - Bundesrats-Drucksache 94/95

Zu den Beratungen des Entwurfs für ein Gesetz über das Bundeskriminalamt erklären die Datenschutzbeauftragten des Bundes und der Länder:

Auch aus Sicht des Datenschutzes ist es zu begrüßen, daß die seit langem überfälligen bereichspezifischen Regelungen zur bundesweiten polizeilichen Datenverarbeitung insbesondere im polizeilichen Informationssystem (INPOL) nunmehr in das Gesetzgebungsverfahren eingebracht werden. Der Gesetzentwurf enthält im Vergleich zu den Vorentwürfen eine Reihe von Vorschriften, die datenschutzrechtlich positiv zu werten sind. Hierzu gehören:

- der Verzicht auf die im Vorentwurf vorgesehenen Befugnisse zur sog. "Feststellung des Anfangsverdachts";
- das Erfordernis der Einwilligung für die Speicherung von Daten über Zeugen und mögliche Opfer;
- Übermittlungsverbote bei überwiegenden schutzwürdigen Interessen der Betroffenen oder bei entgegenstehenden gesetzlichen Verwendungsregelungen;
- die Beachtung landesgesetzlicher Löschungsfristen.

Andererseits begegnet der Gesetzentwurf jedoch nach wie vor gewichtigen Bedenken, da er tiefe Eingriffe in die Rechte von Betroffenen ermöglicht, deren Voraussetzungen und Reichweite unklar oder nicht durch überwiegende Interessen der Allgemeinheit gerechtfertigt sind. Dies gilt insbesondere für

- die Verwendung des Begriffs der Straftaten von erheblicher Bedeutung ohne Definition, um welche Tatbestände es sich handelt, weil damit nicht mehr voraussehbar ist, wann die an diesen Begriff anknüpfenden Eingriffsbefugnisse zur Datenverarbeitung eröffnet sind;
- die Befugnisse der Zentralstelle zu selbständigen Datenerhebungen und Übermittlungen bis hin zum automatisierten Datenverbund mit ausländischen und zwi-

schenstaatlichen Stellen ohne Einvernehmen mit den jeweils verantwortlichen Länderpolizeien;

- die unklare Abgrenzung der Datenverarbeitungsbefugnisse im Hinblick auf die unterschiedlichen Befugnisse zur Strafverfolgung, Gefahrenabwehr, Verhütung von Straftaten und Vorsorge für künftige Strafverfolgung sowie die fehlende klare Zweckbindungs- und Zweckänderungsregelung;
- die Befugnis zur verdeckten Datenerhebung aus Wohnungen ohne eindeutige Begrenzung auf den Schutz gefährdeter Ermittler.

Die Datenschutzbeauftragten fordern den Gesetzgeber auf, die Schwachstellen des Entwurfs auszuräumen. Insbesondere fordern sie klare verfassungskonforme Regelungen zur Auskunftserteilung an Betroffene und der Prüfrechte für INPOL-Daten dahingehend, daß die Datenschutzkontrollrechte bei der datenschutzrechtlichen Verantwortung der Stellen anknüpfen, die die Speicherung im INPOL-System selbst vornehmen oder veranlassen.

Anlage 8

Beschluß
der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27.09.1994

Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen

Angesichts der aktuellen Diskussion über die innere Sicherheit weisen die Datenschutzbeauftragten des Bundes und der Länder darauf hin, daß umfangreiche polizeiliche Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten, insbesondere im technischen Bereich, gesetzlich verankert worden sind.

Zum Kreis der Betroffenen zählen dabei nicht nur Personen, gegen die Verdachtsgründe vorliegen, sondern auch nichtverdächtige Kontakt- und Begleitpersonen und Unbeteiligte, deren Schutz nach Auffassung der Datenschutzbeauftragten besonders wichtig ist.

Vor diesem Hintergrund schlagen die Datenschutzbeauftragten vor, den derzeitigen Erkenntnisstand über die Erforderlichkeit polizeilicher Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten sowie ihre Auswirkungen auf die Rechte der Betroffenen durch folgende Maßnahmen zu verbessern:

1. Die Datenschutzbeauftragten teilen die von einigen Innenministern vertretene Auffassung, daß bloße Angaben über Einsatzzahlen der besonderen Befugnisse zur Datenerhebung nur einen begrenzten Aussagewert haben. Aufschluß über die tatsächliche Praxis, ihre Erforderlichkeit und Verhältnismäßigkeit läßt sich nur durch Überprüfung und Auswertung der einzelnen Einsätze gewinnen. Hierzu müssen unter Beteiligung der Datenschutzbeauftragten und der Wissenschaft, insbesondere der Kriminologie und des Polizeirechts, objektive und nachprüfbare Auswertungskriterien entwickelt werden.

2. Die Datenschutzbeauftragten begrüßen daher die Initiative für eine sog. Rechtstatsachensammlung, die Erhebungen zu polizeilichen Ermittlungsmethoden und Eingriffsbefugnissen durchführen soll. Sie schlagen vor, in diese Rechtstatsachensammlung insbesondere Angaben über den Anlaß einer Datenerhebung mit be-

sonderen Mitteln, die Örtlichkeit und die Dauer der Maßnahme, den Umfang der überwachten Gespräche, den betroffenen Personenkreis sowie die Anzahl der ermittelten, verurteilten, aber auch der entlasteten Personen einzubeziehen. Derartige Aufstellungen wären nicht nur für elektronische Überwachungsmethoden, sondern auch für Observationen, den Einsatz verdeckter Ermittler und V-Personen sowie für Rasterfahndungen denkbar.

3. Einige Polizeigesetze verpflichten dazu, zu überprüfen, ob es notwendig ist, bestehende Dateien weiterzuführen oder zu ändern. Dabei soll nicht nur darauf eingegangen werden, ob die Anwendungen, d.h. die Dateien, weiterhin erforderlich sind, sondern auch auf ihren Nutzen sowie auf ihre Schwachstellen und Mängel. Ferner sind Vorschläge zu machen, wie festgestellte Defizite beseitigt oder minimiert werden können.

4. Die Datenschutzbeauftragten gehen davon aus, daß sie bei den Überlegungen zur Rechtstatsachensammlung rechtzeitig beteiligt und die jeweiligen Materialien und Zwischenergebnisse mit ihnen erörtert werden.

Anlage 9

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 9./10. März 1995

Datenschutz bei Wahlen

Bei der Durchführung von Wahlen haben sich Probleme bei der Verarbeitung personenbezogener Daten ergeben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu die folgende Entschließung gefaßt:

1. Durchführung von Wahlstatistiken

Diejenigen Wahlberechtigten, in deren Wahlbezirk eine repräsentative Wahlstatistik durchgeführt werden soll, sind bereits mit der Wahlbenachrichtigung hierüber zu informieren. In allgemeiner Form ist auch im Wahllokal ein gut sichtbarer Hinweis auf die Einbeziehung in die Wahlstatistik anzubringen.

Die Statistik sollte nur in solchen Wahlbezirken durchgeführt werden, in denen jede Geschlechts- und Altersgruppe wenigstens so viele Wahlberechtigte aufweist, daß das Wahlgeheimnis mit Sicherheit gewahrt bleibt. Das Kriterium ist vom Landeswahlleiter vor der Festlegung der Auswahlbezirke zu prüfen. Gegebenenfalls sind ungeeignete Wahlbezirke auszutauschen.

Die Auszählung der Wahlberechtigten und der Wahlbeteiligung auf der Grundlage der Wählerverzeichnisse sollte durch den Wahlvorstand erfolgen, während die statistische Auszählung der Stimmzettel durch die jeweils für die Durchführung der Statistik zuständige Stelle vorzunehmen ist.

Untersuchungen, bei denen Angaben über die Wahlbeteiligung oder die Stimmabgabe aus verschiedenen Wahlen einzelfall- und personenbezogen zusammengeführt werden, gefährden das Wahlgeheimnis und sind daher unzulässig.

2. Auslegung von Wählerverzeichnissen

Durch die Einsicht in das Wählerverzeichnis besteht nach der jetzigen Rechtslage die Gefahr, daß Daten sowohl von Bürgern, über die in Melderegistern eine Auskunftssperre eingetragen ist, als auch von Bürgern, die in einer speziellen sozialen Situation

leben (z. B. Justizvollzugsanstalten, Frauenhäuser, psychiatrische Kliniken, Obdachlose), offenbart werden.

Um einerseits die Kontrollmöglichkeit durch die Öffentlichkeit im Vorfeld einer Wahl weiterhin zu gewährleisten, andererseits die datenschutzrechtlichen Belange der genannten Betroffenen zu wahren und dem Mißbrauch einer Adreßrecherche vorzubeugen, fordern die Datenschutzbeauftragten des Bundes und der Länder, daß bei allen Wahlen

- entweder in den öffentlich ausliegenden Wählerverzeichnissen nur Name, Vorname und Geburtsdatum der Wahlberechtigten aufgeführt werden
- oder aber bei Wiedergabe der Adressen im Wählerverzeichnis nur Auskünfte zu bestimmten Personen an den Auskunftssuchenden erteilt werden, wenn er vorher die Adresse dieser Person angegeben hat.

Im übrigen sind Daten von Bürgern, für die in Melderegistern eine Auskunftssperre eingetragen ist, im Wählerverzeichnis nicht zu veröffentlichen.

3. Gewinnung von Wahlhelfern

Bei der Gewinnung von Wahlhelfern sind folgende Grundsätze zu beachten:

Es dürfen nur die zur Bestellung erforderlichen Daten, wie Name, Vorname und Wohnanschrift, erhoben werden. Die Betroffenen sind über den Zweck der Datenerhebung und die weitere Datenverarbeitung umfassend zu unterrichten.

Über die Abwicklung der jeweiligen Wahl hinaus dürfen die Daten der Wahlhelfer, soweit sie nicht ausdrücklich widersprochen haben, in einer Wahlhelferdatei nur gespeichert werden, wenn sie dieser Speicherung nicht widersprochen haben. Die Wahlhelfer sind auf ihr Widerspruchsrecht hinzuweisen.

Beschäftigtendaten dürfen nur auf freiwilliger Basis übermittelt werden, sofern nicht eine besondere Rechtsvorschrift die Übermittlung zuläßt. Im Falle der Freiwilligkeit muß es den Beschäftigten möglich sein, selbst die Meldung unmittelbar gegenüber der Wahlbehörde abzugeben. Nach Gründen, die einer Übernahme des Ehrenamtes entgegenstehen, darf erst im förmlichen Verfahren durch die Wahlbehörde gefragt werden.

4. Erteilung von Wahlscheinen

Die in den Wahlordnungen des Bundes und der Länder enthaltene Regelung, nach der die Antragstellung für die Erteilung eines Wahlscheines auf einem Vordruck zu begründen ist und der Grund gegenüber der Gemeinde glaubhaft gemacht werden muß, ist aus datenschutzrechtlicher Sicht unverhältnismäßig. Da sich aus der geforderten Differenzierung der Begründung keine unterschiedlichen Rechtsfolgen ableiten, ist diese entbehrlich. Es genügt in der Antragstellung eine Erklärung des Wahlberechtigten, daß er am Tag der Wahl aus wichtigem Grund das für ihn zuständige Wahllokal nicht aufsuchen kann.

Anlage 10

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 9./10. März 1995

Anforderungen an den Persönlichkeitsschutz im Medienbereich

Die unabhängige und unzensierte Berichterstattung durch Presse, Rundfunk und Film (Art. 5 Abs. 1 Satz 2 GG) dient der freien individuellen und öffentlichen Meinungsbildung. Das Bundesverfassungsgericht hat die freie Meinungsbildung als Voraussetzung sowohl der Persönlichkeitsentfaltung als auch der demokratischen Ordnung bezeichnet. Insofern besteht ein enger Zusammenhang zwischen der Selbstbestimmung des Einzelnen und der Medienfreiheit.

Die rasante Entwicklung der Medientechnik, die Zunahme interaktiver Teledienste und die verstärkte kommerzielle Nutzung von Pressedatenbanken eröffnen einerseits neue Informationsmöglichkeiten für den Bürger, verschärfen aber die Gefährdungen des Rechts auf informationelle Selbstbestimmung. Diesen Gefährdungen muß der Datenschutz auf rechtlicher und technisch-organisatorischer Ebene angemessen begegnen.

Elektronic Publishing und Medienarchive

Neue Formen der Verbreitung von Informationen über Netze und auf elektronischen Datenträgern führen in bisher unbekanntem Maß zu großen Informationsbeständen, in denen potentiell jedermann gezielt auf personenbezogene Daten zugreifen kann. Zudem öffnen Medienarchive, die bislang ausschließlich für journalistische Zwecke genutzt wurden, riesige Datensammlungen für medienfremde Nutzer. In Persönlichkeitsrechte wird dann besonders tief eingegriffen, wenn auch lange zurückliegende Publikationen praktisch von jedermann recherchiert werden können. Damit droht das in verschiedenen Rechtsbereichen vorgesehene „Recht auf Vergessen" wirkungslos zu werden, das z.B. durch die Löschungsvorschriften für das Bundeszentralregister gewährleistet werden soll.

Angesichts dieser Entwicklungen muß die Reichweite der datenschutzrechtlichen Sonderstellung der Medien („Medienprivileg") neu bestimmt werden. Es ist zumindest gesetzlich klarzustellen, daß die geschäftsmässige Verwendung personenbezogener

Daten außerhalb des eigenen Medienbereichs, insbesondere durch kommerzielle Pressedatenbanken, nicht unter das „Medienprivileg" fällt.

Interaktive Dienste und Mediennutzungsprofile

Auch beim Ausbau neuer digitaler Kommunikationsformen (interaktive Dienste wie z.B. Video on Demand) müssen die Persönlichkeitsrechte der Nutzer gewahrt werden. Dabei ist stärker als bisher von vornherein Wert darauf zu legen, daß datenschutzfreundliche Techniken entwickelt werden und zum Einsatz kommen, bei denen personenbezogene Verbindungs- und Nutzungsdaten erst gar nicht entstehen. Von besonderer Bedeutung sind hier anonyme Zahlverfahren, z.B. Prepaid-Karten, auf denen Informationen über die Nutzung ausschließlich dezentral gespeichert werden.

Entsprechend den Bestimmungen im Bildschirmtextstaatsvertrag und in den neueren Mediengesetzen ist sicherzustellen, daß sich die Erhebung und die Aufzeichnung von Verbindungs- und Abrechnungsdaten auf das erforderliche Maß beschränken. Dieser strikte Verarbeitungsrahmen darf auch nicht dadurch ausgeweitet werden, daß die Nutzung eines Dienstes von der Einwilligung in eine zweckfremde Verwendung der Daten abhängig gemacht wird. Die Länder sollten entsprechende einheitliche Regelungen für alle interaktiven Dienste treffen.

Da es sich bei den angesprochenen Diensten um Bestandteile einer entstehenden globalen Informationsinfrastruktur handelt, wird die Bundesregierung aufgefordert, sich auf internationaler Ebene für entsprechende Regelungen einzusetzen.

Rechte der Betroffenen gegenüber den Medien

Während die von der Berichterstattung Betroffenen - neben dem für alle Bereiche geltenden Gegendarstellungsrecht - gegenüber den öffentlich-rechtlichen und privaten Rundfunkveranstaltern inzwischen weitere elementare Datenschutzrechte besitzen, gibt es gegenüber der Presse keine vergleichbaren Regelungen.

So kann derjenige, der durch die Berichterstattung der Rundfunkveranstalter in seinem Persönlichkeitsrecht beeinträchtigt wird, in den meisten Fällen nach der Publikation Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Gegenüber der Presse hat er kein entsprechendes Auskunftsrecht. Die meisten Rundfunkveranstalter sind - anders als die Presse - zudem verpflichtet, etwaige Gegendarstellungen zu den gespeicherten Daten zu neh-

men, auf die sie sich beziehen (Mitspeicherungspflicht). Ein sachlicher Grund für diese Unterscheidungen ist nicht erkennbar.

Das Presserecht sollte insofern der Rechtslage nach dem Rundfunkrecht (z.B. § 41 Abs. 3 BDSG und Art. 17 Abs. 2 ZDF-Staatsvertrag) angeglichen werden.

Gegenüber Pressedatenbanken, die nicht nur dem eigenen internen Gebrauch dienen, sollte der Betroffene darüber hinaus ein Auskunftsrecht bezüglich des zu seiner Person gespeicherten veröffentlichten Materials haben.

Öffentlichkeitsarbeit der Behörden

Personenbezogene Veröffentlichungen von Behörden können das Recht auf informationelle Selbstbestimmung erheblich beeinträchtigen. Das gilt für die Personen, auf die die Aktivitäten der Behörde unmittelbar gerichtet sind, wie auch für andere Verfahrensbeteiligte (wie z.B. Einwender, Opfer von Straftaten, Zeugen) und im besonderen Maße für unbeteiligte Personen aus dem sozialen Umfeld des Betroffenen. Deshalb ist bei der Weitergabe von Daten aus Strafermittlungsverfahren an die Medien besonders zurückhaltend zu verfahren.

Für den Umfang des Anspruchs der Medien auf Weitergabe personenbezogener Daten in Form von Presseerklärungen und Auskünften gibt es keine konkreten gesetzlichen Festlegungen. Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für geboten, daß der Gesetzgeber Kriterien für die Abwägung zwischen dem Persönlichkeitsrecht des Betroffenen und der Freiheit der Berichterstattung durch Rundfunk und Presse deutlicher als bisher festlegt. Dafür kommen die Vorschriften des Landespresserechts, in besonders sensiblen Bereichen aber auch spezialgesetzliche Regelungen wie etwa die Strafprozeßordnung in Betracht.

Gerichtsfernsehen

Die Datenschutzbeauftragten des Bundes und der Länder treten den in jüngster Zeit zunehmend erhobenen Forderungen nach einer Aufhebung des Verbots der Hörfunk- und Fernsehberichterstattung aus Gerichtsverhandlungen entgegen. Insbesondere bei Strafprozessen vor laufenden Mikrofonen und Kameras würde es unweigerlich zu einer gravierenden Beeinträchtigung des Persönlichkeitsrechts der Angeklagten, der Opfer, der Zeugen und ihrer Angehörigen kommen. Selbst mit Einwilligung aller Prozeßbeteiligten darf die Hörfunk- und Fernsehberichterstattung nicht zugelassen werden.

Die Gerichtsverhandlung darf nicht zu einem massenmedial vermittelten „modernen Pranger" werden.

Anlage 11

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 9./10. November 1995

Forderungen an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien (außerhalb der Öffentlichkeitsfahndung der Ermittlungsbehörden)

1. Für die Übermittlung von personenbezogenen Daten durch Justiz und Polizei an die Medien sollte eine bereichsspezifische Rechtsgrundlage geschaffen werden. Die Regelung sollte für den betroffenen Bürger den Umfang des Eingriffs in sein Recht auf informationelle Selbstbestimmung erkennbar machen.

2. Die Übermittlung personenbezogener Daten an die Medien ist nur ausnahmsweise gerechtfertigt, wenn das Verfahren gerade im Hinblick auf die Person des Betroffenen oder die besonderen Umstände der Tat für die Öffentlichkeit von überwiegendem Interesse ist.

3. Bei der Entscheidung, ob und in welchem Umfang personenbezogene Daten an die Medien übermittelt werden, sind die schutzwürdigen Belange der Betroffenen zu berücksichtigen. Dazu zählen insbesondere die privaten und beruflichen Folgen für das Opfer, den Beschuldigten/Angeklagten und deren Angehörige sowie die Schwere, die Umstände und die Folgen des Delikts.

4. Bei der Übermittlung von personenbezogenen Daten über Beschuldigte/Angeklagte sind auch der Grad des Tatverdachts und der Stand des Verfahrens zu berücksichtigen. Vor Beginn der öffentlichen Hauptverhandlung ist ein besonders strenger Maßstab an das Vorliegen eines „überwiegenden Interesses" der Öffentlichkeit anzulegen.

5. Bis zur rechtskräftigen Verurteilung ist die Unschuldsvermutung zugunsten des Beschuldigten oder Angeklagten zu beachten. Zu unterlassen sind alle Auskünfte oder Erklärungen, die geeignet sind, die Unbefangenheit der Verfahrensbeteiligten zu beeinträchtigen. Akeneinsicht durch Medienvertreter kommt nicht in Betracht.

6. Grundsätzlich sind in Auskünfte und Erklärungen über das Ermittlungs- und Strafverfahren keine Namen und sonstige personenbezogene Angaben, die Opfer von Straftaten, Zeugen, Beschuldigte und Angeklagte bestimmbar machen, aufzunehmen. Vor allem bei Hinweisen auf den Wohnort, das Alter, den Beruf und die familiären Verhältnisse oder sonstigen sozialen Bindungen (z.B. Partei- oder Vereinsmitgliedschaft) ist zu prüfen, inwieweit dadurch eine Identifizierung des Betroffenen möglich wird.

7. Personenbezogene Daten dürfen nicht übermittelt werden, wenn besondere bundesgesetzliche oder landesgesetzliche Verwendungsregelungen entgegenstehen.

8. Ist die Bekanntgabe der Person des Beschuldigten oder Angeklagten wegen des überwiegenden öffentlichen Interesses gerechtfertigt, muß auch bei der Übermittlung sonstiger personenbezogener Daten abgewogen werden, ob diese Informationen für die Berichterstattung über die Tat selbst oder die Hintergründe, die zu der Tat geführt haben, erforderlich sind, und in welchem Umfang der Betroffene dadurch in seinem Persönlichkeitsrecht beeinträchtigt wird.

9. Die Bekanntgabe von Vorstrafen ist nur ausnahmsweise zulässig. Sie setzt voraus, daß die frühere Verurteilung im Bundeszentralregister noch nicht getilgt und ihre Kenntnis für eine nachvollziehbare Berichterstattung über eine schwerwiegende Straftat - auch unter Berücksichtigung des Persönlichkeitsrechts des Betroffenen und des Resozialisierungsgedankens - erforderlich ist. Besondere Zurückhaltung ist bei Auskünften und Erklärungen über Sachverhalte geboten, die der früheren Verurteilung zugrunde liegen.

10. Wegen des überragenden Schutzes von Minderjährigen und Heranwachsenden ist bei Auskünften und Erklärungen über Verfahren gegen diesen Personenkreis besondere Zurückhaltung hinsichtlich der Bekanntgabe personenbezogener Daten zu wahren.

11. Opfer, Zeugen und Familienangehörige haben in der Regel keine Veranlassung gegeben, daß ihre persönlichen Lebensumstände in der Öffentlichkeit bekannt gemacht werden. Die Übermittlung personenbezogener Daten über diesen Personenkreis an die Medien kommt deshalb grundsätzlich nicht in Betracht.

12. Bildveröffentlichungen greifen wegen der damit verbundenen sozialen Prangerwirkung besonders tief in das Persönlichkeitsrecht des Betroffenen ein. Eine Bildherausgabe kommt daher für Zwecke der Medienberichterstattung nicht in Betracht.

Anlage 12

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 9./10. März 1995

Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich

Bisher ist der Gesetzgeber im Bereich der Justiz den verfassungsrechtlichen Forderungen nach ausreichenden normenklaren Regelungen über die Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien nicht nachgekommen. So enthalten z.B. die bislang bekannt gewordenen Entwürfe zu einem Strafverfahrensänderungsgesetz nur unzureichende Generalklauseln. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erklärt deshalb:

1. Aufbewahrung, Aussonderung und Vernichtung der Akten und die Speicherung personenbezogener Daten in Dateien im Bereich der Justiz müssen nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil für die Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden gesetzlich geregelt werden, wobei sich die Aufbewahrungsdauer am Recht auf informationelle Selbstbestimmung und am Zweck der Speicherung zu orientieren hat.

   Hierbei hat der Gesetzgeber die grundlegenden Entscheidungen zur Aufbewahrungsdauer selbst zu treffen. Aufgrund einer hinreichend konkreten Verordnungsermächtigung können die Einzelheiten durch Rechtsverordnung bestimmt werden.

2. Die derzeit bestehenden Aufbewahrungsfristen sind konsequent zu vereinfachen und zu verkürzen. Soweit geboten sind Verkürzungen vorzunehmen.

3. Die derzeit geltende generelle 30-jährige Aufbewahrungsfrist für Strafurteile und Strafbefehle mit der Folge der umfassenden Verfügbarkeit der darin enthaltenen Informationen ist nicht angemessen. Bei der Bemessung der Aufbewahrungsfrist von Strafurteilen und Strafbefehlen sowie für die Bestimmung des Zeitpunkts der Einschränkung der Verfügbarkeit ist vielmehr nach Art und Maß der verhängten Sanktionen zu differenzieren.

Bei der Festlegung des Beginns der Aufbewahrungsfrist sollte - abweichend von der bisherigen Praxis, nach der es auf die Weglegung der Akte ankommt - regelmäßig auf den Zeitpunkt des Eintritts der Rechtskraft der ergangenen gerichtlichen Entscheidung abgestellt werden.

Ergeht keine rechtskraftfähige Entscheidung, so sollte die Aufbewahrungsfrist mit dem Erlaß der Abschlußverfügung beginnen.

4. Wird der Akteninhalt auf Bild- oder Datenträgern, die an die Stelle der Urschrift treten, aufbewahrt, so sind gleichwohl unterschiedliche Löschungsfristen für einzelne Aktenteile zu beachten. Aus datenschutzrechtlicher Sicht sind Datenträger zu wählen, die eine differenzierte Löschung gewährleisten. Ist bei Altbeständen eine teilweise Aussonderung technisch nicht möglich oder nur mit unverhältnismäßigem Aufwand zu bewerkstelligen, so hat eine Sperrung der an sich auszusondernden Teile zu erfolgen.

5. Sind in einer Akte Daten mehrerer beteiligter Personen gespeichert, so ist eine Sperre hinsichtlich solcher Aktenteile, die einzelne beteiligte Personen betreffen, vorzusehen, wenn diese Aktenteile eigentlich ausgesondert werden müßten, aus praktischen Gründen aber keine Vernichtung erfolgen kann.

6. Bei Freisprüchen und Einstellungen des Verfahrens wegen Wegfalls des Tatverdachts ist dafür Sorge zu tragen, daß ein Zugriff auf die automatisiert gespeicherten Daten nur noch zu Zwecken der Aktenverwaltung erfolgen kann.

7. Für die Daten von Nebenbeteiligten (z.B. Anzeigeerstatter, Geschädigte) ist eine vorzeitige Löschung vorzusehen. Hinsichtlich der Hauptbeteiligten sollte eine Teillöschung der Personen- und Verfahrensdaten stattfinden, sobald die voll ständigen Daten zur Durchführung des Verfahrens nicht mehr erforderlich sind.

8. Soweit Daten verschiedener Gerichtszweige oder verschiedener speichernder Stellen in gemeinsamen Systemen verarbeitet werden, ist durch rechtliche, technische und organisatorische Maßnahmen sicherzustellen, daß die Zweckbindung der gespeicherten Daten beachtet wird.

Anlage 13

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 09./10. November 1995

Planungen für ein Korruptionsbekämpfungsgesetz

Derzeit gibt es Vorschläge, die Bekämpfung der Korruption durch Verschärfungen des Strafrechts und des Strafprozeßrechts mit weiteren Eingriffen in das Grundrecht auf informationelle Selbstbestimmung zu organisieren. Ein Beispiel dafür ist der Beschluß des Bundesrates vom 3. November 1995 zur Einbringung eines Korruptionsbekämpfungsgesetzes.

Nach dem vom Bundesrat beschlossenen Gesetzentwurf sollen Bestechlichkeit und Bestechung in den Kreis derjenigen Tatbestände aufgenommen werden, bei deren Verdacht die Überwachung des Fernmeldeverkehrs und der Einsatz technischer Mittel ohne Wissen des Betroffenen (§§ 100a, 100c StPO) angeordnet werden dürfen.

Die Datenschutzbeauftragten weisen demgegenüber darauf hin, daß es vorrangig um Prävention, nicht um Repression geht. Die Datenschutzbeauftragten treten für eine entschlossene und wirksame Bekämpfung der Korruption mit rechtsstaatlichen Mitteln unter strikter Beachtung der Freiheitsrechte ein.

Sie wenden sich zugleich gegen eine Rechtspolitik, welche - noch bevor sie sich darüber im klaren ist, was die bisherigen Verschärfungen und Eingriffe an Vorteilen und an Nachteilen gebracht haben - auf weitere Verschärfungen und Eingriffe setzt.

Gerade gegenüber der Korruption gibt es Möglichkeiten, welche Effektivität versprechen und gleichwohl die Privatsphäre der unbeteiligten und unschuldigen Bürgerinnen und Bürger nicht antasten:

- Rotation derjenigen Mitarbeiterinnen und Mitarbeiter einer Behörde, deren Position und Aufgaben erfahrungsgemäß für Bestechungsversuche in Betracht kommen;
- Vier- und Sechsaugenprinzip bei bestimmten Entscheidungen;
- Trennung von Planung, Überwachung und Ausführung, von Ausschreibung und Vergabe;
- Prüfverfahren und Innenrevision;

- Codes of Conduct (formalisierte "Ethikprogramme") im Bereich der Wirtschaft;
- verbesserte Transparenz von Entscheidungsprozessen in der Verwaltung.

Die in den Gesetzentwürfen vorgesehene weitere Einschränkung von Grundrechten, die mit einer abermaligen Erweiterung der Telefonüberwachung verbunden wäre, ist nur vertretbar, wenn sie nach einer sorgfältigen Güter- und Risikoabwägung zusätzlich zu den o. g. Verfahrens- und Verhaltensmaßregeln als geeignet und unbedingt erforderlich anzusehen wäre.

Die Datenschutzbeauftragten verlangen, daß vor einer zusätzlichen Aufnahme von Straftatbeständen in den Katalog der Abhörvorschrift des § 100a StPO diese Abwägung durchgeführt wird.

Die Datenschutzbeauftragten fordern weiterhin, daß eine Erweiterung des genannten Straftatenkataloges nur befristet vorgenommen wird, damit sich vor einer Verlängerung die Notwendigkeit stellt, auf der Grundlage einer sorgfältigen Erfolgs- und Effektivitätskontrolle erneut die Erforderlichkeit und Verhältnismäßigkeit einer solchen Erweiterung des Grundrechtseingriffs zu überprüfen.

Die Datenschutzbeauftragten verlangen, daß der Gesetzgeber vor weiteren Eingriffen in Freiheitsrechte eine sorgfältige Güter- und Risikoabwägung vornimmt und dabei insbesondere verantwortlich prüft, ob sich die innenpolitischen Ziele mit Mitteln erreichen lassen, welche die informationelle Selbstbestimmung der Bürgerinnen und Bürger schonen.

Schließlich gibt die anstehende erneute Erweiterung des Katalogs von § 100a StPO Veranlassung, den Umfang der darin genannten Straftaten sobald wie möglich grundlegend zu überprüfen.

Anlage 14

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 22./23. Oktober 1996

Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich

Die Entwicklung moderner Informations- und Telekommunikationstechniken führt zu einem grundlegend veränderten Kommunikationsverhalten der Bürger.

Die Privatisierung der Netze und die weite Verbreitung des Mobilfunks geht einher mit einer weitreichenden Digitalisierung der Kommunikation. Mailboxen und das Internet prägen die Informationsgewinnung und -verbreitung von Privatleuten, von Unternehmen und öffentlichen Institutionen gleichermaßen.

Neue Dienste wie Tele-Working, Tele-Banking, Tele-Shopping, digitale Videodienste und Rundfunk im Internet sind einfach überwachbar, weil personenbezogene Daten der Nutzer in digitaler Form vorliegen. Die herkömmlichen Befugnisse zur Überwachung des Fernmeldeverkehrs erhalten eine neue Dimension; weil immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden, können sie mit geringem Aufwand kontrolliert und ausgewertet werden. Demgegenüber stehen jedoch auch Gefahren durch die Nutzung der neuen Technik zu kriminellen Zwecken. Die Datenschutzbeauftragten erkennen an, daß die Strafverfolgungsbehörden in die Lage versetzt werden müssen, solchen mißbräuchlichen Nutzungen der neuen Techniken zu kriminellen Zwecken wirksam zu begegnen.

Sie betonen jedoch, daß die herkömmlichen weitreichenden Eingriffsbefugnisse auch unter wesentlich veränderten Bedingungen nicht einfach auf die neuen Formen der Individual- und Massenkommunikation übertragen werden können. Die zum Schutz der Persönlichkeitsrechte des einzelnen gezogenen Grenzen müssen auch unter den geänderten tatsächlichen Bedingungen der Verwendung der modernen Informationstechnologien aufrechterhalten und gewährleistet werden. Eine Wahrheitsfindung um jeden Preis darf es auch insoweit nicht geben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher Thesen zur Bewältigung dieses Spannungsverhältnisses entwickelt.

Sie hebt insbesondere den Grundsatz der spurenlosen Kommunikation hervor. Kommunikationssysteme müssen mit personenbezogenen Daten möglichst sparsam umgehen. Daher verdienen solche Systeme und Technologien Vorrang, die keine oder möglichst wenige Daten zum Betrieb benötigen. Ein positives Beispiel ist die Telefonkarte, deren Nutzung keine personenbezogenen Daten hinterläßt und die deshalb für andere Bereiche als Vorbild angesehen werden kann. Daten allein zu dem Zweck einer künftig denkbaren Strafverfolgung bereitzuhalten ist unzulässig.

Bei digitalen Kommunikationsformen läßt sich anhand der Bestands- und Verbindungsdaten nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Eine staatliche Überwachung dieser Vorgänge greift tief in das Persönlichkeitsrecht der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse (z. B. Arztgeheimnis, anwaltliches Vertrauensverhältnis). Die Datenschutzbeauftragten fordern daher, daß der Gesetzgeber diesen Gesichtspunkten Rechnung trägt.

Die Datenschutzbeauftragten wenden sich nachhaltig dagegen, daß den Nutzern die Verschlüsselung des Inhalts ihrer Nachrichten verboten wird. Die Möglichkeit für den Bürger, seine Kommunikation durch geeignete Maßnahmen vor unberechtigten Zugriffen zu schützen, ist ein traditionelles verfassungsrechtlich verbürgtes Recht.

Aus Sicht des Datenschutzes besteht andererseits durchaus Verständnis für das Interesse der Sicherheits- und Strafverfolgungsbehörden, sich rechtlich zulässige Zugriffsmöglichkeiten nicht dadurch versperren zu lassen, daß Verschlüsselungen verwandt werden, zu denen sie keinen Zugriff haben. Eine Reglementierung der Verschlüsselung, z.B. durch Schlüsselhinterlegung, erscheint aber aus derzeitiger technischer Sicht kaum durchsetzbar, da entsprechende staatliche Maßnahmen - insbesondere im weltweiten Datenverkehr - ohnehin leicht zu umgehen und kaum kontrollierbar wären.

Anlage 15

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 14./15. März 1996

Transplantationsgesetz

Bei der anstehenden gesetzlichen Regelung, unter welchen Voraussetzungen die Entnahme von Organen zur Transplantation zulässig sein soll, werden untrennbar mit der Ausformung des Rechts auf Selbstbestimmung auch Bedingungen des Rechts auf informationelle Selbstbestimmung festgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont hierzu, daß von den im Gesetzgebungsverfahren diskutierten Modellen die „enge Zustimmungslösung" - also eine ausdrückliche Zustimmung des Organspenders - den geringsten Eingriff in das Recht auf informationelle Selbstbestimmung beinhaltet. Sie zwingt niemanden, eine Ablehnung zu dokumentieren. Sie setzt auch kein Organspenderegister voraus.

Mit einer engen Zustimmungslösung ist auch vereinbar, daß der Organspender seine Entscheidung z.B. einem nahen Angehörigen überträgt.

Anlage 16

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 9./10. März 1995

Sozialgesetzbuch VII
Verfassungsgemäßer Datenschutz für Unfallversicherte erforderlich

Durch die Träger der gesetzlichen Unfallversicherung werden oft Daten der Versicherten hinter deren Rücken oder zumindest ohne deren konkrete Kenntnis erhoben und weitergegeben. Der vorliegende Referentenentwurf des Bundesministeriums für Arbeit und Sozialordnung zum Unfallversicherungs-Einordnungsgesetz - SGB-VII sieht dazu keine Änderungen vor.

Aus dem Recht auf informationelle Selbstbestimmung der Versicherten, insbesondere auf Transparenz der einzelnen Verfahrensschritte, ergeben sich mehrere grundlegende Forderungen, die bei einer Überarbeitung des Referentenentwurfes berücksichtigt werden müssen:

1. **Auskunftspflicht behandelnder Ärzte gegenüber Unfallversicherungsträgern**
   Für behandelnde Ärzte sollte eine gesetzliche Auskunftspflicht gegenüber Unfallversicherungsträgern nur festgelegt werden, soweit dies erforderlich ist für eine sachgerechte und schnelle Heilung (§§ 557 Abs. 2 RVO - § 34 Referentenentwurf SGB VII). Die gesetzliche Auskunftspflicht ist daher auf Angaben über die Behandlung und den Zustand des Verletzten zu beschränken. Danach dürfen Vorerkrankungen, die aus Sicht des Arztes mit dem aktuellen Status in keinem Zusammenhang stehen oder keine Bedeutung im Zusammenhang mit dem Arbeitsunfall oder der Berufskrankheit haben, nicht übermittelt werden (Beispiel: Handverletzung und Salmonellenvergiftung).

2. **Datenerhebung, -verarbeitung und -nutzung durch Durchgangsärzte und Berufskrankheitenärzte**

   Soweit von den Unfallversicherungsträgern bestellte Durchgangsärzte personenbezogene Daten über den Unfallverletzten erheben und Unfallversicherungsträgern und anderen Stellen mitteilen, muß dies auf eine normenklare gesetzliche Grundlage gestellt werden; die bisherige Regelung in dem zwischen den Verbän-

den der Kassenärzte und der Unfallversicherungsträger geschlossenen "Ärzteabkommen" reicht für die damit verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen nicht aus. Entsprechendes gilt für die geplante Einführung eines Berufskrankheitenarztes.

3. Mitteilung personenbezogener Patientendaten durch Unfallversicherungsträger an ärztliche Gutachter

Im Hinblick auf das Recht der Betroffenen, der Bestellung eines bestimmten Gutachters im Einzelfall aus wichtigem Grund - z. B. wegen möglicher Befangenheit - zu widersprechen, haben die Betroffenen ein besonderes berechtigtes Interesse an der Transparenz dieser Datenübermittlungen.

Gesetzlich festzulegen ist daher, daß dem Betroffenen vor Übermittlung seiner Daten an einen Gutachter der Zweck des Gutachtens und die Person des Gutachters unter Hinweis auf sein Widerspruchsrecht nach § 76 Abs. 2 SGB X mitzuteilen sind.

4. Eingriffe der Unfallversicherungsträger und ihrer Verbände in das Recht auf informationelle Selbstbestimmung

Aufgaben der Unfallversicherungsträger und ihrer Verbände und ihre Befugnisse zur Datenerhebung, -verarbeitung und -nutzung - einschließlich der Aufbewahrungsfristen - sind differenziert in der verfassungsrechtlich gebotenen Klarheit gesetzlich zu regeln. Der vorliegende Referentenentwurf erscheint in diesem Punkt weitgehend unzureichend. So werden undifferenziert Unfallversicherungsträger und ihre Verbände behandelt, die Fachaufgaben dieser Stellen nicht oder nicht hinreichend deutlich genannt und andererseits Selbstverständlichkeiten wie das Führen von Dateien über erforderliche Daten aufgeführt. Außerdem beschränkt sich die Regelung auf die Datenverarbeitung in Dateien und übergeht die gerade im Bereich der Berufsgenossenschaften mit Gutachten und ähnlichen Unterlagen stark ausgeprägte Datenverarbeitung in Akten.

Die Zuweisung von Aufgaben und Befugnissen an Verbände der gesetzlichen Unfallversicherung muß zudem wie bei allen anderen Verbänden von Leistungsträgern durch die Einrichtung einer staatlichen Aufsicht ergänzt werden.

Soweit Vorschriften der Unfallversicherungsträger und ihrer Verbände (z. B. Unfallverhütungsvorschriften) durch Regelungen über die Erhebung, Verarbeitung und

Nutzung sensibler medizinischer Daten in das Recht auf informationelle Selbstbestimmung eingreifen, sind diese Eingriffe gesetzlich zu regeln.

5. Anzeige eines Berufsunfalls und einer Berufskrankheit

Bei Datenschutzkontrollen der bisherigen Anzeigen von Berufsunfällen und -krankheiten hat sich gezeigt, daß der Umfang der an die verschiedenen Stellen übermittelten Daten zum Teil dem Grundsatz der Verhältnismäßigkeit, insbesondere der Erforderlichkeit nicht Rechnung trägt. Der Inhalt dieser Anzeigen muß an diesen Grundsätzen gemessen neu festgelegt werden.

6. Zentraldateien mehrerer Unfallversicherungsträger oder ihrer Verbände

Zweck und Inhalt zentral geführter Dateien sind in angemessenem Umfang gesetzlich präzise zu regeln. Dasselbe gilt für die Datenverarbeitung und -nutzung sowie die Festlegung der jeweils speichernden Stelle.

Die rechtzeitige Beteiligung des jeweils zuständigen Bundes- oder Landesbeauftragten für den Datenschutz vor Einrichtung einer Zentraldatei ist vorzusehen.

7. Anforderung medizinischer Unterlagen bei anderen Sozialleistungsträgern

Der in § 76 Abs. 2 SGB X vorgesehene Hinweis auf das Widerspruchsrecht gegen die Übermittlung medizinischer Daten geht stets dann ins Leere, wenn bei der speichernden bzw. übermittelnden Stelle kein Verwaltungsverfahren läuft.

Es ist daher festzulegen, daß ein Unfallversicherungsträger vor der Anforderung von Sozialdaten im Sinne des § 76 SGB X bei anderen Sozialleistungsträgern den Versicherten auf dessen Widerspruchsrecht nach § 76 Abs. 2 SGB X gegenüber der übermittelnden Stelle hinzuweisen hat.

8. Akteneinsichtsrecht der Versicherten

Hinsichtlich des gesetzlichen Akteneinsichtsrechts nach § 25 SGB X treten in der Praxis seitens der Unfallversicherungsträger Unsicherheiten auf, ob zum Schutz von Betriebs- und Geschäftsgeheimnissen oder Urheberrechten das Einsichtsrecht beschränkt werden muß. Hierzu ist eine gesetzliche Klarstellung geboten, daß diese Rechte dem Akteneinsichtsrecht nicht entgegenstehen.

Anlage 17

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 22./23. Oktober 1996

Automatisierte Übermittlung von Abrechnungsdaten durch Kassenzahnärztliche Vereinigungen an gesetzliche Krankenkassen

Der in dem Schiedsspruch vom 20. Februar 1995 für die Abrechnung festgelegte Umfang der Datenübermittlung zwischen Kasssenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen erfüllt nicht die Anforderungen des Sozialgesetzbuches an diesen Datenaustausch.

§ 295 SGB V fordert, daß Daten nur **im erforderlichen Umfang** und **nicht versichertenbezogen** übermittelt werden dürfen.

Die Datenschutzbeauftragten begrüßen es deshalb, daß der größte Teil der gesetzlichen Krankenkassen in "Protokollnotizen" - Stand 22. März 1996 - den Umfang der zu übermittelnden Daten reduziert hat. Das Risiko der Identifizierbarkeit des Versicherten wurde dadurch deutlich verringert. Zum letztlich erforderlichen Umfang haben die Spitzenverbände der gesetzlichen Krankenkassen erklärt, daß genauere Begründungen für die Erforderlichkeit der Daten erst gegeben werden könnten, wenn das DV-Projekt für das Abrechnungsverfahren auf Kassenseite weit genug entwickelt sei.

Der Verband der Angestellten-Ersatzkassen (VdAK) hat bisher als einziger Spitzenverband der gesetzlichen Krankenkassen diese Datenreduzierungen nicht mitgetragen. Die Datenschutzbeauftragten fordern den VdAK auf, sich für die Frage der Datenübermittlung zwischen Kassenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen der einheitlichen Linie anzuschließen. Dies liegt im gesetzlich geschützten Interesse der Versicherten.

Die besonderen Vorgaben des Sozialgesetzbuches für die Prüfung der Wirtschaftlichkeit der ärztlichen Abrechnung werden dadurch nicht berührt.

Anlage 18

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 9./10. März 1995

Eingeschränkter Zugriff auf Versichertendaten bei landesweiten oder überregionalen gesetzlichen Krankenkassen

Die gesetzlichen Krankenkassen schließen sich zunehmend zu landesweiten oder überregionalen gesetzlichen Krankenkassen zusammen. Es stellt sich daher verstärkt die Frage, welche bzw. wiewiele Geschäftsstellen solcher Krankenkassen umfassend auf alle gespeicherten Daten eines Versicherten zugreifen können.

Die Datenschutzbeauftragten halten nur folgendes für vertretbar:

1. Geschäftsstellen einer Krankenkasse können ohne schriftliches Einverständnis des Versicherten nur auf einen "Stammdatensatz" zugreifen. Dieser "Stammdatensatz" darf nur den Namen, das Geburtsdatum, die Anschrift, die Krankenversichertennummer und die betreuende Geschäftsstelle des Versicherten umfassen.

2. Lediglich eine Geschäftsstelle kann umfassend auf den Datensatz eines Versicherten zugreifen, sofern der Versicherte nicht ausdrücklich und eindeutig schriftlich in derartige Zugriffsmöglichkeiten durch weitere Geschäftsstellen eingewilligt hat.

3. Vor der Einwilligung ist der Betroffene umfassend aufzuklären. Die Daten dürfen nur zweckgebunden verwendet werden.

Anlage 19

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 09./10. November 1995

Datenschutzrechtliche Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 47. Konferenz am 09./10. März 1994 kritisch zum Einsatz von Chipkarten im Gesundheitswesen Stellung genommen. In dem Beschluß wird die Nutzung von Patientenkarten von mehreren Voraussetzungen zur Sicherung des Persönlichkeitsrechts abhängig gemacht.

Seitdem werden in mehreren Ländern Modellversuche und Pilotprojekte durchgeführt. Die Bandbreite reicht

- von allgemeinen Patientenkarten, die an möglichst viele Patienten/Versicherte ausgegeben werden, eine Vielzahl von Krankheitsdaten enthalten und von einem unbestimmten Kreis von Personen und Institutionen des Gesundheitswesens zu vielfältigen Zwecken verwendet werden können (z.B. Vital-Card der AOK Leipzig, Persönliche Patientenkarte Neuwied, BKK-Patientenkarte Berlin)
- bis zu krankheitsspezifischen Karten für bestimmte Patientengruppen mit reduziertem Datensatz und einer Definition der Verwendung (z.B. Dialyse-Card, Diab-Card, Krebsnachsorgekarte, Defi-Card).

Datenschutzrechtlich stellen sich vor allem folgende Probleme:

- Die massenhafte Einführung der Karten erzeugt einen sozialen Druck auf die Betroffenen, sie mitzuführen und vorzuzeigen. Diesen Erwartungen wird sich der Betroffene vielfach nur unter Befremden des Arztes oder sogar der Gefahr, daß dieser die Behandlung ablehnt, verweigern können.
- Die Verwendung von allgemeinen Patientenkarten bringt die Gefahr einer pauschalen Offenbarung von medizinischen Daten mit sich.
- Dem Patienten wird die Last aufgebürdet, für die Sicherheit seiner medizinischen Daten selbst zu sorgen.

Die Datenschutzbeauftragten fordern alle für Kartenprojekte im Gesundheitswesen Verantwortlichen in Politik, Industrie, Ärzteschaft, Wissenschaft und in den Krankenversicherungen auf, das Recht auf informationelle Selbstbestimmung der betroffenen Patienten bzw. Versicherten zu gewährleisten. Die 50. Konferenz hält folgende Voraussetzungen für elementar:

1. Besondere Schutzwürdigkeit medizinischer Daten

Medizinische Daten sind besonders schutzwürdig, unabhängig davon, welche Technologien eingesetzt werden, ob die Patientendaten beim Arzt gespeichert und versandt oder über ein Netz abgerufen werden oder ob der Patient die Daten auf einer Chipkarte bei sich hat. Es handelt sich oftmals um belastende, schicksalhafte Daten. Zudem geht es nicht nur um Daten des Patienten, sondern auch um fremde Einblicke in die ärztliche Tätigkeit.

2. Wirksame Entscheidung der Betroffenen über die Verwendung einer Karte

Die freie Entscheidung der Betroffenen (Patienten/Versicherten), eine Chipkarte zu verwenden, muß gewährleistet sein. Dies umfaßt die Entscheidung,

- ob Daten auf einer Chipkarte gespeichert werden,
- welche der Gesundheitsdaten auf die Karte aufgenommen werden,
- welche Daten auf der Karte wieder gelöscht werden,
- ob die Karte bei einem Arztbesuch bzw. einem Apothekenbesuch vorgelegt wird und
- welche Daten im Einzelfall zugänglich gemacht werden.

Ein Widerruf der Entscheidung muß ohne Nachteile für die Betroffenen möglich sein. Die gleiche Freiheit der Entscheidung für oder gegen die Verwendung der Chipkarte muß für Ärzte und Apotheker gewährleistet sein. Eine wirksame Entscheidung für oder gegen die Verwendung einer Chipkarte setzt eine schriftliche, objektive, vollständige und nachvollziehbare Information über Zweck, Art, Umfang und Beteiligte der Chipkarten-Kommunikation voraus. Das Gesamtkonzept des Chipkarteneinsatzes und der damit verbundenen Datenverarbeitung muß für die Betroffenen überschaubar sein.

Auf der Karte darf nicht der Datensatz der Krankenversichertenkarte nach § 291 Abs. 2 SGB V, insbesondere nicht die Krankenversicherung und die Krankenversiche-

rungsNr., gespeichert werden, da andernfalls - zumal bei allgemeinen Patientenkarten mit hohem Verbreitungsgrad - die Krankenversichertenkarte verdrängt und deren Nutzungsbeschränkungen umgangen werden.

3. Freiheit der Entscheidung

Die uneingeschränkte Freiheit der Entscheidung der Betroffenen für oder gegen die Verwendung einer Chipkarte muß gewährleistet sein, denn der Einsatz von Chipkarten im Gesundheitswesen führt keineswegs zwangsläufig zu größerer Autonomie der Patienten. Neue Technologien können sich auch als Verführung erweisen, deren Preis erst langfristig erkennbar wird. Die individuelle Entscheidung des Bürgers über die Verarbeitung seiner Daten war und bleibt ein zentrales Recht gegenüber Eingriffen in seine Freiheitssphäre. Mit der Chipkarte können sich jedoch Situationen ergeben, in denen wirkliche Freiheit, tatsächliche Wahlmöglichkeit der Betroffenen nicht mehr gewährleistet sind und durch technische und organisatorische, rechtliche und soziale Rahmenbedingungen wiederhergestellt werden müssen.

Dem Staat kommt hier eine veränderte Rolle zu: Freiheitsrechte nicht einzuschränken, sondern sie zu sichern, wo Entwicklungen des Marktes und der Technologien sowie Gruppeninteressen die Entscheidungsfreiheit des Bürgers bedrohen. Die Technologie selbst kann für die Sicherung der Freiheitsrechte ein wertvolles Hilfsmittel sein. Darüber hinaus kommt der Informiertheit der Betroffenen ein zentraler Stellenwert zu. Ihre Kompetenz zur Entscheidung und zum praktischen Umgang mit der Karte muß gestärkt werden, damit sie auch langfristig die größtmöglichen Chancen haben, ihre Interessen durchzusetzen.

Mit der Ausstellung der Karte dürfen nur die Vorteile verknüpft werden, die sich unmittelbar aus den Nutzungspraktiken der Karte selbst ergeben. Die freie Entscheidung der Betroffenen, eine Karte zu nutzen oder dies abzulehnen, darf nicht durch einen Nutzungszwang oder eine Bevorzugung von Karten-Nutzern (z.B. durch Bonuspunkte) bzw. durch eine Benachteiligung von Karten-Verweigerern eingeschränkt werden.

4. Keine Verschlechterung der Situation der Betroffenen

Durch die Einführung von Kommunikationssystemen mit Chipkarten dürfen die Betroffenen nicht schlechter gestellt werden als im konventionellen Verfahren. Die medizinische Versorgung, der Schutz der Gesundheitsdaten und die Mitentscheidungsrechte der Betroffenen müssen in Umfang und Qualität erhalten bleiben.

Das therapeutische Verhältnis Arzt/Patient darf sich durch den Einsatz von Chipkarten nicht verschlechtern. Freiheit und Vertrauen innerhalb des Arzt-Patienten-Verhältnisses sowie der Grundsatz der Abschottung der dem Arzt anvertrauten Informationen und der ärztlichen Erkenntnisse nach außen, gegen die Kenntnisnahme durch Dritte, müssen erhalten bleiben. Insbesondere muß der Gesetzgeber sicherstellen, daß die auf der beim Patienten befindlichen Chipkarte gespeicherten medizinischen Daten ebenso gegen Beschlagnahme und unbefugte Kenntnisnahme geschützt sind wie die beim Arzt gespeicherten Daten. Eine Kommunikation unter Vorlage der Karte mit Personen oder Stellen außerhalb des Arzt-Patienten-Verhältnisses, z.B. Arbeitgebern oder Versicherungen, muß vom Gesetzgeber untersagt werden.

Das sich im Gespräch entwickelnde Vertrauensverhältnis zwischen Arzt und Patient darf nicht durch eine Chipkarten-vermittelte Kommunikation verdrängt werden. Verkürzte Darstellungen medizinischer Sachverhalte auf der Chipkarte - z.B. mit Hilfe von Schlüsselbegriffen - dürfen nicht zu einer Minderung der Qualität des therapeutischen Verhältnisses führen; das liegt auch im Interesse des Arztes. Der Patient muß auch weiterhin die Möglichkeit des individuellen Dialogs wählen können. Dies schließt insbesondere die Freiheit des Betroffenen ein, eine Chipkarte im Einzelfall nicht vorzulegen, auf der Chipkarte nur einen begrenzten Datensatz speichern zu lassen oder zu entscheiden, welchem Arzt welche Informationen oder Informationsbereiche offenbart werden. Der Patient darf durch die Ausgestaltung und den Verwendungszusammenhang der Chipkarte nicht zur pauschalen Offenbarung seiner Daten gezwungen sein. So sind Daten auf der Chipkarte so zu ordnen, daß z.B. beim Zahnarzt die gynäkologische Behandlung geheim bleiben kann.

Es darf keine "Einwilligung" in Chipkarten und Chipkartensysteme mit verminderter Datensicherheit geben. Der Gesetzgeber muß die Patienten vor "billigen Gesundheitskarten" ohne ausreichende Sicherung vor einer Nutzung durch Dritte schützen.

5. Sicherstellung der Integrität und Authentizität der Daten

Zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der Daten auf Chipkarten im Gesundheitswesen und zur Differenzierung der Zugriffsmöglichkeiten nach dem Grundsatz der Erforderlichkeit in unterschiedlichen Situationen sind kryptographische Verfahren sowie geeignete Betriebssysteme zur Abschottung unterschiedlicher Anwendungsbereiche nach dem Stand der Technik in Chipkarten und Schreib-/Lese-Terminals zu implementieren. Eine Protokollierung der Lösch- und Schreibvorgänge auf der Karte ist unverzichtbar.

Darüber hinaus ist für das infrastrukturelle Kartenumfeld (Herstellung, Verteilung, Personalisierung,..., Rücknahme) sicherzustellen, daß ausreichende technische und organisatorische Maßnahmen Berücksichtigung finden. Für die zur Erstellung und Personalisierung von Gesundheits-Chipkarten dienenden Systeme sowie die informationstechnischen Systeme und Verfahren, mit denen Daten auf der Chipkarte gelesen, eingetragen, verändert, gelöscht oder verarbeitet werden, muß der gleiche hohe Sicherheitsstandard erreicht werden.

6. Keine neuen zentralen medizinischen Datensammlungen

Der Einsatz von Chipkarten im Gesundheitswesen darf nicht zur Entstehung neuer zentraler Dateien von Patientendaten bei Kassenärztlicher Vereinigung, Krankenkassen, Kartenherstellern oder sonstigen Stellen führen. Dies gilt auch für das Hinterlegen von Sicherungskopien der auf der Karte gespeicherten medizinischen Daten. Es steht in der freien Entscheidung der Betroffenen, ob sie dem Arzt ihres Vertrauens eine umfassende Pflege aller Chipkarten-Daten - einschließlich der Sicherungskopien - übertragen oder nicht.

7. Leserecht des Karteninhabers

Der Karteninhaber muß das Recht und die Möglichkeit haben, seine auf der Chipkarte gespeicherten Daten vollständig zu lesen.

8. Suche nach datenschutzfreundlichen Alternativen

Angesichts der aufgezeigten Gefährdungen der informationellen Selbstbestimmung im Gesundheitswesen muß die Suche nach datenschutzfreundlichen Alternativen zur Chipkarte fortgesetzt werden.

Vorstehende Kriterien sind der Maßstab für die datenschutzrechtliche Bewertung von Projekten für die Einführung von Chipkarten im Gesundheitswesen.

Die Datenschutzbeauftragten von Bund und Ländern fordern die Gesetzgeber auf, die dringend notwendigen Regelungen zur Sicherung der Rechte von Patienten und Ärzten zu schaffen. Ebenso ist durch die Gesetzgeber den Besonderheiten der Datenverarbeitung auf Chipkarten durch bereichsspezifische Regelungen Rechnung zu tragen.

Anlage 20

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 09./10. November 1995

Datenschutz bei der Neuordnung der Telekommunikation (Postreform III)

Mit der Postreform III soll die Neugestaltung des Telekommunikationssektors in Deutschland nach den Vorgaben des Liberalisierungskonzepts der Europäischen Union abgeschlossen werden. Entstehen wird ein riesiger Markt mit einer Vielzahl von großen und kleinen, teilweise auch grenzüberschreitend tätigen Netzbetreibern und Diensteanbietern. Die Akteure auf diesem Telekommunikationsmarkt werden zum größeren Teil als Privatunternehmen operieren, es werden aber auch öffentliche Stellen ihre Leistungen anbieten. Der gesetzgeberische Abschluß der Liberalisierung und der Privatisierung des TK-Sektors wird die rechtliche Grundlage bilden für den endgültigen Eintritt in das Zeitalter von weltweiter Vernetzung, Multimedia und interaktiven Diensten und damit für den rapiden Anstieg des Konsums von Angeboten der Telekommunikation, des interaktiven Rundfunks und der Datenverarbeitung.

Die Konsequenzen sind absehbar: Gegenüber der heutigen Situation werden unvergleichlich mehr personenbezogene Daten durch mehr Stellen registriert und ausgewertet werden. Betroffen sind alle, die fernsehen, telefonieren, fernkopieren, Texte und Dokumente über Datenleitung schicken oder Telebanking oder Teleshopping betreiben. Die Risiken für den Einzelnen durch die vermehrten Möglichkeiten der Verhaltens- und Umfeldkontrolle oder der Ausforschung persönlicher Lebensgewohnheiten und Eigenschaften vergrößern sich entsprechend.

Der vom Bundesministerium für Post und Telekommunikation vorgelegte Referentenentwurf für ein Telekommunikationsgesetz (TKG-E, Stand: 06.10.95) macht es erforderlich, erneut die Realisierung der grundlegenden Rahmenbedingungen für eine datenschutzgerechte Gestaltung der künftigen Telekommunikationslandschaft - soweit die Gesetzgebungskompetenz des Bundes betroffen ist - anzumahnen.

Ein wirksamer Datenschutz muß - wie bereits jetzt gesetzlich fixiert - auch künftig gleichberechtigtes Regulierungsziel neben z.B. der Sicherstellung der flächendeckenden Grundversorgung mit Telekommunikationsdienstleistungen bleiben.

Kundenwünsche nach variablerer und komfortablerer Nutzung der technischen Möglichkeiten werden zunehmen. Gerade deshalb müssen die Prinzipien der Datenvermeidung und der strikten Begrenzung der Datenverarbeitung auf das erforderliche Ausmaß ihren Vorrang bei der Ausgestaltung der kommunikationstechnischen Infrastruktur behalten. Netzbetreiber und Diensteanbieter sollten verpflichtet werden, überall dort, wo dies technisch möglich ist, auch anonyme Zugangs- und Nutzungsformen für ihre Leistungen bereitzustellen. Für eine sichere Datenübertragung sind ohnè prohibitive Zusatzkosten wirksame Verschlüsselungsverfahren bereitzustellen.

Das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis müssen für alle Netzbetreiber und Diensteanbieter ungeachtet ihrer Rechtsform und ihrer Kundenstruktur (z.B. sog. Corporate Networks) einheitlich auf einem hohen Niveau gesichert werden. Der bisherige Schutzstandard darf keinesfalls unter den durch die Postreform II erreichten Stand gesenkt werden. Ein hohes Datenschutzniveau ist als Grundversorgung unabdingbar; seine Gewährleistung sollte deshalb Teil der Universaldienstleistung sein. Die in Grundrechte eingreifenden Regelungen sind im Telekommunikationsgesetz selbst und nicht in Verordnungen zu treffen. Die untergesetzlichen, den Datenschutz betreffenden Normen gehören in eine einzige, nicht verstreut in mehrere Verordnungen.

Entscheidend für die Wirksamkeit des Grundrechtsschutzes ist die strikte Einhaltung der Zweckbindung der Verbindungs- und Rechnungsdaten. Das "Feststellen mißbräuchlicher Inanspruchnahme" oder die "bedarfsgerechte Gestaltung" von TK-Leistungen dürfen nicht als Anlaß für eine umfassende Auswertung dieser Angaben oder sogar der Nachrichteninhalte herangezogen werden.

Für den Kunden bzw. Teilnehmer ist es von größter Bedeutung, die Verarbeitungsvorgänge im TK-Bereich überschauen zu können. Er muß auch künftig über die Nutzungsrisiken bestimmter Kommunikationstechniken (z.B. Mobilfunk) ebenso wie über seine Widerspruchsmöglichkeiten umfassend aufgeklärt werden. Keinesfalls darf die Einwilligung des Betroffenen mißbraucht werden um bereichsspezifischer Schutznormen oder effiziente Datensicherungsvorkehrungen zu umgehen.

Um auch und gerade für das besonders schutzwürdige Fernmeldegeheimnis einen durchgängig hohen Schutzstandard zu sichern, braucht es eine unabhängige Kontrolle nach bundesweit einheitlichen Kriterien. Die Zuweisung dieser Überwachungsaufgabe an die im TKG-Entwurf vorgesehene Regulierungsbehörde ist wegen deren mangelhafter Unabhängigkeit und der von ihr wahrzunehmenden Regu-

lierungsaufgaben, die mit Interessenkonflikten verbunden sein werden, nicht akzeptabel.

Deshalb sollte aufgrund seiner langjährigen fachlichen Erfahrung bei der Kontrolle der TELEKOM und seiner umfassenden Querschnittskenntnisse im TK-Bereich der Bundesbeauftragte für den Datenschutz eine zentrale Funktion für die Kontrolle im Telekommunikationsbereich erhalten. Die Aufgaben, die die Landesbeauftragten für den Datenschutz und die Aufsichtsbehörden im Rahmen ihrer Zuständigkeiten erfüllen, sind gesetzlich klar zu regeln.

Die Akzeptanz der Informationsgesellschaft der Zukunft hängt wesentlich ab von der Sicherung des Grundrechts auf unbeobachtete Kommunikation. Das Telekommunikationsgesetz wird einen entscheidenden Baustein für die rechtliche Ausgestaltung der künftigen TK-Infrastruktur bilden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher dazu auf, die von ihr vorgeschlagenen Regelungen im weiteren Gesetzgebungsverfahren zu berücksichtigen und sich für ihre Umsetzung auch auf der europäischen Ebene (z.B. in der ISDN-Richtlinie) einzusetzen.

Anlage 21

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19. September 1995

Entwurf einer Telekommunikations- und Informationsdienstunternehmen-Datenschutzverordnung (TIDSV) des Bundesministeriums für Post und Telekommunikation (Stand: 6. Juni 1995)

Das Bundesministerium für Post- und Telekommunikation hat den Entwurf einer Telekommunikations- und Informationsdienstunternehmen-Datenschutzverordnung (TIDSV) vorgelegt, der auf der Grundlage des bereits seit Anfang dieses Jahres geltenden Gesetzes über die Regulierung der Telekommunikation und des Postwesens (PTRegG) den Schutz personenbezogener Daten der am Fernmeldeverkehr beteiligten Bürger regeln soll. Die Verordnung muß entsprechend der gesetzlichen Vorgabe dem Grundsatz der Verhältnismäßigkeit genügen, insbesondere hat sie die Erhebung, Verarbeitung und Nutzung der Daten auf das Erforderliche zu beschränken und ihre Zweckbindung zu gewährleisten. Die Datenschutzbeauftragten des Bundes und der Länder stellen fest, daß der vorliegende Entwurf diesen aus der Verfassung abgeleiteten gesetzlichen Vorgaben teilweise nicht genügt.

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung vom 8. März 1991 auf die Bedeutung des Grundrechts auf unbeobachtete Kommunikation hingewiesen und gefordert, daß das Telekommunikationsdatenschutzrecht dieses Grundrecht zu sichern hat. Im Zeitalter der elektronischen Information und Kommunikation ist es geboten, die Betreiber zur Bereitstellung anonymer Nutzungsmöglichkeiten zu verpflichten und den Bürger in die Lage zu versetzen, selbst zu entscheiden, ob er seine personenbezogenen Daten preisgeben und sich den damit verbundenen Risiken aussetzen will.

Im einzelnen halten die Datenschutzbeauftragten den vorliegenden Entwurf in folgenden Punkten für verbesserungsbedürftig, auch um eine Absenkung des Datenschutzniveaus gegenüber der gegenwärtigen Rechtslage zu verhindern:

- Die Verarbeitung von Kundendaten muß auch in Zukunft ausdrücklich auf Telekommunikationszwecke und Zwecke der Informationsdienstleistung beschränkt werden; jede Aufweichung des Zweckbindungsgrundsatzes ist abzulehnen.

- Auch im Bereich des Sprachtelefondienstes soll nach dem Entwurf die Speicherung der vollständigen Rufnummer des angerufenen Teilnehmers bis zu 80 Tagen nach Rechnungsversand zur Regel werden. Bislang war dies nur vorgesehen, wenn der Anrufer einen Einzelverbindungsnachweis beantragt hat; dabei sollte es auch in Zukunft bleiben.

- Eine Auswertung der Verbindungsdaten nach Zielrufnummern auch außerhalb des Sprachtelefondienstes ohne Einwilligung des Kunden ist nach § 10 Abs. 2 Nr. 2 PTRegG unzulässig. Hiernach „dürfen Daten des Anrufenden nur mit dessen Einwilligung verwendet und müssen Daten des Angerufenen unverzüglich anonymisiert werden."

- Die Übermittlung von Verbindungsdaten an Diensteanbieter darf auch für Zwecke des Entgelteinzuges weiterhin nur mit Einwilligung des Kunden zugelassen werden, wenn der Datenempfänger sich vertraglich zur Einhaltung des Fernmeldegeheimnisses verpflichtet hat.

- Ein Einzelverbindungsnachweis sollte auch in Zukunft nur erteilt werden, wenn der Antragsteller das Einverständnis der zum Haushalt gehörenden Mitbenutzer des Anschlusses nachweisen kann.

- Die Anonymität von Anrufern bei Beratungseinrichtungen muß auch dann gewährleistet sein, wenn sie über ein Mobilfunknetz anrufen. Es ist nicht nachzuvollziehen, daß gerade an den dynamischsten und modernsten Teilbereich der Telekommunikation geringere Datenschutzanforderungen gestellt werden sollen als an das traditionelle Festnetz. Ohnehin ist eine Entwicklung absehbar, die Mobilfunk- und Festnetze zusammenwachsen läßt.

- Der Anrufer muß im Sprachtelefondienst die kostenfreie Möglichkeit haben, die Übermittlung seiner Rufnummer an den angerufenen Anschluß dauernd oder fallweise auszuschließen.

- Beim angerufenen Anschluß im Sprachtelefondienst muß auch in Zukunft die Abschaltung der Rufnummernanzeige allgemein und im Einzelfall möglich sein, damit

Personen, die sich in räumlicher Nähe zum Angerufenen aufhalten, nicht zwangsläufig Kenntnis vom jeweiligen Anrufer erhalten.

– Die regelmäßige Herausfilterung der Daten solcher Verbindungen, für die tatsächliche Anhaltspunkte den Verdacht eines strafbaren Mißbrauchs von Fernmeldeanlagen oder der mißbräuchlichen Inanspruchnahme von Telekommunikations- oder Informationsdienstleistungen begründen, kommt einer präventiven Rasterfahndung der dem Fernmeldegeheimnis unterliegenden Verbindungsdaten gleich, in die bereits im Vorfeld eines konkreten Verdachts sämtliche Teilnehmer einbezogen werden. Die entsprechende Regelung sollte dieses Verfahren lediglich auf den Einzelfall beschränken.

– Hinsichtlich der Erhebung, Verarbeitung und Nutzung von Nachrichteninhalten sind die strengen Vorgaben von § 10 Abs. 2 Sätze 2-5 PTRegG einzuhalten. Insoweit fehlt in dem vorliegenden Entwurf eine Einschränkung auf den Einzelfall und die Verankerung der nach § 10 PTRegG vorgesehenen Informations- und Unterrichtungspflichten.

– Die geplante Umwandlung der bisherigen Telefonauskunft ist datenschutzrechtlich nur vertretbar, wenn der Kunde über die Verwendungsmöglichkeit in der Telefonauskunft und sein Widerspruchsrecht hinreichend informiert wird. So muß er insbesondere wissen, daß nicht nur seine Rufnummern, sondern sämtliche Angaben, die er für die Teilnehmerverzeichnisse freigegeben hat, auch beauskunftet und verwendet werden können, sofern er dem nicht widersprochen hat.

– Die vorgesehenen Regelungen über öffentliche Kundenverzeichnisse und die Telefonauskunft tragen den besonderen Risiken der Verbreitung von Kundendaten in elektronischer Form, etwa auf CD-ROM oder durch Abruf aus Online-Diensten (Adreß-Selektion, bundesweite Recherche, umgekehrte Rufnummernsuche) nicht Rechnung. Der Kunde muß ein differenziertes Widerspruchsrecht erhalten, das ihm ermöglicht, seine Daten zwar in das herkömmliche Telefonbuch aufnehmen oder von der Telefonauskunft mitteilen zu lassen, eine Aufnahme in elektronische Verzeichnisse mit qualitativ weitergehenden Verarbeitungsmöglichkeiten jedoch zu unterbinden.

– Der Verordnungsentwurf läßt abweichend von der gegenwärtigen Praxis bei der Deutschen Telekom AG die Erstellung von Einzelverbindungsnachweisen mit vollständigen Zielrufnummern ohne Einflußmöglichkeit der angerufenen Kunden zu. Die Anonymität des Angerufenen wird aber auch durch die Verkürzung der Zielruf-

nummer um die letzten drei Ziffern nicht hinreichend gewährleistet. Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung vom 9./10. März 1994 darauf hingewiesen, daß dem Schutz des informationellen Selbstbestimmungsrechts und des Fernmeldegeheimnisses des Angerufenen am besten dadurch entsprochen würde, wenn jeder inländische Anschlußinhaber selbst entscheiden könnte, ob und gegebenenfalls wie seine Rufnummer auf Einzelverbindungsnachweisen erscheinen soll. Obwohl ein entsprechendes Verfahren in den Niederlanden bereits erfolgreich praktiziert wird, hat der Bundesminister für Post und Telekommunikation diesen Vorschlag bisher nicht aufgegriffen.

- Die Vorschriften für Bildschirmtextdienste sollten, auch im Sinne der Rechtssicherheit, möglichst weitgehend mit denen des Bildschirmtext-Staatsvertrages harmonisiert werden. Insbesondere sollte die Speicherung von Abrechnungsdaten so beschränkt werden, daß Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von den einzelnen Kunden in Anspruch genommener Angebote nicht erkennbar sind, es sei denn, der Kunde beantragt mit Einverständnis der Mitbenutzer einen Einzelverbindungsnachweis. Ferner ist vorzusehen, daß Abrechnungsdaten nicht erst sechs Monate nach Bekanntgabe der Entgeltrechnung gelöscht werden, sondern unverzüglich, wenn sie für Abrechnungszwecke nicht mehr erforderlich sind.

Anlage 22

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 29. April 1996

Eckpunkten für die datenschutzrechtliche Regelung von Mediendiensten

In letzter Zeit finden Online-Dienste und Multimedia-Anwendungen zunehmend Verbreitung. Mit den - häufig multimedialen - Angeboten, auf die interaktiv über Telekommunikationsnetze zugegriffen werden kann, sind besondere Risiken für das Recht auf informationelle Selbstbestimmung der Teilnehmer verbunden; hinzuweisen ist insbesondere auf die Gefahr, daß das Nutzerverhalten unbemerkt registriert und zu Verhaltensprofilen zusammengeführt wird. Das allgemeine Datenschutzrecht reicht nicht aus, die mit den neuen technischen Möglichkeiten und Nutzungsformen verbundenen Risiken wirkungsvoll zu beherrschen.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für dringend erforderlich, durch bereichsspezifische Regelungen technische und rechtliche Gestaltungsanforderungen für die elektronischen Dienste zu formulieren, die den Datenschutz sicherstellen. Leitlinie sollte hierbei der Grundsatz der Datenvermeidung bzw. -minimierung sein. Die Datenschutzbeauftragten haben dazu in einer Entschließung vom 14./15. März 1996 zur Modernisierung und zur europäischen Harmonisierung des Datenschutzrechts vorgeschlagen, daß die informationelle Selbstbestimmung bei Multimediadiensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsverfahren anzubieten, durch den Schutz vor übereilter Einwilligung, z.B. durch ein Widerspruchsrecht, und durch strenge Zweckbindung für die bei der Verbindung, Nutzung und Abrechnung anfallenden Daten sichergestellt wird.

Die Datenschutzbeauftragten weisen darauf hin, daß auch mit Inhalten, die durch Mediendienste verbreitet werden, datenschutzrechtliche Probleme verbunden sein können. Auf diese Probleme wird im folgenden jedoch - ebenso wie auf die Datenschutzaspekte der Telekommunikation - nicht näher eingegangen. Bei den datenschutzrechtlichen Eckpunkten wird ferner bewußt darauf verzichtet, den Regelungsort - etwa einen Länder-Staatsvertrag oder ein Bundesgesetz - anzugeben. Die Datenschutzbeauftragten appellieren an die Gesetzgeber in Bund und Ländern, eine ange-

messene datenschutzgerechte Regulierung der neuen Dienste nicht an Kompetenzstreitigkeiten scheitern zu lassen.

1. Anonyme bzw. datensparsame Nutzung: Die Dienste und Multimedia-Einrichtungen sollten so gestaltet werden, daß keine oder möglichst wenige personenbezogene Daten erhoben, verarbeitet und genutzt werden; deshalb sind auch anonyme Nutzungs- und Zahlungsformen anzubieten. Auch zur Aufrechterhaltung und zur bedarfsgerechten Gestaltung von Diensten und Dienstleistungen (Systempflege) sind soweit wie möglich anonymisierte Daten zu verwenden. Soweit eine vollständig anonyme Nutzung nicht realisiert werden kann, muß jeweils geprüft werden, ob durch andere Verfahren, z.B. die Verwendung von Pseudonymen, ein unmittelbarer Personenbezug vermieden werden kann. Die Herstellung des Personenbezugs sollte bei diesen Nutzungsformen nur dann erfolgen, wenn hieran ein begründetes rechtliches Interesse besteht.

2. Bestandsdaten: Bestandsdaten dürfen nur in dem Maße erhoben, verarbeitet und genutzt werden, soweit sie für die Begründung und Abwicklung eines Vertragsverhältnisses sowie für die Systempflege erforderlich sind. Die Bestandsdaten dürfen zur bedarfsgerechten Gestaltung von Diensten und Dienstleistungen sowie zur Werbung und Marktforschung genutzt werden, soweit der Betroffene dem nicht widersprochen hat. Für die Werbung und Marktforschung durch Dritte dürfen Bestandsdaten nur mit der ausdrücklichen Einwilligung des Betroffenen verarbeitet werden.

3. Verbindungs- und Abrechnungsdaten: Verbindungs- und Abrechnungsdaten dürfen nur für Zwecke der Vermittlung von Angeboten und für Abrechnungszwecke erhoben, gespeichert und genutzt werden. Sie sind zu löschen, wenn sie für die Erbringung der Dienstleistung oder für Abrechnungszwecke nicht mehr erforderlich sind. Soweit Verbindungsdaten ausschließlich zur Vermittlung einer Dienstleistung gespeichert werden, sind sie spätestens nach Beendigung der Verbindung zu löschen. Die Speicherung der Abrechnungsdaten darf den Zeitpunkt, die Dauer, die Art, den Inhalt und die Häufigkeit bestimmter von den einzelnen Teilnehmern in Anspruch genommener Angebote nicht erkennen lassen, es sei denn, der Teilnehmer beantragt eine dahingehende Speicherung. Verbindungs- und Abrechnungsdaten sind einer strikten Zweckbindung zu unterwerfen. Sie dürfen über den hier genannten Umfang hinaus nur mit der ausdrücklichen Einwilligung des Betroffenen erhoben, verarbeitet und genutzt werden. Unberührt hiervon bleibt die Speicherung von Daten von Verantwortlichen für Angebote im Zusammenhang mit Impressumspflichten.

4. Interaktionsdaten: Werden im Rahmen von interaktiven Dienstleistungen darüber hinaus personenbezogene Daten erhoben, die nachweisen, welche Eingaben der Teilnehmer während der Nutzung des Angebots zur Beeinflussung des Ablaufs vorgenommen hat (Interaktionsdaten; hierzu gehören z.B. Daten, die bei lexikalischen Abfragen, in interaktive Suchsysteme - etwa elektronische Fahrpläne und Telefonverzeichnisse - und bei Online-Spielen eingegeben werden), darf dies nur in Kenntnis und mit ausdrücklicher Einwilligung des Betroffenen geschehen. Interaktionsdaten dürfen nur unter Beachtung einer strikten Zweckbindung verarbeitet und genutzt werden. Sie sind grundsätzlich zu löschen, wenn der Zweck, zu dem sie erhoben wurden, erreicht wurde (so müssen Daten über die interaktive Suche von Angeboten unmittelbar nach Beendigung des Suchprozesses gelöscht werden). Eine weitergehende Verarbeitung dieser Daten ist nur auf Grundlage einer ausdrücklichen Einwilligung des Betroffenen zulässig.

5. Einwilligung: Der Abschluß oder die Erfüllung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, daß der Betroffene in die Verarbeitung oder Nutzung seiner Daten außerhalb der zulässigen Zweckbestimmung eingewilligt hat. Soweit Daten aufgrund einer Einwilligung erhoben werden, muß diese jederzeit widerrufen werden können. Für die Form und Dokumentation elektronisch abgegebener Einwilligungen und sonstiger Willenserklärungen ist ein Mindeststandard zu definieren, der einen fälschungssicheren Nachweis über die Tatsache, den Zeitpunkt und den Gegenstand gewährleistet. Dabei ist sicherzustellen, daß der Teilnehmer bereits vor der Einwilligung soweit wie möglich über den Inhalt und die Folgen seiner Einwilligung und über sein Widerrufsrecht informiert ist. Deshalb müssen die Betroffenen sowohl vor als auch nach Eingabe der Erklärung die Möglichkeit haben, auf Einwilligungen, Verträge und sonstige Informationen über die Bedingungen der Nutzung von Diensten, Multimedia-Einrichtungen und Dienstleistungen zuzugreifen und diese auch in schriftlicher Form zu erhalten. Da Verträge oder andere rechtswirksame Erklärungen, die in einer Fremdsprache verfaßt sind, unter Umständen juristische Fachbegriffe enthalten, die nur vor dem Hintergrund der jeweiligen Rechtsordnung zu verstehen sind, sollten zumindest diejenigen Dienste, die eine deutschsprachige Benutzeroberfläche anbieten, derartige Unterlagen auch in deutscher Sprache bereitstellen.

6. Transparenz der Dienste und Steuerung der Datenübertragung durch die Teilnehmer: Die automatische Übermittlung von Daten durch die beim Betroffenen eingesetzte Datenverarbeitungsanlage ist auf das technisch für die Vertragsabwicklung notwendige Maß zu beschränken. Eine darüber hinausgehende Übermittlung ist nur aufgrund einer besonderen Einwilligung zulässig. Im Hinblick darauf, daß die

Teilnehmer bei der eingesetzten Technik nicht erkennen können, in welchem Dienst sie sich befinden und welche Daten bei der Nutzung von elektronischen Diensten bzw. bei der Erbringung von Dienstleistungen automatisiert übertragen und gespeichert werden, ist sicherzustellen, daß die Teilnehmer vor Beginn der Datenübertragung hierüber informiert werden und die Möglichkeit haben, den Prozeß jederzeit abzubrechen. Die zur Nutzung vom Anbieter oder Netzbetreiber bereitgestellte Software muß eine vom Nutzer aktivierbare Möglichkeit enthalten, den gesamten Strom der ein- und ausgehenden Daten vollständig zu protokollieren. Bei einer Durchschaltung zu einem anderen Dienst bzw. zu einer anderen Multimedia-Einrichtung müssen die Teilnehmer über die Durchschaltung und damit mögliche Datenübertragungen informiert werden. Diensteanbieter haben zu gewährleisten, daß sie keine erkennbar unsicheren Netze für die Übertragung personenbezogener Daten nutzen bzw. den Schutz dieser Daten durch angemessene Maßnahmen sicherstellen. Entsprechend dem Stand der Technik sind geeignete (z.B. kryptographische) Verfahren anzuwenden, um die Vertraulichkeit und Integrität der übertragenen Daten sowie eine sichere Identifizierung und Authentifikation zwischen Teilnehmern und Anbietern zu gewährleisten.

7. Rechte von Betroffenen: Die Rechte von Betroffenen auf Auskunft, Sperrung, Berichtigung und Löschung sind auch bei multimedialen und sonstigen elektronischen Diensten zu gewährleisten. Soweit personenbezogene Daten im Rahmen eines elektronischen Dienstes veröffentlicht wurden, der dem Medienprivileg unterliegt, ist das Gegendarstellungsrecht der von der Veröffentlichung Betroffenen sicherzustellen.

8. Datenschutzkontrolle: Eine effektive, unabhängige und nicht anlaßgebundene Datenschutzaufsicht ist zu gewährleisten. Den für die Kontrolle des Datenschutzes zuständigen Behörden ist ein jederzeitiger kostenfreier elektronischer Zugriff auf die Dienste und Dienstleistungen und der Zugang zu den eingesetzten technischen Einrichtungen zu ermöglichen. Bei elektronischen Diensten, für die das Medienprivileg gilt, ist die externe Datenschutzkontrolle entsprechend zu beschränken.

9. Geltungsbereich: Der Geltungsbereich der jeweiligen Regelungen ist eindeutig festzulegen. Es ist sicherzustellen, daß die Datenschutzbestimmungen auch gelten, sofern personenbezogene Daten nicht in Dateien verarbeitet werden.

10. Internationale Datenschutzregelung: Im Hinblick auf die zunehmende Bedeutung grenzüberschreitender elektronischer Dienste und Dienstleistungen ist eine Fortentwicklung der europäischen und internationalen Rechtsordnung dringend erfor-

derlich, die auch bei ausländischen Diensten, Dienstleistungen und Multimedia-Angeboten ein angemessenes Datenschutzniveau gewährleistet. Die Verabschiedung der sog. ISDN-Datenschutzrichtlinie mit einem europaweiten hohen Schutzstandard ist überfällig. Kurzfristig ist es notwendig, den Betroffenen angemessene Mittel zur Durchsetzung ihrer Datenschutzrechte gegenüber ausländischen Betreibern und Dienstleistern in die Hand zu geben. Die in Deutschland aktiven Dienste aus Nicht-EG-Staaten haben im Sinne der EG-Datenschutzrichtlinie (95/46/EG) vom 24.10.1995 einen verantwortlichen inländischen Vertreter zu benennen.

Anlage 23

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 22./23. Oktober 1996

Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen

Mit der Markteinführung des digitalen Fernsehens eröffnen sich für die Anbieter - neben einem deutlich ausgeweiteten Programmvolumen - neue Möglichkeiten für die Vermittlung und Abrechnung von Sendungen. Hinzuweisen ist in erster Linie auf Systeme, bei denen die Kunden für die einzelnen empfangenen Sendungen bezahlen müssen. Dort entsteht die Gefahr, daß die individuellen Vorlieben, Interessen und Sehgewohnheiten registriert und damit Mediennutzungsprofile einzelner Zuschauer erstellt werden. Die zur Vermittlung und zur Abrechnung verfügbaren technischen Verfahren können die Privatsphäre des Zuschauers in unterschiedlicher Weise beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter und Programmlieferanten auf, den Nutzern zumindest alternativ auch solche Lösungen anzubieten, bei denen die Nutzung der einzelnen Programmangebote nicht personenbezogen registriert werden kann, wie es der Entwurf des Mediendienste-Staatsvertrages bereits vorsieht. Die technischen Voraussetzungen für derartige Lösungen sind gegeben.

Die technischen Verfahren sind so zu gestalten, daß möglichst keine personenbezogenen Daten erhoben, gespeichert und verarbeitet werden (Prinzip der Datensparsamkeit). Verfahren, die im voraus bezahlte Wertkarten - Chipkarten - nutzen, um die mit entsprechenden Entgeltinformationen ausgestrahlten Sendungen zu empfangen und zu entschlüsseln, entsprechen weitgehend dieser Forderung. Allerdings setzt eine anonyme Nutzung voraus, daß beim Zuschauer gespeicherte Informationen über die gesehenen Sendungen nicht durch den Anbieter abgerufen werden können.

Die Datenschutzbeauftragten sprechen sich außerdem dafür aus, daß für die Verfahren auf europäischer Ebene Vorgaben für eine einheitliche Architektur mit gleichwertigen Datenschutzvorkehrungen entwickelt werden.

Anlage 23

Anlage zur Entschließung
der Datenschutzbeauftragten des Bundes und der Länder

vorgelegt vom Arbeitskreis Medien

Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen

Grundsätzlich werden auch Pay-per-View-Programme - wie das traditionelle Abonnenten-Fernsehen - verschlüsselt übertragen. Der Kunde braucht einen Decoder, um die Programme empfangen zu können (die sog. „Set-Top-Box"). Die Sendesignale werden von dem Decoder nur entschlüsselt, wenn er „freigeschaltet" wurde. Die Freischaltung kann mit verschiedenen technischen Verfahren realisiert werden:

1. Zentrale Freischaltung aus dem Netz

Mit dem Sendesignal gekoppelt werden die Benutzernummern sämtlicher Kunden übertragen, die eine bestimmte Sendung sehen wollen. Der Decoder wird auf diese Weise aus dem Netz nur für die betreffende Sendung „freigeschaltet". Dieses Verfahren setzt voraus, daß die Kunden entweder telefonisch oder über einen Rückkanal beim Sender die Freischaltung für eine Sendung verlangen. Damit wird das vom Kunden gewünschte Programmangebot grundsätzlich zunächst registriert.

Zudem werden mit dem über Kabel oder Satellit verteilten Signal für die Sendung auch die Nutzernummern der Interessenten - unverschlüsselt - übertragen, deren Decoder freigeschaltet werden soll; sie könnten im gesamten Netz mit verhältnismäßig geringem Aufwand mitgelesen und ausgewertet werden. Im Unterschied zur periodischen Freischaltung von Decodern im Abonnenten-Fernsehen ist damit eine sendungsspezifische Registrierung des Nutzungsverhaltens möglich.

Nur durch zusätzliche organisatorische Maßnahmen - etwa die Einschaltung eines neutralen Dritten, der die Freischaltung im Auftrag des Anbieters übernimmt, jedoch keinen direkten Kundenkontakt hat - läßt sich bei diesem Verfahren eine direkt personenbezogene Speicherung des Nutzungsverhaltens vermeiden.

2. Lokale Freischaltung durch den Nutzer

Jede Sendung wird mit einer elektronischen Entgeltinformation (Token) versehen. Die Kunden, die das Programmangebot sehen wollen, teilen dies per Fernbedienung dem Decoder mit. Das Guthaben auf der Chipkarte, die in den Decoder eingeführt ist, wird entsprechend verringert und der Decoder lokal freigeschaltet.

Das Token-System läßt sich mit vorhandener Technik so gestalten, daß beim Anbieter keinerlei personenbezogene Informationen über die Inanspruchnahme einzelner Sendungen entstehen. Eine vollständig anonyme Nutzung kann insbesondere durch den Einsatz von Wertkarten realisiert werden. Selbst bei Einsatz personalisierter wiederaufladbarer Wertkarten besteht die Möglichkeit, daß lediglich der Ladevorgang (z.B. durch Einzahlung eines Guthabens an einem Automaten oder bei Aufladung aus dem Netz), nicht jedoch die einzelne Programmnutzung durch den Anbieter oder einen zwischengeschalteten Dritten registriert wird.

Allerdings besteht die Gefahr, daß auch bei Token-Verfahren auf der Chipkarte Informationen über die einzelnen Programmabrufe gespeichert und - per Rückkanal - an den Anbieter für Zwecke seiner Abrechnung mit Programmlieferanten übermittelt bzw. von diesem abgerufen werden.

Dem datenschutzrechtlichen Gebot, technische Verfahren so zu gestalten, daß möglichst wenige personenbezogene Daten entstehen und auch eine anonyme Nutzung gewährleistet ist, kann durch das Token-Verfahren bei Pay-per-View besser entsprochen werden als durch Verfahren mit individueller zentral gesteuerter Freischaltung. Eine anonyme Nutzung ist jedoch auch bei dem Token-Verfahren nur dann zu gewährleisten, wenn der Abruf der Daten über die einzelnen gesehenen Sendungen durch den Anbieter unterbleibt.