Fünfzehnter Bericht

über die

Tätigkeit des Landesbeauftragten für Datenschutz
gemäß § 27 des Saarländischen Gesetzes
zum Schutz personenbezogener Daten
(Berichtszeitraum: 1993/1994)

Ausgegeben: 23.01.95

Herausgeber:
SAARLAND
Der Landesbeauftragte für Datenschutz
Fritz-Dobisch-Str. 12
66111 Saarbrücken
Tel.: 6681/503-415
Fax: 0681/498629
eMail: lfd-saar@t-online.de

I N H A L T S V E R Z E I C H N I S

A N L A G E N V E R Z E I C H N I S

Entschließungen
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder

A B K Ü R Z U N G S V E R Z E I C H N I S

ABl	Amtsblatt des Saarlandes
AO	Abgabenordnung
BDSG	Bundesdatenschutzgesetz
BGBl	Bundesgesetzblatt
BNDG	Gesetz über den Bundesnachrichtendienst
BRRG	Beamtenrechtsrahmengesetz
BSHG	Bundessozialhilfegesetz
BVerfGE	Entscheidung des Bundesverfassungsgerichts
BVerfSchG	Bundesverfassungsschutzgesetz
Dipol	DV-Struktur für die Polizei
EU	Europäische Union
GG	Grundgesetz
GMBl	Gemeinsames Ministerialblatt
INPOL	Informationssystem der Polizei
INZOLL	Informationssystem des Zolls
ISDN	Integrated Services Digital Network (dienste-integrierendes digitales Fernmeldenetz)
KJHG	Kinder- und Jugendhilfegesetz (SGB VIII)
KSVG	Kommunalselbstverwaltungsgesetz
KVK	Krankenversicherungskarte
LKA	Landeskriminalamt
LStatG	Landesstatistikgesetz
Lt-Drucksache	Landtagsdrucksache

MADG	Gesetz über den Militärischen Abschirmdienst
MG	Meldegesetz
NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenschrift
SchoG	Schulordnungsgesetz
SDSG	Saarländisches Datenschutzgesetz
SGB	Sozialgesetzbuch
SKHG	Saarländisches Krankenhausgesetz
SPolG	Saarländisches Polizeigesetz
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVollZG	Strafvollzugsgesetz
StVZO	Straßenverkehrszulassungsordnung
SVerf	Saarländische Verfassung
TB	Tätigkeitsbericht des Landesbeauftragten für Datenschutz

1. Vorbemerkungen

1.1 Zehn Jahre Volkszählungsurteil

Im Dezember 1983 hat das Bundesverfassungsgericht in seinem Urteil zur Volkszählung die Grundsätze des Datenschutzes festgeschrieben. Nach nunmehr zehn Jahren kann ein Rückblick auf die bisherige Entwicklung nicht nur Zufriedenheit aufkommen lassen (vgl. Entschließung der DSB-Konferenz vom 09.10.3.1994, Anlage1).

Informationen vermitteln nicht nur Wissen, sondern auch Macht; personenbezogene Daten als Träger von Informationen sind Mittel der Herrschaft, die im Rechtsstaat gebunden sein müssen. "Der Mensch braucht nicht nur Brot und Freiheit, sondern auch stabilen Schutz gegen fremde, ihm weit überlegene Neugier" (Hassemer, Einführungsrede im Hessischen Landtag am 22.10.1991). In verschiedenen Bereichen ist der Gesetzgeber - das ist positiv zu vermerken - seiner Mitwirkungsverpflichtung nachgekommen, die Grenzen der Eingriffe durch Informationsverarbeitung öffentlicher Stellen festzulegen. Das informationelle Selbstbestimmungsrecht des Bürgers ist ein Grundrecht, das zwar wegen der Gemeinschaftsbezogenheit des einzelnen nicht absolut sein kann, das aber die grundsätzliche Verfügungsmacht des Bürgers, über die Preisgabe seiner Daten selbst entscheiden zu können, berücksichtigen muß und deshalb gleichermaßen optimal zur Geltung kommen muß wie andere Grundrechtspositionen auch.

Neben grundlegenden Novellierungen der Datenschutzgesetze in Bund und Ländern traten spezielle Gesetze in Kraft, zu denen auf der Ebene des Bundes vor allem einzelne Bücher des Sozialgesetzbuches, das Personalaktenrecht für Beamte und die Gesetze über die Nachrichtendienste zählen. Der Bund hat aber bis heute

noch keine hinreichenden datenschutzrechtlichen Regelungen getroffen auf dem Gebiet des Arbeitnehmerdatenschutzes, der Justizmitteilungen und der Zwangsvollstreckung, des Abgabenrechts, des Mieterschutzes, der Detekteien und Auskunfteien. Ganz besonders ins Gewicht fallen die Regelungsdefizite im Strafverfahrensrecht.

Auf Landesebene sind neben der Novellierung des Datenschutzgesetzes Fortschritte insbesondere zu vermelden durch die Verabschiedung des Polizeigesetzes, des Verfassungsschutzgesetzes, des Landeskrankenhausgesetzes, des Statistikgesetzes, des Archivgesetzes. Entwürfe zum Meldegesetz und zum Beamtengesetz liegen vor, die nunmehr vorrangig zur Ausfüllung der bundesrechtlichen Rahmenregelungen einer Verabschiedung durch das Landesparlament zugeführt werden müssen. Auf dem Gesundheitssektor harrt die Informationsverarbeitung in den Gesundheitsämtern einschließlich des behördlichen Umgangs mit psychisch Kranken und Süchtigen im Vorfeld der Anstaltseinweisung einer gesetzlichen Regelung und das epidemiologische Krebsregister der Fortschreibung.

Die gegenwärtige Situation ist bestimmt durch immer knapper werdende finanzielle Ressourcen der öffentlichen Hand, die sich nachhaltig auf die Wirtschafts- und Sozialordnung auswirken, das Anwachsen der Kriminalität und die bislang nicht vorhersehbare Steigerung der Leistungsfähigkeit vernetzter Computer. Die Folge sind neue Überwachungsverfahren etwa zur Vermeidung des Subventionsbetrugs und zur Mißbrauchsbekämpfung im Sozial- und Ausländerbereich, die auch den Korrekten und Unverdächtigen einschließen.

Die Fernmeldeaufklärung des Bundesnachrichtendienstes, die bisher nur zur Abwendung von Gefahren eines bewaffneten Angriffes auf die BRD eingesetzt wurde, darf

neuerdings für die Bekämpfung schwerwiegender Straftaten mit Inlandsbezug genutzt werden: Die massenhafte Überwachung des Fernsprechverkehrs unbescholtener Bürger wird ermöglicht; damit einher geht der Abbau von Schranken zwischen Geheimdiensten und Strafverfolgungsbehörden.

Auf dem Gebiet der Strafverfolgung haben sich die Ermittlungen früher vor allem auf den Beschuldigten konzentriert; sie wurden zumeist offen geführt. Die Möglichkeiten der heimlichen Ermittlung wurden inzwischen gestärkt und zunehmend werden auch Unverdächtige und Kontaktpersonen einbezogen. Was Polizeigesetze der Länder vorexerziert haben, hat das Gesetz zur Bekämpfung der organisierten Kriminalität (Org KG) für die Strafprozeßordnung nachvollzogen (verdeckte Ermittler, Rasterfahndung, längerfristige Observation). Die frühere Trennung zwischen Strafverfolgung und vorbeugender Verbrechensbekämpfung hat sich weitgehend verflüchtigt. Die Banken müssen aufgrund des Geldwäschegesetzes Bartransaktionen größeren Ausmaßes personenbezogen aufzeichnen und bei "Verdachtsfällen" den Strafverfolgungsbehörden melden.

Mag auch die Sinnhaftigkeit der Überwachungsmaßnahmen, ja auch ihre Rechtmäßigkeit vielfach nicht in Frage gestellt werden können - eine breite öffentliche Meinung bietet der Politik überdies ein gutes Fundament-, so muß doch gefragt werden, ob die Summe schwerer Eingriffe in Grundrechte mit dem Menschenbild des Grundgesetzes vereinbar ist, wenn der Staat dem Bürger mit immer mehr Mißtrauen begegnet und das Kontrollnetz immer dichter zieht. Die Entwicklung ist weitaus problematischer als diejenigen Kritiker des Datenschutzes wahrhaben wollen, die schon unwirsch allein bei der Erwähnung dieses Grundrechts reagieren, mit wohlfeilen Argumenten gegen den "Datenschutz als Täterschutz" agieren und eilfertig den Eindruck erwecken,

daß das "informationelle Selbstbestimmungsrecht" etwas "Unanständiges für unanständige Leute" sei.

Wer nicht mehr wissen kann wer was über ihn weiß, wird dazu neigen, sich mit seiner Meinungsäußerung zurückzuhalten und seine Teilnahme am politischen Leben zu verweigern. Datenschutz ist deshalb Demokratieschutz (Simitis, 20. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten). Engmaschige Überwachungs- und Überprüfungsmöglichkeiten, die auch den Unverdächtigen und an sich Unbeteiligten zwangsläufig mit einbeziehen, wirken sich auf das soziale Klima, auf das Verhältnis des Bürgers zum Staat aus. Die jederzeit recherchierbare Aufzeichnung jeder Berührung des Bürgers mit der Polizei, die uneingeschränkte Informationsspeicherung in automatisierten Verfahren und Dateien der Nachrichtendienste wäre das Schreckbild eines Überwachungsstaates. Perfektionistische, brutale Computerisierung führt zur Erosion gemeinsam als verbindlich angesehener, sozialer Normen. Informationsdefizite sollten daher von vornherein in Kauf genommen werden, wenn die gemeinsame Substanz des gesellschaftlichen Zusammenlebens nicht leiden soll. Immer mehr Stimmen werden laut, die einen rationaleren Umgang mit der steigenden Verbrechensfurcht für notwendig halten. Die Polizei darf von vornherein nicht etwa jede gespeicherte Information zu präventiven Zwecken nutzen (§ 30 Abs. 2 SPolG, § 31 SPolG). Nachrichtendienste dürfen in automatisierten Verfahren und Dateien Informationen nur speichern, soweit es vorher festgelegte Beobachtungsobjekte betrifft und tatsächliche Anhaltspunkte für einen Verdacht vorliegen (§ 10 Abs. 1 SVerfSchG). Insoweit bieten das Saarländische Polizeigesetz und das Saarländische Verfassungsschutzgesetz wertvolle Anknüpfungsgesichtspunkte. §

Nur wenn der Bürger auch im übrigen sicher sein kann, daß seine dem Staat und der Wirtschaft überlassenen

Daten soweit wie möglich geschützt sind, wird er aktiv am Gemeinschaftsleben teilnehmen. Maßstäbe für die Informationserhebung und -verarbeitung müssen die im Volkszählungsurteil dargelegten Grundsätze bleiben.

Die Technik in ihren verschiedenen Spielarten bedroht auch in anderer Hinsicht die Persönlichkeitsrechte. Die Fortentwicklung der Chipkartentechnik - größere Speicherkapazität und Verarbeitungsintelligenz - wird dazu führen, daß die gesamte Krankengeschichte eines Patienten, ja sogar Röntgenbilder, abgespeichert werden können. Mit Hilfe dieser Technik könnte die Kommunikation zwischen Ärzten verbessert, unnötige Doppeluntersuchungen vermieden und damit Kosten gemindert werden können. Zugleich steigen aber auch die Gefahren für die Persönlichkeitsrechte nicht nur durch Verlust und unbefugten Zugriff. Der Patient hat u.a. das verfassungsmäßige Recht, über den Umgang mit seinen Daten selbst zu bestimmen. Wird der Patient wirklich frei entscheiden können, ob er die Gesundheitskarte überhaupt nutzen, welche Informationen er speichern lassen, wann und welchem Arzt und in welchem Umfang er die abgespeicherten Informationen jeweils offenbaren will. Die Einwilligung des Betroffenen als Rechtsgrundlage darf keinesfalls überstrapaziert werden, da sich der Bürger häufig in der Situation des faktischen Zwangs befindet und deshalb nicht frei in seinen Entschlüssen ist. Der Gesetzgeber sollte wenigstens die Rahmenbedingungen und technischen Vorkehrungen zum Schutze der Persönlichkeitsrechte vorgeben.

Kritiker des Computerzeitalters wie Joseph Weizmann machen es sich zu einfach, wenn sie den grundsätzlichen Verzicht auf die Informationsnetze empfehlen. Hier ist eine Gratwanderung angesagt, die Vor- und Nachteile dieser Technik berücksichtigt. Das Bundesverfassungsgericht hat bereits die Notwendigkeit externer, unabhängiger Datenschutzkontrolle als Mittel

eines vorbeugenden Rechtsschutzes unterstrichen. Vor dem erstmaligen Einsatz und wesentlicher Änderung von automatisierten Verfahren ist daher von Gesetzes wegen der Landesbeauftragte für Datenschutz rechtzeitig zu beteiligen (§ 8 Abs. 2 SDSG). Ebenso ist der Landesbeauftragte über Planungen des Landes zum Aufbau automatisierter Systeme rechtzeitig zu unterrichten (§ 22 Abs. 2 SDSG). Auf diesem Sektor haben sich unsere Anstrengungen verstärkt (vgl. Tz. 15). Defizite beruhen teils auf mangelnder Mitwirkung der öffentlichen Stellen, sind aber auch auf mangelnde Kontrolle infolge personeller Engpässe beim Landesbeauftragten für Datenschutz zurückzuführen.

1.2 Auswirkungen der Novellierung des Saarländischen Datenschutzgesetzes auf die Dienststelle des Landesbeauftragten für Datenschutz

Seit Inkrafttreten der Novellierung zum Saarländischen Datenschutzgesetz erstattet der Landesbeauftragte für Datenschutz seine Tätigkeitsberichte in einem Rhythmus von zwei Jahren. Die hierin liegende Entlastung für eine Dienststelle mit einer - am Aufgabenspektrum orientiert - zu kleinen, personellen Ausstattung ist zu begrüßen.

Die Ansiedlung meiner Dienststelle beim Landtag hat sich bei allen Vorteilen für die Unabhängigkeit des Landesbeauftragten für Datenschutz auch nachteilig ausgewirkt.

Die Zusammenfassung der Datenschutzkontrolle für den privaten Bereich und die öffentlichen Stellen im Saarland ist aufgegeben worden. Nach dem Bundesdatenschutzgesetz bestimmt die Landesregierung die für die Überwachung oder Durchführung des Datenschutzes im privaten Bereich zuständige Aufsichtsbehörde (§ 38 Abs. 6

BDSG). Diese war bisher das Innenministerium, und diese Stelle ist es geblieben, weil dem Landesbeauftragten, solange er bei diesem Ressort angesiedelt war, die Funktionen insoweit nur durch verwaltungsinterne Anordnung übertragen waren. Diese Verfügung war gegenstandslos geworden, nachdem durch Gesetz die Verlagerung zum Parlament zu vollziehen war.

Bereits vor der Verabschiedung des Gesetzes habe ich die Befürchtung geäußert, daß dem Bürger die Zweiteilung der Kontrollkompetenz nicht zu vermitteln sein wird und daß sich hieraus eine Kompetenzfalle ergeben könnte (13. TB, Lt-Drucksache 10/941, Vorbemerkung Seite 4). In Einzelfällen muß ich den Petenten immer wieder meine Unzuständigkeit erläutern, bevor ich die Vorgänge an das Innenressort abgebe. Der Vorgang ist nachteilig und zeitraubend für den Bürger, insbesondere wenn es sich um einheitliche Lebenssachverhalte handelt, die in beide Kompetenzbereiche fallen.
Durch die längst fällige Zuweisung eines Diplominformatikers im Berichtszeitraum ist zwar in der Grundausstattung in einem wichtigen Arbeitsgebiet ein Fortschritt erzielt worden. Im Interesse von Personaleinsparungen hat das Land in den letzten fünf Jahren verstärkt Automationsverfahren entwickelt und eingeführt; die EDV-Kapazität dürfte sich in den Jahren 1990 bis 1994 um etwa 300 Prozent gesteigert haben (Gesamtaufwand etwa 44 Millionen). Dem mir inzwischen zugewiesenen Diplominformatiker stehen zirka 270 Bedienstete im Landesdienst gegenüber, die mit EDV-Organisation beschäftigt sind. Weitere umfangreiche EDV-Kapazitäten werden im Bereich der nachgeordneten Körperschaften (z. B. AOK, LVA) und in den 52 Gemeinden vorgehalten. Mit dieser rasanten Entwicklung der Automation hat die Personalausstattung des Landesbeauftragten für Datenschutz, die im Vergleich zu allen Datenschutzbeauftragten in anderen Bundesländern spär-

lich zu nennen ist, nicht Schritt gehalten. Zwischen seinen Kontrollmöglichkeiten und den im Land vorgehaltenen EDV-Kapazitäten besteht ein deutliches Mißverhältnis.

Mängel in der Personalausstattung habe ich bereits in meinem 14. Tätigkeitsbericht (Lt-Drucksache 10/1403, Tz. 12) eingehend dargelegt. Hemmend für meine Tätigkeit vor der Verlagerung zum Parlament wirkten sich vor allem die Verfügungen des Innenministers über das mir zugewiesene Personal aus. Hohe Personalfluktuation im höheren Dienst beeinträchtigte die Kontinuität der Aufgabenwahrnehmung.

Ein juristischer Mitarbeiter des höheren Dienstes, der mir durch Organisationsverfügung bereits zugesprochen war, wurde ohne Angabe von Gründen einer anderen Stelle zugewiesen. Ich sehe in der nicht vollzogenen Zuordnung die Anerkennung eines Bedarfs, der bis heute noch nicht erfüllt ist.

Einen Mitarbeiter des höheren Dienstes hat das Innenministerium trotz meines Protestes mit anderen Aufgaben zusätzlich betraut, obgleich dies mit meinem ausschließlichen Weisungsrecht gegenüber dem mir zugewiesenen Personal und meiner unabhängigen Aufgabenwahrnehmung nicht vereinbar war (§ 21 Abs. 4 Satz 2 SDSG). Mein Einfluß auf die Personalauswahl war im übrigen mehr als gering.

Aus dem Wegfall der aufsichtsbehördlichen Funktion für den privaten Bereich haben sich im Berichtszeitraum in anderer personeller Hinsicht Nachteile ergeben. Die Entflechtung der Funktionen im Zuge der Ansiedlung beim Parlament hat zu erheblichen Schwierigkeiten geführt (vgl. Antwort der Landesregierung auf die parlamentarische Anfrage des Abgeordneten Kiefaber, Lt-Drucksache 10/1983). Ein Beamter des gehobenen

Dienstes und eine Halbtagsschreibkraft wurden von meiner Dienststelle abgezogen, ein bei der ohnehin dürftigen Personalausstattung meiner Dienststelle außerordentlich großer Aderlaß. Meinen drei Referatsleitern stehen zwei Beamte des gehobenen Dienstes und regelmäßig nur eine einzige Schreibkraft zur Verfügung. Die beim Innenministerium verbliebenen, beiden Bediensteten waren keineswegs nur im privaten Sektor tätig. Dies ergibt sich allein schon daraus, daß die Aufsichtsbehörde die Durchführung des Datenschutzes in diesem Bereich weitgehend nur "im Einzelfall" überprüft (§ 38 Abs. 1 BDSG) und deshalb die beiden Bediensteten zum ganz überwiegenden Teil Funktionen des Landesbeauftragten für Datenschutz im öffentlichen Bereich wahrgenommen haben. Der Regierungsamtmann war insbesondere neben seiner Prüftätigkeit mit Querschnittsfunktionen betraut (Haushalt, Materialbeschaffung, PC-Einsatz, Posteingang, -ausgang, Aktenverwaltung). Die Wahrnehmung dieser Funktionen geht nunmehr zu Lasten notwendiger Kontrollen. In diesem Zusammenhang wird deutlich, daß Synergieverluste durch das Auseinanderfallen der Kontrollkompetenzen zu beklagen sind.

Es muß befremden, daß bei den Verhandlungen und Diskussionen über meine personelle Ausstattung, an der ich nicht unmittelbar beteiligt wurde, keine angemessene Lösung für den Sozialfall einer Schreibkraft gefunden wurde, die wegen Schwerbehinderung (60 Prozent) und Erwerbsunfähigkeit ihre Rentenansprüche vor dem Sozialgericht verfolgt und wegen andauernder Dauererkrankung seit über vier Jahren ihren Dienst nur noch sporadisch (im letzten Jahr waren es insgesamt zirka vier Wochen) verrichtete. Diese nicht voll einsetzbare Bedienstete, wenn sie denn überhaupt ihren Dienst versieht, im Zuge des personellen Revirements meiner kleinen Dienststelle zu belassen, läßt erhebliche Defizite hinsichtlich des sozialen Einfühlungsvermö-

gens auf Seiten der Landesregierung erkennen. Hätte die Landesregierung nicht dafür Sorge tragen müssen, daß diese schwerbehinderte Frau in einer größeren Dienststelle beschäftigt wird, die eine ihren Möglichkeiten entsprechenden Arbeitsplatz zur Verfügung stellen kann, wenn sie denn überhaupt in der Lage ist, ihren Dienst aufzunehmen. Der Abhilfe schaffenden Vorlage des Präsidiums des Landtages hat die Landesregierung nachhaltigen Widerstand entgegensetzt. Dies kommt auch in der abweichenden Vorlage des Landtagspräsidiums für den Haushalt 1994 zum Ausdruck. Aus dem Protokoll zu den Verhandlungen im Ausschuß für Haushalts- und Finanzfragen vom 11. November 1993 geht hervor, daß der Landtagspräsident und das Landtagspräsidium sich von der Vorstellung haben leiten lassen, daß die Ausstattung des Landesbeauftragten für Datenschutz durch die Ansiedlung beim Parlament sich nicht verschlechtern dürfe. Dem kann ich nur zustimmen, zumal die Kontrollkompetenz des Landesbeauftragten sich nach der Novellierung des Saarländischen Datenschutzgesetzes neuerdings auf den Verfassungsschutz und die Sparkassen erstreckt und damit zusätzliche, arbeitsintensive Aufgabe hinzugekommen sind, die das Aufgabenvolumen der inzwischen weggefallenen aufsichtsbehördlichen Funktion ohne weiteres ausgleichen.

Mit einer einzigen, derzeit uneingeschränkt zur Verfügung stehenden Schreibkraft, die zudem auch noch Verwaltungsaufgaben wahrzunehmen hat, ist eine ordnungsgemäße Aufgabenwahrnehmung nicht mehr sichergestellt. Bei Ausfall durch Krankheit und Urlaub tritt sogar zeitweise völlige Funktionsunfähigkeit ein, weil auch die Landtagsverwaltung nicht immer in der Lage ist, das Defizit ausreichend auszugleichen.

Man kann nur hoffen, daß der Landtag des Saarlandes im Rahmen des Haushalts 1995 seine Stellenplanvorstellungen im Interesse einer unabhängigen, funktionsfähigen Datenschutzkontrolle verwirklicht.

2. Polizei

2.1 Polizeiinformationssystem Dipol

Über Dipol berichtete ich bereits wiederholt (11. TB, Lt-Drucksache 10/1403, Tz. 3.2; 12. TB, Lt-Drucksache 10/451, Tz. 3.1; 14. TB, Lt-Drucksache 10/1403, Tz. 2.6). Der Minister des Innern hat im Berichtsjahr die praktische Testphase für dieses umfassende, landesweite, polizeiliche Informationssystem eingeleitet. In einer Polizeiinspektion wird derzeit die Funktionalität des Systems auch hinsichtlich der Leitungsfunktionen der Polizeidirektion erprobt; zugleich werden Polizeibeamte zentral geschult.

Im Rahmen des 15-Millionen-Projektes Dipol sollen in den nächsten beiden Jahren insgesamt zirka 780 Bildschirmarbeitsplätze, 170 Rechner und 260 Laserdrucker zum Einsatz kommen, die über das bereits in Betrieb befindliche moderne ISDN-Sondernetz der Polizei miteinander verbunden werden. Dipol ermöglicht die Speicherung und Verarbeitung aller Polizeiinformationen und die Kommunikation zwischen sämtlichen Polizeidienststellen im Saarland. Im Interesse der Verbrechensbekämpfung und Gefahrenabwehr soll die Polizei zwar über alle modernen technischen Errungenschaften der Automation und der Nachrichtentechnik verfügen können. Die besonderen Risiken dieses Informationssystems für die Persönlichkeitsrechte der Betroffenen dürfen jedoch nicht übersehen werden.

Jede Berührung des Bürgers mit der Polizei nicht nur als Beschuldigter und Verdächtiger, sondern auch als Unverdächtiger - als Opfer, Geschädigter, Anzeiger, Hinweisgeber, Zeuge, Auskunftsperson oder Finder - hinterläßt ihre elektronischen Spuren in Dipol. Das komplexe System kann die Polizei im Saarland in die Lage versetzen, Informationen lokal aber auch zentral

in einem bisher nicht vorstellbaren Umfang gezielt abrufbar vorzuhalten. Hierin liegt ein Qualitätssprung im Vergleich zur bisherigen, konventionellen Arbeitsweise, die Gefahren für den Bürger zur Folge haben kann. Es muß zu einem Ausgleich zwischen den Persönlichkeitsrechten einerseits und dem Polizeiauftrag zur Sicherstellung der Gefahrenabwehr und der Straftatenbekämpfung andererseits kommen. Dipol darf nicht zu einem Verdachtsverdichtungsinstrument entarten, das Ermittlungen "ins Blaue hinein" und damit eine Allgegenwärtigkeit der Polizei ermöglicht. Die im Polizeigesetz vorgesehenen Schranken der Zweckbindung sind zu beachten, die eine Verwendung personenbezogener Daten zur vorbeugenden Straftatenbekämpfung nur in engen Grenzen zulassen. Aus Strafermittlungsverfahren dürfen zu diesem Zweck erst nach einer sorgfältigen Prognoseentscheidung Wiederholungstäter abrufbar gespeichert werden (§ 30 Abs. 2 SPolG). Die zur sogenannten Vorgangsverwaltung gespeicherten personenbezogenen Daten, die insbesondere zur Dokumentation polizeilichen Handelns und zum Wiederauffinden der Vorgänge gespeichert werden, dürfen nicht zu Zwecken der Prävention verwendet werden (§ 31 SPolG).

Die Berechtigung zum Speichern, Lesen, Verändern, Verknüpfen der Informationen sowie das Ingangsetzen von Verfahren und Dialogen in Dipol sind von fundamentaler Bedeutung, weil auf diese Weise der Umgang mit dem System, die gezielte Auswertung der vorgehaltenen Informationen und Nutzung seiner Kommunikationsmöglichkeiten gesteuert werden. Es müssen deshalb Vorkehrungen im System getroffen werden, die die gesetzlichen Nutzungsbeschränkungen gewährleisten helfen. Die Zweckbindung muß durch Zugriffsbeschränkungen eine edv-gestützte Absicherung erfahren. Es besteht Einigkeit mit dem Minister des Innern, daß es eines "abgestuften Systems von Datensicherungsmaßnahmen und Zugriffsregelungen ... (bedürfe), das die Nutzung der Informa-

tionen und Kommunikationsmöglichkeiten in Dipol steuert" (Presseerklärung vom 12.2.1990). Ebenso wichtig ist, daß die Speicherungsdauer der in Dipol gespeicherten Informationen genau festgelegt ist. Auch hierüber besteht Einigkeit mit dem Minister des Innern (Presseerklärung vom 5.10.94).

Aus der komplexen Problematik seien zur Erinnerung folgende Eckpunkte besonders erwähnt:

- Zentrale, auskunftsfähige, personenbezogene Informationssammlungen dürfen - wie bisher - nur für ungeklärte Fälle und Wiederholungstäter entstehen. Weitere zentrale Dateien personenbezogener Informationen, die eventuell aus technischen Gründen im Interesse der flächendeckenden Kommunikation entstehen, dürfen dem Zugriff nicht eröffnet werden. Ein zentraler, auskunftsfähiger Index aller auf örtlicher Dienststellenebene geführten Vorgänge wird nicht eingerichtet.

- Zugriffe auf personenbezogene Daten eines Vorgangs in Bearbeitung - insbesondere aus laufenden Ermittlungen - sind beschränkt auf den zuständigen Sachbearbeiter, bei seiner Abwesenheit auf seine zuständigen Vertreter.

- Die Auswertungen (Suchvorgänge) dürfen nicht beliebig erfolgen, sondern sollen standardisiert werden (nur bestimmte Kombinationen von Selektionsmerkmalen sind zuzulassen).

- Ein abgestuftes Löschungssystem ist einzurichten, das von vier Monaten seit der Erfassung im System für Mitteilungen, Meldungen, Feststellungen, Ersuchen bis hin zu fünf Jahren für Strafanzeigen reicht. Selbst bei dieser kurzen Löschungsfrist für Mitteilungen und Anfragen sind Belastungen für den

Betroffenen nicht völlig auszuschließen, weil diese Vorgänge nicht fortgeschrieben werden und deshalb unrichtige oder nicht mehr aktuelle Ergebnisse zu seiner Person vorgehalten werden können.

- Vorgangsverwaltungsdaten, die lediglich zum Nachweis des Eingangs der Bearbeitung, des Ausgangs und des Verbleibs aller Vorgänge dienen und nicht zu präventiven Zwecken benutzt werden dürfen (§ 31 SPolG), stehen Sachbearbeitern nach Vorgangsabschluß (Abverfügung durch die Leitungsebene), nicht mehr zur Verfügung. Diese Vorkehrung trägt dazu bei, daß diese Daten nur in unmittelbarem Zusammenhang mit dem konkreten Vorgang verwendet werden, wenn die Leitungsebene diesen reaktiviert. Recherchierbar sind bei abverfügten Vorgängen personenbezogene Daten von Beschuldigten und in ungeklärten Fällen von Geschädigten, soweit es zum Wiederauffinden erforderlich ist. Nach Reaktivierung sind jedoch auch die personenbezogenen Daten von Zeugen, Sachverständigen, Auskunftspersonen, Hinweisgebern, Findern, Verlierern wieder verfügbar. Die Textdokumente hingegen werden nach Abverfügung gelöscht; Grundlage für die eventuelle weitere Bearbeitung von Vorgängen bleibt die Ermittlungsakte.

- Die Zweckbindung der Vorgangsverwaltungsdaten, die nur unmittelbar im Zusammenhang mit dem konkreten Fall verwendet werden dürfen, zu dem sie gespeichert werden, erfordert insbesondere zum Schutze der Unverdächtigen eine Funktionstrennung zwischen Sachbearbeitung und Vorgangsverwaltung. Der Sachbearbeiter darf nur auf Vorgänge in Bearbeitung zugreifen, während ihm die Vorgangsverwaltungsdaten nach (eventuell auch nur vorläufigem) Abschluß nicht mehr zur Verfügung stehen dürfen.

Diese Feststellungen beruhen im wesentlichen auf den in den vorbereitenden Untersuchungen festgehaltenen Ergebnissen, dem Schriftwechsel und der mündlichen Diskussion mit der Arbeitsgruppe Dipol beim Ministerium des Innern. Noch nicht überprüfbar vor Ort waren jedoch die Ergebnisse hinsichtlich der Zugriffsregelung (Rechteverwaltung).

Der geschilderte, pragmatische Lösungsansatz für die Behandlung der Vorgangsverwaltungsdaten hat seine Schwächen, die ich in meinem 12. TB (a.a.O.) bereits angesprochen habe: - Die Recherchierbarkeit der Vorgangsverwaltungsdaten kann sowohl dem vorbestimmten Zweck, nämlich dem Wiederauffinden der Akten und Vorgängen, aber auch der Prävention (vorbeugenden Straftatenbekämpfung) dienen, ein ambivalentes Ergebnis, das gerade den Geschädigten und das Opfer einer Straftat unverhältnismäßig belastet, weil dieser Personenkreis an sich unverdächtig ist.- Die Informationen über Anzeiger, Zeugen, Auskunftspersonen, Finder, Verlierer sind zwar zunächst nicht mehr recherchierbar, können aber nach Reaktivierung des Vorgangs wieder genutzt werden.- Der Zugriff auf die Vorgangsverwaltungsdaten steht der Leitungsebene offen, die einen relativ großen Personenkreis umfaßt und die teilweise auch sachbearbeitende Funktionen ausübt (Kriminaldienst-, Sachgebiets-, Dienstgruppenleiter). Insoweit entfällt die systemseitig vorgesehene Vorkehrung, durch Zugriffsregelung Sachbearbeitung und Vorgangsverwaltung zu trennen; die Zweckbindung wird somit systemseitig nicht mehr unterstützt.

Diese Risiken könnten durch folgende Maßnahmen gemindert werden:- Durch organisatorische Maßnahmen ist nach Möglichkeit zu gewährleisten, daß Sachbearbeitung und Vorgangsverwaltung nicht in einer Hand vereinigt sind. - Beide Funktionen sollten allenfalls gemeinsam in kleinen, überschaubaren Funktionsbereichen (Geschäftszimmer) zusammengefaßt sein.- Ist auch dieser kleine, überschaubare Funktionsbereich - etwa zur Nachtzeit - nicht besetzt, sollte die Quasileitungsebene, die zugleich sachbearbeitend tätig ist, nur aus abschließend festgelegten, zeitkritischen Anlässen auf Vorgangsverwaltungsdaten zugreifen können. Zu denken wäre auch an eine Sicherung durch Schlüssel (Paßwörter), die nur bei unabweisbarem Bedarf (versiegelter Umschlag) oder nur einmal (Wegwerfschlüssel) zur Verfügung stehen.Eine präventive Wirkung sollte aber auch durch nachträgliche Feststellung unbefugter Zugriffe erreicht werden. Die Möglichkeiten der Protokollierung sind deshalb zu nutzen, die aber nur dann sinnvoll sind, wenn ausreichende Prüfkapazitäten vorhanden sind, die eine zeitnahe, kritische Kontrolle sicherstellen. Die Bedeutung einer effizienten, internen Revision zur Sicherung der gesetzlichen Nutzungsbeschränkungen kann nicht nachhaltig genug unterstrichen werden.Die Überprüfung des Pilotprojekts vor Ort am 14.10. und am 22.11.1994 ergab - was zu diesem Zeitpunkt nicht verwundern kann -, erhebliche Mängel, deren Behebung das Ministerium gegenüber der beauftragten Firma einforderte (z.B. häufige Systemausfälle, fehlerhaft zugeordnete Vorgänge, Verlust von Textdokumenten). Angesichts der Fehleranfälligkeit des Systems

in dieser Phase besteht Einvernehmen mit der Polizei darüber, daß bis zur Freigabe Grundlage der aktuellen Polizeiarbeit auch im Testbereich die bisherige konventionelle Form der Informationsverarbeitung bleiben muß. Lediglich die Büroarbeiten dürfen in den Testdienststellen mit Hilfe des Computers erledigt werden, wodurch bereits eine Entlastung durch die Verringerung der Erfassungstätigkeit (Einmalerfassung von Daten) erreicht wird. Derzeit dürfen jedoch im Schattenversuch eingesetzte Systemkomponenten für Abfragen und Auswertungen nicht genutzt werden.Neben der mangelnden Konsistenz waren einzelne Teile
von Dipol noch nicht überprüfbar, weil sie noch nicht implementiert waren (Zugriffsregelung durch Rechteverwaltung). Andere entsprachen nicht den Vorgaben der Voruntersuchung (zum Beispiel nach Verfahrensabschluß keine eindeutige Zuordnung der Vorgänge sowie keine Löschung der Textdokumente). Der Umfang der zur Speicherung vorgesehenen Datenarten
war teilweise zur Aufgabenwahrnehmung nicht erforderlich (zum Beispiel Familienstand, Anzahl der Kinder, Geburtsort für Zeugen, Geschädigte, Hinweisgeber, Finder, Verlierer, Bevollmächtigte; Personenbeschreibungen für Betroffene in Ordnungswidrigkeitenverfahren und für alle Arten von Geschädigten).Ich habe um rechtzeitige, weitere Beteiligung gebeten,
damit eine datenschutzgerechte Version verwirklicht werden kann.2.2 Neufassung der Polizeidienstvorschriften (PDV)Mit der Novelle vom 8. November 1989 war das Saarländische Polizeigesetz mit besonderen Auswirkungen für die Voraussetzungen der Informationsverarbeitung durch die

Polizei fortgeschrieben worden. Hieraus ergibt sich die Notwendigkeit, die Polizeidienstvorschriften anzupassen. Bisher war stets eine Zweiteilung - Bundesteil und ergänzender Landesteil - eingehalten worden, um eine einheitliche Terminologie bundesweit zu gewährleisten. Ich habe zunächst angeregt, daß in den entsprechenden Bund-Länder-Gremien auf eine einheitliche Begriffsbildung im Bundes- sowie im ergänzenden Landesteil hingewirkt werden sollte. Die Schwierigkeiten liegen indessen auf der Hand, weil die Landespolizeigesetze in mancher Hinsicht Unterschiede aufzeigen. So wird zum Beispiel der Begriff der "gefährlichen Straftat" bei der Beschreibung der Voraussetzungen für die polizeiliche Beobachtung (Kontrollmeldung) nach dem saarländischen Gesetz nicht mehr verwendet. Die Aufteilung in einen Bundes- und in einen hierzu interpretierenden Landesteil läßt ohnehin leicht Unübersichtlichkeiten aufkommen. Die Polizei muß indessen eindeutige und klare Handlungsanweisungen auf der Grundlage des geltenden Landespolizeigesetzes erhalten. Dies ist am ehesten durch Dienstvorschriften "aus einem Guß" zu erreichen. Das Ministerium hält offensichtlich an der bisherigen Konzeption der Zweiteilung in einen Bundes- und einen Landesteil fest. Die Entwürfe für die Fortschreibung der Landesteile zu den Polizeidienstvorschriften "polizeiliche Beobachtung" (PDV 384.2) und Bearbeitung von Jugendsachen (PDV 382) wurden mir vorgelegt. Generell war zu bemängeln, daß unbestimmte Rechtsbegriffe des Saarländischen Polizeigesetzes nicht näher konkretisiert wurden.Der Verweis auf Gesetzesbestimmungen, die ebenfalls unbestimmte Rechtsbegriffe enthalten, kann nicht ausreichen, zumal die Dienststellen der Polizei erfah-

rungsgemäß nicht genügend Gesetzestexte zur Verfügung haben. Die Argumentation des Ministeriums des Innern, der Gesetzgeber habe sich über meine Forderung, unbestimmte Rechtsbegriffe zu präzisieren, bewußt hinweggesetzt, ist für den Erlaß einer Verwaltungsvorschrift nicht stichhaltig. Zur Vermeidung einer Überfrachtung des Gesetzestextes wird im Gesetzgebungsverfahren auf Konkretisierungen verzichtet, da Verwaltungsvorschriften der geeignete Standort für die Ausfüllung unbestimmter Rechtsbegriffe sein können. Insofern wurde die Komplettierung gesetzgeberischer Arbeit in den Dienstvorschriften versäumt. In der PDV "Polizeiliche Beobachtung" sind die zugrundeliegenden Rechtsvorschriften (§ 163 e StPO und § 29 Saarländisches Polizeigesetz) näher zu erläutern. Vor allem der Begriff der "Straftat von erheblicher Bedeutung" wäre näher zu konkretisieren gewesen. Vor allem fehlten auch klärende Regelungen zu der Frage der Speicherung unter Berücksichtigung der "Rahmenrichtlinie Informationsverarbeitung".Nach dem bundeseinheitlichen Teil wird dem Amt für Verfassungsschutz "Zugang" zum Datenbestand "Polizeiliche Beobachtung" eingeräumt. Derartig allgemeine Formulierung, die möglicherweise sogar Akteneinsicht durch das Amt für Verfassungsschutz eröffnet, ist mit dem Saarländischen Verfassungsschutzgesetz vom 24. März 1993 nicht mehr vereinbar und muß im Lichte dieses Gesetzes präzisiert werden. Der Entwurf genügte mit Rücksicht auf die Eingriffsintensität der polizeilichen Beobachtung nicht den Anforderungen. Eine überarbeitete Fassung wurde mir bislang nicht vorgelegt. Die Fortschreibung der Dienstvorschriften nach Inkrafttreten des neuen Polizeigesetzes (01.01.1990) ist vordringlich, um der neuen Rechtslage gerecht zu werden.

Zum Landesteil der PDV "Bearbeitung von Jugendsachen bei der Polizei", die die Besonderheiten bei der Behandlung Jugendlicher in begrüßenswerter Weise regelt, habe ich die erkennungsdienstliche Behandlung von Kindern kritisiert. Es ergeben sich insbesondere im Vergleich zum bundeseinheitlichen Teil Nachteile für diesen Personenkreis. Nach der Bundesregelung sind erkennungsdienstliche Maßnahmen bei Kindern zulässig, wenn eine "hohe kriminelle Energie" erkennbar ist oder wiederholt rechtswidrige Taten begangen worden sind und die Gefahr der Wiederholung besteht. Nach dem Landesteil zur PDV 382 sollen Kinder nach der auch für Erwachsene geltenden Bestimmung des § 10 Saarländisches Polizeigesetz erkennungsdienstlich behandelt werden können. Für Kinder sollen daher keine anderen Voraussetzungen als für Erwachsene gelten, ohne daß den besonderen Belangen bei der Behandlung von Kindern Rechnung getragen wird. Wenn mit dem Diversionsverfahren eine Entkriminalisierung Jugendlicher und Heranwachsender erreicht werden soll, ist insofern eine am Bundesteil zu dieser PDV orientierte Formulierung geboten. Der Landesteil der Polizeidienstvorschrift ist in diesem Punkt verbesserungsbedürftig, um auch Auslegungsschwierigkeiten entgegenzuwirken, die sich aus den Unterschieden in der Formulierung im Vergleich zum Bundesteil ergeben. Zu begrüßen ist, daß die Daten von Kindern im Rahmen
der vorbeugenden Bekämpfung von Straftaten nur ausnahmsweise gespeichert werden sollen, wenn tatsäche Anhaltspunkte, die auf die Begehung künftiger Straftaten schließen lassen, kurz vor Erreichen des Alters der Strafmündigkeit bekannt werden. Meinem Vorschlag, die Rechtsentscheidungen nur in
anonymisierter Form in den Informationsaustausch über die Jugenddelinquenz zwischen den verschiedenen öf-

fentlichen Stellen zu bringen, wurde gefolgt. Auch enthält die PDV nunmehr eine Regelung, daß die Sorgeberechtigten in jedem Fall einer Speicherung von personenbezogenen Daten von Kindern unterrichtet werden, sobald die Aufgabenerfüllung dadurch nicht mehr gefährdet wird. Von einer Unterrichtung kann allerdings nach der in der Polizeidienstvorschrift in Bezug genommenen Bestimmung abgesehen werden, solange zu besorgen ist, daß die Unterrichtung zu erheblichen Nachteilen für das Kind führt.2.3 Einsichtnahme der Polizei in das Personalausweis-

registerIn der Vergangenheit wurden Beschwerden von Bürgern darüber geführt, daß die Polizei zur Verfolgung von Verkehrsordnungswidrigkeiten Einsicht in das Personalausweisregister genommen hat, wenn die Ermittlung des Kraftfahrzeugführers auf andere Weise nicht möglich erschien.Ich habe dieses Verfahren gegenüber dem Ministerium des Innern wiederholt bemängelt. Der Lichtbildervergleich, der an Hand des Registers vorgenommen wird, kommt einer erkennungsdienstlichen Maßnahme gleich, die einen tiefgreifenden Eingriff in das Persönlichkeitsrecht des Betroffenen darstellt. Ein derart eingriffsintensives Verfahren hat sich am Verfahrensgrundsatz der Verhältnismäßigkeit auszurichten. Es stellte sich von Anfang an die Frage, ob im Bagatellbereich, insbesondere bei der Verwarnung, der Lichtbilderabgleich zwingend geboten ist, zumal eine einheitliche Vorgehensweise der Behörden nicht immer gesichert erschien. Hierzu dürfte vor allem ein früherer Erlaß des Innenministeriums aus dem Jahre 1989 beigetragen haben, wonach ein Lichtbildvergleich nur dann zulässig war, wenn es sich um "erhebliche innerörtliche Geschwindigkeitsüberschreitungen" oder "schwerwiegende

Rotlichtverstöße" handelte, die zu einer Eintragung in das Verkehrszentralregister in Flensburg führten. Die Beschreibung der Voraussetzungen gab im einzelnen Anlaß zu Diskussionen. Zwar sind die gesetzlichen Voraussetzungen für die Einsichtnahme in das Personalausweisregister im Jahre 1986 weit gefaßt worden (§ 2 b Abs. 2 Personalausweisgesetz). Spätestens seit dieser Gesetzesänderung ist klargestellt, daß die Behörde zunächst versucht haben muß, den Betroffenen im Wege der Vorladung oder durch Aufsuchen zu identifizieren. Das Innenministerium hat daraufhin den genannten Erlaß unter Bezugnahme auf die Gesetzeslage aufgehoben, weil er die Voraussetzungen durch den Gesetzgeber ausreichend klargestellt angesehen hat.Die Probleme sind seither jedoch nicht geringer geworden. Aufgrund der Eingaben hat sich der Eindruck verdichtet, daß die Beachtung des Grundsatzes der Verhältnismäßigkeit noch nicht in dem gebotenen Umfang gewährleistet ist. Es ist deshalb aus datenschutzrechtlicher Sicht zu begrüßen, daß nunmehr das Innenministerium durch Erlaß vom 07.06.1994 die Vollzugspolizei angewiesen hat, in Verwarngeldverfahren keine Nachermittlungen durch Einsichtnahme in das Personalausweis-/Paßregister durchzuführen. Auch in Rheinland-Pfalz werden seit einiger Zeit in diesem Bereich solche Verfahren nicht mehr durchgeführt. In dem genannten Erlaß des Innenministeriums ist eine datenschutzrechtliche Konkretisierung des Verhältnismäßigkeitsgrundsatzes zu sehen, der auch für eigene Ermittlungen der Bußgeldbehörden - ohne Einschaltung der Polizei - Auswirkungen haben muß.Im übrigen gehe ich davon aus, daß im Interesse der Verhältnismäßigkeit auch in allen anderen Verfahren

zur Verfolgung von Verkehrsordnungswidrigkeiten vor der Einsichtnahme in das Personalausweis-/Paßregister folgende Stufen für das Verfahren der Fahrerermittlung eingehalten werden:- Vorladung des Betroffenen,- Aufsuchen des Betroffenen in der Wohnung,- Vergleich vorhandener Lichtbilder mit dem Personal-
ausweis-/Paßregister,- Befragung im Haus, in der nächsten Nachbarschaft
oder gegebenenfalls an der Arbeitsstelle.Gerade die sehr belastenden Nachbarschaftsbefragungen
sollten nur als letzte Möglichkeit in Betracht kommen.
Es steht außer Frage, daß der Lichtbildervergleich gegenüber dieser Maßnahme sehr viel weniger belastend für den Betroffenen ist.2.4 Gemeinsame Ermittlungsgruppe von Polizei und Zoll
in der RauschgiftkriminalitätDas Ministerium des Innern hat mir den Entwurf einer
Vereinbarung über die Einrichtung einer gemeinsamen Ermittlungsgruppe von Polizei und Zoll zur Bekämpfung der Rauschgiftkriminalität (GER) vorgelegt.Die angestrebte Kooperation darf nicht zu einer unzu-
lässigen Mischverwaltung und damit auch zu Unklarheiten in der Verantwortung der beteiligten Stellen führen. Bund und Länder haben sich generell an die Organisationsformen zu halten, die das Grundgesetz anbietet (z.B. Bundesfinanzverwaltung Art. 87 Abs. 1 GG). Denn das Feld unzulässiger Mischverwaltung kann nicht immer klar von den Formen und Variationen legitimen Kooperierens unterschieden werden (Maunz-Dürig, Grundgesetz, Art. 83 Rdnr. 84 ff, Rdnr. 90). Bundeszollverwaltung und Landespolizei sind zwar auf dem Gebiet der Straf-

verfolgung funktionell in sachlich übereinstimmenden (§ 404 AO, § 163 StPO), im übrigen jedoch in sachlich getrennten Bereichen tätig, die durch Gesetz festgeschrieben sind. Die deliktsgruppenorientierte, sachliche Zuständigkeit des Zolls (§ 372, 373, 369, 386, 399 AO) wird nicht ohne weiteres dadurch hinfällig, daß beide Institutionen Rechte und Pflichten der Staatsanwaltschaft in Ermittlungsverfahren wahrnehmen. Die Finanzbehörde führt das Ermittlungsverfahren in Steuerstrafsachen an Stelle der Staatsanwaltschaft in eigener Verantwortung durch (§ 386 Abs. 2 AO). Die Polizei hingegen muß der Sachherrschaft der Staatsanwaltschaft Rechnung tragen. So darf die Polizei während des laufenden Ermittlungsverfahrens personenbezogene Informationen nur mit Zustimmung der Staatsanwaltschaft übermitteln (§ 32 Abs. 1 Satz 3 SPolG).Ich halte es dessenungeachtet für sinnvoll, daß Polizei- und Zollbeamte zur Vermeidung von Doppelarbeit zusammenwirken, wenn die Aufgaben und Zuständigkeiten deckungsgleich sind. Damit kann auch ein zu begrüßender Datenschutzeffekt erreicht werden, weil für den Betroffenen belastende Doppelerhebungen ausgeschlossen werden. So wird in der GER eine einzige, gemeinsame Ermittlungsakte geführt, während die Zugriffe auf INPOL der Polizei und auf INZOLL der Zollverwaltung vorbehalten bleiben. Entsprechende Maßnahmen der Datensicherung werden getroffen.Der Vereinbarungsentwurf wies Mängel auf, die ich beanstandet habe:

- Nicht eindeutig zum Ausdruck kam, daß die gemeinsamen Ermittlungen von Zoll und Polizei sich nur auf den Bereich der Strafverfolgung unter Ausschluß der Prävention erstrecken dürfen. Im Bereich der vorbeugenden Verbrechensbekämpfung sind die gesetzlichen Grundlagen für den Zoll und die Polizei in der Ab-

gabenordnung und im Saarländischen Polizeigesetz unterschiedlich ausgestaltet. Schon deshalb war die Klarstellung erforderlich, daß die GER sich nicht im Bereich der Prävention betätigt. Auf meine Anregung wurde klargestellt, daß die GER ausschließlich aufgrund eines strafrechtlich relevanten Anfangsverdachts tätig wird (§ 163, § 152 Abs. 2 StPO).- Abgelehnt wurde mein Vorschlag, daß das Landeskriminalamt und das Zollfahndungsamt Saarbrücken für den jeweiligen Zuständigkeitsbereich in der Vereinbarung zu geeigneten Maßnahmen sich verpflichten sollen, die eine Dokumentation der Datenübermittlung aus dem Bereich der beteiligten Stellen an die GER sicherstellt. Zwar hat das Innenministerium in einem Schriftsatz erläutert, daß die Datenübermittlungen an die jeweils andere Sparte in Form von Vermerken erfolgen sollen. In der Vereinbarung ist hierüber jedoch nichts festgelegt. Die Datenübermittlung an und innerhalb einer mehr oder weniger strukturierten, gemeinsamen Gruppe ist - wenn dies nicht ausdrücklich festgelegt ist - nicht nur in schriftlicher Form denkbar. Wenn dem tatsächlich so wäre, hätte man sich gegen die Festlegung in der Vereinbarung nicht sträuben müssen. Die Datenübermittlung muß sich nicht zwangsläufig in Vermerken in der gemeinsamen Akte niederschlagen. Nicht jeder Informationsaustausch muß im Strafverfahren nachvollziehbar sein. Die Zulässigkeitsvoraussetzungen der Übermittlung sind somit nicht in jeder Hinsicht überprüfbar. Mit Rücksicht auf das Steuergeheimnis (§ 30 AO) und die polizeirechtlichen Übermittlungsregelungen (§ 32, § 30 SPolG) sind Entscheidungen im Einzelfall zu treffen, die einen ungeprüften Datentransfer ausschließen.- Die Kompetenz für die Entscheidung über Datenschutzrechte des einzelnen - insbesondere Akteneinsichts-

und Aktenauskunftsrecht - im Hinblick auf die gemeinsame Akte wurde in der Vereinbarung nicht geklärt. Die Gruppe "speist sich selbst"; das heißt: die Initiative für Ermittlungsmaßnahmen geht von ihr selbst aus. Somit sind Informationen in der gemeinsamen Akte erfaßt, die nicht notwendigerweise auch in dem polizeilichen oder Zollinformations-System gespeichert sein müssen. Deshalb wäre eine Klarstellung unerläßlich gewesen, welche Stelle über die Individualrechte des Betroffenen zu entscheiden hat. Zwar hat die Staatsanwaltschaft im vorbereitenden Verfahren die Entscheidung über die Akteneinsicht (§ 147 StPO). Die Zollverwaltung ermittelt selbständig, solange die Staatsanwaltschaft die Sache nicht "an sich gezogen" hat (§ 386 Abs. 2, Abs. 4 AO), so daß sie auch insoweit über die Akteneinsicht zu entscheiden hat. Zwar ist die GER in ein Dezernat des LKA "eingebunden". Ob damit auch die Ermittlungen als "polizeiliche" zu charakterisieren sind, für die die Staatsanwaltschaft generell die Entscheidung über die Akteneinsicht zu treffen hat, ohne daß sie die Sache an sich gezogen hat, ist jedoch offen. Mein Vorschlag, die Zuständigkeit der akteneinsichtsgewährenden Stelle generell im Interesse der Klarheit festzuschreiben, wurde nicht aufgegriffen.

2.5 Übereinkommen der Mitgliedstaaten der Europäischen Union über die Errichtung eines Europäischen Polizeiamtes (Europol)

Die Mitgliedstaaten der Europäischen Union (EU) haben in dem Vertrag über die Europäische Union vom 7.2.1992 die Schaffung eines Europäischen Polizeiamtes vereinbart. Seine Errichtung dient der gemeinsamen Zielsetzung der Mitgliedstaaten, eine Verbesserung der polizeilichen Zusammenarbeit im Bereich des Terrorismus,

des illegalen Drogenhandels und sonstiger schwerwiegender Formen der internationalen Kriminalität herbeizuführen. An der Notwendigkeit einer Konvention zur Regelung der Zusammenarbeit besteht kein Zweifel; datenschutzrechtlichen Anforderungen muß jedoch Rechnung getragen werden.Die bisher vorliegenden Entwürfe zu dem Übereinkommen
gaben Anlaß zu der Besorgnis, bundes- und landesrechtliche Kompetenzen einschließlich der verfassungsrechtlich geregelten Gesetzgebungskompetenzen könnten ausgehöhlt werden. Die datenschutzrechtliche Verantwortlichkeit der zuständigen Polizeibehörde muß gewährleistet sein. Nur die Polizeibehörde, die personenbezogene Daten rechtmäßig erhoben hat, ist auch aufgrund der Kenntnis der Unterlagen im Stande, die Richtigkeit und Vollständigkeit der anderen europäischen Polizeien übermittelten Daten zu beurteilen. Weder der Bundesgesetzgeber noch die Europäische Union sind dazu befugt, eine eigenständige polizeiliche Aufgabe zu schaffen; dem Bund hat das Grundgesetz lediglich die Kompetenz zur Regelung der Zusammenarbeit mit ausländischen Behörden übertragen (Art. 73 Nr. 10 GG). Deshalb darf sich die Europol-Konvention nicht über die datenschutzrechtliche Verantwortlichkeit der Bundesländer hinwegsetzen. Der Vertrag über die Europäische Union stellt zudem ausdrücklich fest, daß die Verantwortung der Mitgliedstaaten bei der Aufrechterhaltung der öffentlichen Ordnung und dem Schutz der inneren Sicherheit unberührt bleibt (Artikel K 2 Abs. 2). Die Konferenz der Datenschutzbeauftragten hat zu den
datenschutzrechtlichen Anforderungen an das Übereinkommen eine Entschließung gefaßt (Anlage 2), in der insbesondere eine klarstellende Regelung zur Verantwortung der Länder im polizeilichen Bereich gefordert wird.

Angemessene Sicherungen für die Individualrechte der Betroffenen, insbesondere ihres Rechtes auf Auskunft, dessen Wahrnehmung nicht unangemessen kompliziert sein darf, sollten ein integraler Bestandteil der internationalen Zusammenarbeit im Rahmen von Europol sein.Soweit der mir vorliegende letzte Entwurf (Stand 14.9.94) die Verarbeitung personenbezogener Daten von Zeugen, Opfern und Kontaktpersonen vorsieht, wird dem Grundsatz der Verhältnismäßigkeit nicht ausreichend Rechnung getragen; die Datenverarbeitungsbefugnisse sind nicht hinreichend präzisiert. Die Datenschutzbeauftragten der EU-Staaten haben erst kürzlich erneut ihre Bereitschaft bekundet, bei der Ausarbeitung der Datenschutzprinzipien in der Europol-- Konvention behilflich zu sein.

3. AusländerzentralregistergesetzDie Datenschutzbeauftragten des Bundes und der Länder
haben in den vergangenen Jahren den Bundesgesetzgeber mehrfach aufgefordert, das im Bundesverwaltungsamt in Köln geführte Ausländerzentralregister (AZR), in dem mehr als 8 Millionen Ausländer gespeichert sind, auf eine gesetzliche Grundlage zu stellen (vgl. meinen 10. TB, Lt-Drucksache 9/2075 Tz. 2.3 und Anlage 2). Am 01.10.1994 ist das Gestz über das Ausländerzentralregister (AZRG) in Kraft getreten. Das Recht auf informationelle Selbstbestimmung steht auch den in der BRD lebenden Angehörigen anderer Staaten zu. Abgesehen von einigen Verbesserungen, die erreicht werden konnten, bleiben grundlegende Vorbehalte bestehen.Die Datenschutzbeauftragten des Bundes und der Länder
haben in ihrer Entschließung vom 09./10.03.1994 (Anlage 3) den Gesetzentwurf kritisiert. Außer Frage steht die Funktion des Registers als Index
zum Zwecke der Feststellung, welche Ausländerbehörde über einen bestimmten Ausländer Akten führt. Diente das AZR früher vorwiegend der Aufenthaltsermittlung von Ausländern und der Vorbereitung ausländerrechtlicher Entscheidungen, so ist es nunmehr zu einem umfassenden Melde-, Fahndungs-, Personenstands- und Aktensuchsystem ausgebaut worden. Die vergleichbaren Funktionen werden für deutsche Staatsangehörige von unterschiedlichen, zum Teil länderspezifischen Registern erfüllt und durch vielfältige gesetzliche Vorschriften geregelt. Es ist nicht vorstellbar, daß jemand auf den Gedanken kommen könnte, für deutsche Staatangehörige vergleichbare Aufgaben und Funktionen in einem zentralen, bundesweiten Register zusammenzufassen. Auf Ersuchen wird allen öffentlichen Stellen aus dem
AZR ein begrenzter Datensatz übermittelt (§ 14 AZRG).

Ein größerer, je nach Behörde differenzierter Datensatz steht auf Anfrage neben den Sicherheitsbehörden unter anderem der Bundesanstalt für Arbeit zur Verfügung; ihnen kann auch der automatisierte Direktzugriff eingeräumt werden (§ 22 AZRG).Vor allem begegnet Bedenken, daß das AZR in das Sicherheitssystem der BRD einbezogen ist. Die Sicherheitsbehörden - Grenzpolizei, Polizeibehörden des Bundes und der Länder, Staatsanwaltschaften, Zollkriminalinstitut, Verfassungsschutzbehörden, Militärischer Abschirmdienst und Bundesnachrichtendienst - können nicht nur Informationen aus dem Register erhalten, sondern auch unmittelbar in das Register eingeben. So werden der INPOL-Fahndungsbestand, soweit es um Ausschreibungen zur Festnahme oder Aufenthaltsermittlung geht, und Angaben zu Personen in das Register eingestellt, bei denen Anhaltspunkte für den Verdacht bestehen, daß sie bestimmte schwere Straftaten (etwa aus dem Bereich des Terrorismus) planen, begehen oder begangen haben. Die genannten Sicherheitsorgane verfügen jedoch über eigene Informationssysteme, so daß die Speicherung solcher für die Verbrechensbekämpfung bestimmter Informationen in einer Datei zur Wahrnehmung ausländerrechtlicher Aufgaben weder zwingend geboten, noch zu diesem Zweck voll ausreichend ist, weil Informationen zum Beispiel über Mord, Totschlag im AZR nicht gespeichert werden. Daten aus den unterschiedlichsten Aufgabenbereichen werden in großem Umfang zusammengefaßt und in großzügiger Weise zu unterschiedlichen Zwecken wieder zur Verfügung gestellt. Ob diese Zweckdurchbrechungen vor allem mit dem Hinweis auf Verfahrenserleichterungen gerechtfertigt werden können, muß eher kritisch gesehen werden.Bedenklich ist aber auch der jedenfalls praktisch uneingeschränkte automatisierte Zugriff der Sicherheitsorgane. Eine wirksame Hürde dürften die in einem

besonderen Zulassungsverfahren zu beachtenden Förmlichkeiten ("Vielzahl von Übermittlungsersuchen", "besondere Eilbedürftigkeit") nicht darstellen. Ist das Abrufverfahren eingerichtet, kann die zugreifende Behörde mit den "fremden" Daten praktisch so arbeiten, als ob es sich um eigene handelt. Eine präventive Kontrolle ist jedenfalls nicht möglich. Vergebens haben die Datenschutzbeauftragten vor allem gefordert, wenigstens auf den (wenn auch eingeschränkten) Online-Zugriff der Nachrichtendienste zu verzichten, für die der Gesetzgeber eine derartige Möglichkeit im Hinblick auf außerhalb ihrer eigenen Informationssysteme liegende Einrichtungen bisher eindeutig ausgeschlossen hat (§ 27 BVerfSchG; § 13 MADG; § 11 BNDG). Mit Hilfe des Ausländerzentralregistergesetzes werden die ohnehin schon im Ausländergesetz festgeschriebenen Kommunikationspflichten öffentlicher Stellen in Sachen Ausländer (vgl. meinen 13. TB, Lt-Drucksache 10/941 Tz. 2.5) fortgeschrieben. Diese erhalten durch die automatisierten Direktzugriffe eine neue Qualität. Die in der Literatur bereits zum Ausländergesetz vertretene Auffassung, daß seine Bestimmungen zur Datenverarbeitung den Ausländern das Recht auf informationelle Selbstbetimmung entziehe, erhält eine weitere Stütze. Inzwischen liegt der Entwurf einer Durchführungsverordnung zum Ausländerzentralregistergesetz vor. In meiner Stellungnahme dazu habe ich darauf gedrungen, daß durch einschränkende, konkretisierende Regelungen den bestehenden grundsätzlichen Bedenken entgegengewirkt wird und die Defizite des zugrunde liegenden Gesetzes gemindert werden. Dies sollte insbesondere durch verstärkte Mitverantwortung der Stellen geschehen, die dem Register Informationen übermitteln, ferner durch strenge Voraussetzungen im Zulassungsverfahren zum automatisierten Direktzugriff. Löschungsverpflichtungen der Registerstelle und Kontrollrechte des Bundes-

beauftragten und der Landesbeauftragten für Datenschutz auf der Grundlage von Zwangsprotokollen und Aufzeichnungspflichten erhalten ein besonderes Gewicht.

4. Justiz4.1 Opferschutz im StrafverfahrenDie datenschutzrechtlich mangelhafte Ausgestaltung des Strafverfahrensrechts war Gegenstand mehrerer Eingaben von Verfahrensbeteiligten, deren Recht auf informationelle Selbstbestimmung im sensiblen Bereich der Gesundheitsdaten stärker berücksichtigt werden sollte.In einem Strafverfahren wegen Körperverletzung waren mehrere Petenten als Verletzte und Nebenkläger beteiligt. In dem mehrere Fälle verbindenden Verfahren war ein zusammengefaßtes, medizinisches Gutachten für alle Verletzte erstellt worden. Die Verfahrensakte enthielt auch im übrigen Operationsberichte und umfangreiche Gutachten über den früheren und gegenwärtigen Gesundheitszustand der Betroffenen. Die Petenten haben sich massiv darüber beschwert, daß durch Akteneinsicht der Verfahrensbeteiligten und durch Verteilung von Operationsberichten durch das Gericht sie sich in ihren Persönlichkeitsrechten beeinträchtigt sehen. Inwieweit dies zutraf und inwieweit die Offenbarung sensibler, medizinischer Angaben notwendig und mit dem Gesetz vereinbar war, war mit Rücksicht auf die Unabhängigkeit des Gerichts im einzelnen nicht zu prüfen. Ich habe die Petenten auf die Pflicht der Staatsanwaltschaft und der Gerichte hingewiesen, die schutzwürdigen Belange der Verletzten - auch gegenüber Nebenklägern - vor Gewährung der Akteneinsicht zu berücksichtigen (§ 406 e Abs. 2 StPO). Unter rechtspolitischen Gesichtspunkten habe ich mit dem Ministerium der Justiz die Probleme der Verfahrensverbindung, der zusammengefaßten Erstellung von Gutachten mehrerer Betroffener und der Akteneinsicht Verfahrensbeteiligter diskutiert. Die zusammengefaßte Begutachtung mehrerer Verletzter erschwert die Berücksichtigung schutzwürdiger

Belange Einzelner bei der Akteneinsicht. Im übrigen stehen sich hier Gesichtspunkte der Prozeßökonomie und des Schutzes der Persönlichkeitsrechte gegenüber. Ich habe mich vor allem dafür ausgesprochen, daß Aktenteile, die infolge ihres Charakters oder ihrer Entstehung in besonderem Maße persönlichkeitsrelevant sind oder sein können, besonders geheftet werden, damit die Entscheidung der Staatsanwaltschaft und des Gerichts über die Zulässigkeit der Offenbarung dieser Daten im Wege der Akteneinsicht vor allem hinsichtlich des Umfangs auch organisatorisch besser unterstützt wird. Eine entsprechende Bestimmung vorbeugenden Charakters besteht bereits für die beim Einsatz eines verdeckten Ermittlers anfallenden Informationen (§ 110 d Abs. 2 StPO). Eine solche Verfahrensweise kann die Entscheidung erleichtern, ob, inwieweit und an wen (z.B. Verletzter, Versicherung) unter Abwägung der schutzwürdigen Interessen des Beschuldigten oder anderer Personen die Akteneinsicht gewährt werden darf.Ein unter Datenschutzgesichtspunkten bisher wenig beachtetes Problem ist das Verhältnis Strafverteidiger und Sachverständiger, der nicht vom Gericht bestellt, lediglich als Gehilfe der Verteidigung tätig wird. Die Petenten haben sich bei mir darüber beschwert, daß der Verteidiger des Angeklagten im Verlauf des Strafprozesses Operationsberichte und ärztliche Befunde an seine sachverständigen Gehilfen weitergegeben und dieser überdies eigene Ermittlungen durch Anforderung ärztlicher Unterlagen durchgeführt hat. Man wird zwar dem Anwalt grundsätzlich das Recht zugestehen müssen, zur Vorbereitung einer sachgerechten Verteidigung einen Sachverständigen seiner Wahl hinzuzuziehen. Die Strafprozeßordnung regelt bisher ausdrücklich nur den Fall der Akteneinsicht durch den vom Gericht bestellten Sachverständigen (§ 80 Abs. 2 StPO). Angesichts der Eingriffsintensität der Informationsverarbeitung im

Falle von Krankheitsdaten, die dem Arztgeheimnis unterliegen, kann die Informationsübermittlung durch den Verteidiger an einen im Prozeß nicht unmittelbar Beteiligten mangels ausreichender gesetzlicher Ermächtigung nicht akzeptiert werden. Für eine sachgerechte Verteidigung hätte es durchaus ausgereicht, wenn der Anwalt lediglich anonymisierte Informationen zur Verfügung gestellt hätte. Ebensowenig steht dem sachverständigen Gehilfen der
Verteidigung das Recht zu, Krankenberichte und Befundmaterial für Zwecke der Verteidigung von Arztkollegen anzufordern. Die Strafprozeßordnung regelt zwar, auf welchem Wege ein vom Gericht bestellter Sachverständiger weitere Aufklärung zur Vorbereitung seines Gutachtens erhalten kann (§ 80 StPO). Aber auch insoweit besteht kein Zweifel, daß er eigene Ermittlungen nicht durchführen darf. Erst recht ist eine solche Vorgehensweise des lediglich als Gehilfen der Verteidigung tätigen Sachverständigen nicht erlaubt. Der Sachverständige hat sich mit dem Hinweis zu rechtfertigen versucht, daß er die Unterlagen nur zu Forschungszwecken angefordert und genutzt habe. Aber auch insoweit waren die gesetzlichen Voraussetzungen nicht beachtet.Rechtspolitisch bedürfen die Informationsbeziehungen zwischen Sachverständigem und Verteidiger unter Datenschutzgesichtspunkten - insbesondere im Hinblick auf sensible, der Geheimhaltungspflicht unterliegende Informationen - einer genaueren Prüfung.

4.2 Einsichtnahme in Telefonüberwachungsunterlagen durch eine VersicherungEin Petent, dessen Telefon im Rahmen eines Ermittlungsverfahrens für die Dauer von drei Monaten überwacht wurde, hat sich darüber beschwert, daß eine private Versicherung im Wege der Akteneinsicht Kenntnis vom Inhalt der Telefonüberwachungsprotokolle erhalten habe. Gegen den Petenten wurde wegen schwerer Brandstiftung ermittelt. Seine Haftpflichtversicherung äußerte zudem den Verdacht eines Versicherungsbetruges. Ihrem Anwalt wurde Einsicht in die Telefonüberwachungsakte zur Klärung dieses weiteren Tatvorwurfs gewährt. Die Staatanwaltschaft trägt vor, daß die Akteneinsicht nur in Teile der Telefonüberwachungsakte eingeräumt wurde. Das Ermittlungsverfahren wegen des Verdachts der Brandstiftung wurde eingestellt; der Verdacht des Versicherungsbetruges konnte ebenfalls nicht erhärtet werden. Bereits vor Gewährung der Akteneinsicht hatte die Staatsanwaltschaft die Vernichtung der Telefonunterlagen angeordnet, weil sie - wie es das Gesetz in einem solchen Fall vorsieht (§ 100 b Abs. 6 StPO) - nach Aufassung der Staatsanwaltschaft nicht mehr benötigt wurden. Die Anordnung war jedoch zum Zeitpunkt der Akteneinsicht noch nicht vollzogen.Einige durchnummerierte Leerblätter ließen erkennen, daß einzelne Seiten abhanden gekommen waren.Ich halte die Gewährung der Einsichtnahme in die Telefonüberwachungsunterlagen durch den Anwalt der Versicherung für bedenklich. Ein zwingender Versagungsgrund für die Akteneinsicht liegt nach geltendem Recht nur vor, soweit überwiegen-

de schutzwürdige Interessen des Beschuldigten oder anderer Personen entgegenstehen (§ 406 e Abs. 2 StPO).Eine sorgfältige Güterabwägung war um so mehr geboten, als wegen des Verdachts des Betruges eine Telefonüberwachung nicht zulässig ist; diese Straftat gehört nicht zu dem im Gesetz abschließend festgelegten Katalog strafbarer Handlungen, die eine solch eingriffsintensive, das Grundrecht auf Wahrung des Telefongeheimnisses einschränkende Maßnahme rechtfertigt; die Telefongespräche des Betroffenen wurden immerhin drei Monate lang überwacht. Die Staatsanwaltschaft macht zwar geltend, daß mit Rücksicht auf die Rechtsprechung nicht nur Katalogtaten, die die Telefonüberwachung rechtfertigen (§ 100 a StPO), sondern auch Zufallsfunde, sofern sie nicht in anderen Strafverfahren verfolgt werden (Argument § 100 b Abs. 5 StPO), keinem Verwertungsverbot unterliegen. Diese Auffassung mag zwar den staatlichen Verfolgungsanspruch insoweit begründen. Zweifelhaft bleibt jedoch, ob die Äußerung des Verdachts einer strafbaren Handlung auch die Akteneinsicht privater Stellen in Telefonüberwachungsakten rechtfertigen kann. Im Stadium der Ermittlung diente diese nicht primär der Verwertung, sondern der Suche nach Zufallsfunden. Private Stellen haben jedoch keine Strafermittlungsbefugnisse. Die Staatsanwaltschaft hatte jedenfalls bereits vor der Einsichtnahme die Vernichtung der Telefonunterlagen angeordnet, weil sie nach ihrer Auffassung zur Strafverfolgung nicht mehr erforderlich waren (§ 100 b Abs. 6 StPO). Wäre diese Anordnung - wie im Gesetz vorgesehen - "unverzüglich" vollzogen worden, hätte eine Akteneinsicht nicht stattfinden können. Zwischen der Vernichtungsanordnung und der Akteneinsicht lagen immerhin mehr als zwei Monate. Regiert hier der Zufall oder das Recht? Zudem sprechen Leerblätter nicht unbedingt für datenschutzgerechte Aktenverwaltung. Es war

nicht nachvollziehbar aufgezeichnet, ob die Gesamtakte oder nur bestimmte Aktenteile dem Anwalt zur Akteneinsicht vorlagen. Die Überlassung der gesamten Telefonüberwachungsakte würde Bedenken rechtfertigen, daß die Akteneinsicht der unzulässigen Ausforschung des Verdächtigen diente.Nachträglich hat die Staatsanwaltschaft die Vernichtung der Telefonüberwachungsakte veranlaßt.4.3 Berichtspflichten in Strafsachen und die richterliche UnabhängigkeitIm Geschäftsbereich des Ministeriums der Justiz besteht eine Verwaltungsanordnung über Berichtspflichten in Strafsachen aus dem Jahre 1958 (BeStra Nr. 10). Diese richtet sich vor allem an die Staatsanwaltschaft. In Privatklagesachen soll auch der Richter zur Mitteilung auf dem Dienstweg an das Ministerium der Justiz verpflichtet sein. Dabei handelt es sich um Verfahren, in denen sich der Verletzte zur Durchsetzung des Strafanspruchs unmittelbar an das Gericht wenden kann, ohne daß es der vorherigen Anrufung der Staatsanwaltschaft bedarf (z.B. bei Hausfriedensbruch, Beleidigung, Verletzung des Briefgeheimnisses, Körperverletzung, Sachbeschädigung). Eine Mitteilungspflicht soll dann bestehen, wenn die Angelegenheit wegen der Persönlichkeit oder Stellung eines Beteiligten (z.B. Bürgermeister, Politiker, Unternehmern) wegen der Art der Beschuldigung oder aus anderen Gründen weitere Kreise beschäftigt oder dies voraussichtlich der Fall sein wird. Das Gericht soll in diesem Fall eine Abschrift der Privatklage übersenden.

Ich habe bereits in früheren Tätigkeitsberichten (vgl. zuletzt 12. TB, LT-Drucksache 10/451, Seite 34) vorgetragen, daß Mitteilungen aus gerichtlichen Verfahren einer gesetzlichen Ermächtigung bedürfen. Alle Mitteilungen sollten in einem Justizmitteilungsgesetz zusammenfassend geregelt werden. Die bisherige Regelung durch Verwaltungsvorschrift entspricht nicht mehr den Anforderungen. Auch die Anordnung über Berichtspflichten in Strafsachen zählt zu diesen Verwaltungsvorschriften.Meiner Empfehlung diese Vorschrift zu streichen, ist das Ministerium der Justiz letztlich nicht gefolgt mit der Begründung, die Verwaltungsanordnung habe der Richter aufgrund allgemeinen Dienstrechts zu befolgen.Ich vermag diese Auffassung schon deshalb nicht zu teilen, weil die Privatklageschrift das gerichtliche Strafverfahren einleitet, für dessen Durchführung dem Richter von Verfassungs wegen richterliche Unabhängigkeit und damit Freistellung von jeglicher Beeinflussung gewährleistet ist. Die vom Gericht zu beachtenden Bestimmungen in Privatklageverfahren sind abschließend im Strafverfahrensrecht (§§ 374 StPO ff) geregelt. Auch hat der Richter die Pflicht, die Amtsverschwiegenheit zu wahren, so lange das Verfahrensrecht eine Öffentlichkeit der Verhandlung nicht vorschreibt. Auch wenn eine Dienstpflicht im Einzelfall als Maßnahme der Richterdienstaufsicht in Betracht kommen sollte, entzieht sich die Materie einer allgemeinen Regelung, weil konkrete, begründende Einzelanlässe nicht voraussehbar sind. Eine generalisierende Regelung ist aber mit der verfassungsrechtlich garantierten Unabhängigkeit des Richters nicht vereinbar.Die Erforderlichkeit muß zudem bezweifelt werden. Als Indiz für die mangelnde Notwendigkeit mag die seitens

des Ministeriums eingeräumte Tatsache sein, daß in den letzten Jahren kein Eingang von Mitteilungen eines Richters in Privatklagesachen registriert wurde. 4.4 Entwurf eines Strafverfahrensänderungsgesetzes

(StVÄG 1994)Mit der Zielsetzung, der Rechtsprechung des Bundesverfassungsgerichts, insbesonderem dem Volkszählungsurteil, Rechnung zu tragen, haben die Bundesländer Saarland, Hessen und Bayern im Auftrag der Justizministerkonferenz einen Entwurf eines Strafverfahrensänderungsgesetzes erarbeitet. Der Bundesrat hat im Oktober 1994 beschlossen, diesen Gesetzesentwurf beim Deutschen Bundestag einzubringen. Es ist zu begrüßen, daß die Anstrengungen, datenschutzrechtlich bedeutsame Ergänzungen der Strafprozeßordnung zu formulieren, fortgesetzt wurden. Bereits 1989 hat das Bundesjustizministerium Vorschläge entwickelt, zu denen ich Stellung genommen habe (vgl. meinen 9. TB, Lt-Drucksache 9/1521, Tz. 2.1, Entschließung der DSB-Konferenz Anlage 1; meinen 11. TB, Lt-Drucksache 10/4, Tz. 5 und Entschließung der DSB-Konferenz Anlage 11; meinen 12. TB, Lt-Drucksache 10/451, Tz. 4.1). Datenschutzrechtliche Defizite im Bereich der Justizmitteilungen (vgl. meinen 8. TB, Lt-Drucksache 9/1038, Tz. 3.2.1) und der Aufbewahrungsdauer von Strafakten werden allerdings in dem Entwurf 1994 nicht einmal ansatzweise angesprochen. Insgesamt bleibt der neue Entwurf unter Datenschutzgesichtspunkten hinter dem im Entwurf 1989 Erreichten zurück.Die neukonzipierten Informationserhebungsregelungen für die Staatsanwaltschaft und die Polizei vermögen dem Dilemma nicht zu entgehen, bei geringgewichtigen Informationseingriffen (im Gegensatz zu besonderen

Ermittlungsmethoden wie z.B. Rasterfahndung, Schleppnetzfahndung, verdeckte Ermittler) sich mit pauschalisierenden Klauseln zu behelfen. Die Insuffizienz der Norm gegenüber der Vielfalt der Informationsbeschaffungssituationen (z.B. spontane und angeforderte Informationslieferungen öffentlicher Stellen) wird nicht verkannt; eine allzugroße Regelungsdichte könnte ihrerseits wiederum Gefahren für die Transparenz der Informationsverarbeitung zur Folge haben. Während man insoweit bemüht war, eine weitgespannte Ermächtigungsgrundlage zu geben, war man beispielsweise weniger geneigt, die schutzwürdigen Belange der im Strafverfahren Betroffenen, insbesondere von Opfern, Verletzten, Zeugen, hinreichend gegen unangemessene Informationsbegehrlichkeiten anderer Stellen und vor allem privater Dritter, die nicht Verletzte sind, zu schützen. Hochsensible Informationen aus der Intimsphäre der Betroffenen (z.B. medizinische und pychologische Gutachten, Abhörprotokolle aus der Telefonüberwachung), die auch mit Zwangsmitteln ermittelt werden, dürfen in Strafakten als Informationsquelle nicht am Strafverfahren Beteiligter nur unter eingeschränkten Voraussetzungen dienen. Die Akteneinsicht hat gegenüber der weniger eingriffsintensiven Auskunft zurückzutreten.Die Vorschriften für die Einrichtung einer Zentraldatei für mehrere Staatsanwaltschaften eines Landes oder zweier benachbarter Staatsanwaltschaften zweier Bundesländer für ein kriminalgeographisch einheitlich zu betrachtendes Gebiet bedürfen weiterer Präzisierungen.Die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederum mit der Thematik befaßt (vgl. Entschließung vom 09./10.03.1994 Anlage 4; Entschließung vom 26./27.09.1994 Anlage 5).

Der eingebrachte Gesetzesentwurf hat dieser Kritik in zwei Punkten Rechnung getragen. So dürfen personenbezogene Daten, die durch besondere Ermittlungsmaßnahmen - also etwa durch Rasterfahndung oder den Einsatz verdeckter Ermittler - gewonnen werden, den Polizeibehörden nur unter einschränkenden Voraussetzungen zur Verfügung stehen. Erst wenn dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit oder zur Verhütung von Straftaten von erheblicher Bedeutung erforderlich ist, sollen die Daten den Polizeibehörden übermittelt werden dürfen. Außerdem sollen Datenbestände regelmäßig daraufhin überprüft werden, ob die Speicherung weiterhin erforderlich ist. 4.5 Behandlung von Pfändungs- und Überweisungsbeschlüssen durch GerichtsvollzieherHat der Lohnempfänger Schulden können Probleme entstehen, wenn der Gläubiger zur Befriedigung seiner Ansprüche auf den Lohn "zugreift" und aus einem Urteil unmittelbar gegenüber dem Arbeitgeber - also gegenüber dem Drittschuldner - vollstreckt (§ 840 ZPO). Klagen sind laut geworden, daß bei der Zustellung von Pfändungs- und Überweisungsbeschlüssen an den Arbeitgeber der Gerichtsvollzieher die Dokumente offen an der Pforte des Unternehmens, beim Hausmeister oder sonstigen Arbeitnehmern abgegeben hat. Dadurch wurden die wirtschaftlichen Verhältnisse des Betroffenen in nicht hinnehmbarem Umfang gegenüber Dritten offenbart. Die Zustellung sollte jedoch auch unter Beachtung der gesetzlich vorgeschriebenen Förmlichkeiten in einer für den Betroffenen möglichst schonenden Weise erfolgen. In den meisten Fällen ist eine Zustellung an den Firmeninhaber persönlich oder bei juristischen Personen an den gesetzlichen Vertreter nicht möglich. Die

dann notwendige Ersatzzustellung sollte grundsätzlich an einen Bediensteten erfolgen, der ermächtigt ist, im Zusammenhang mit Forderungspfändungen verbindliche Erklärungen (Drittschuldnererklärung) abzugeben (z.B. Bedienstete des Lohnbüros). Sind auch solche besonders ermächtigten Bediensteten für den Gerichtsvollzieher nicht erreichbar, sollte die Zustellung gegenüber anderen Bediensteten nur in verschlossenem Umschlag mit der Bitte um Weiterleitung an die Geschäftsführung übergeben werden. Die Geschäftsanweisung der Gerichtsvollzieher erlaubt in solchen Fällen die offene Übergabe der Unterlagen, selbst wenn von diesem Personenkreis eine Drittschuldnererklärung nicht verlangt werden kann. Eine Neufassung der Geschäftsanweisung ist - auch nach Überzeugung der Justizverwaltung - geboten.4.6 Prüfung der JustizvollzugsanstaltEine in der Justizvollzugsanstalt Saarbrücken durchgeführte Prüfung hat erhebliche Mängel offenbart. Der Datenschutz hat bislang die hohen Gefängnismauern noch nicht überwunden. Zwar hat der Gefangene im Vergleich zum freien Bürger
Einschränkungen seiner Grundrechte hinzunehmen; das Grundrecht auf informationelle Selbstbestimmung darf ihm jedoch im Kern nicht vorenthalten werden. Auch im Strafvollzug gilt das Erforderlichkeitsprinzip. Wie soll der Gefangene das Vollzugsziel, nämlich seine Resozialisierung erreichen, wenn ihm nicht eine gewisse Grundausstattung an Bürgerrechten auch hinter Gefängnismauern garantiert wird, die geeignet sind, eine Eigenverantwortlichkeit und Selbständigkeit zu stärken. Alle Formen der Informationsverarbeitung im Strafvollzug sind deshalb an der Erforderlichkeit für die Belange des Vollzugs, der Sicherheit des Vollzugsbe-

diensteten, aber auch an der Notwendigkeit zu messen, den Gefangenen zu resozialisieren. Da auch die interne Informationsverarbeitung in der Vollzugsanstalt einen Eingriff in das Selbstbestimmungsrecht darstellt, bedarf es einer besonderen Ermächtigung durch bereichsspezifische Regelungen. Die Bereinigung von Defiziten in dieser Hinsicht sind schon seit einiger Zeit angemahnt. Bisher ist es jedoch nicht gelungen, das Strafvollzugsgesetz den rechtstaatlichen Anforderungen des Datenschutzes anzupassen. In der Übergangszeit bis zur Verabschiedung normenklarer Regelungen müssen jedoch bereits alle Möglichkeiten für einen schonenden Umgang mit den Daten der Gefangenen genutzt werden.Bei der Aufnahme eines Gefangenen in die Strafvollzugsanstalt liegen bereits eine große Zahl von Angaben zur Person des Betroffenen vor, die mit dem Aufnahmeersuchen übermittelt werden. Bereits zu diesem Zeitpunkt können unter anderem bei Strafen von mehr als einem Monat die vollständige Abschrift des zu vollstreckenden Urteils mit Informationen über Dritte wie Zeugen, Opfer, Geschädigte vorliegen; ferner in Bezug auf die Gefangenen auch Hinweise auf seelische oder geistige Abartigkeit, Selbstmordgefahr, gleichgeschlechtliche Neigungen, Suchtgefahr, Neigung zu gewalttätigem Verhalten. In der Regel sind zwar ärztliche und psychologische Gutachten aus dem Ermittlungsverfahren dem Ersuchen nicht beigefügt, können jedoch auch im Interesse der Vollzugsplanung von der Vollzugsanstalt angefordert werden. Im Verlauf des Vollzuges werden diese Informationen in vielfältiger Hinsicht angereichert. Beim Neuzugang werden bereits auf verschiedenen Formularen zusätzliche Informationen erhoben. Der sogenannte A-Bogen enthält den Basisdatensatz, der unter anderem Personengrunddaten, die Zahl der Vorstrafen, frühe-

re Maßregeln, das religiöse Bekenntnis, Familienstand und Kinderzahl, Namen und Wohnung der nächsten Angehörigen, erlernten Beruf sowie Tatgenossen enthält. Dieser Bogen dient der Unterrichtung einer Vielzahl von Stellen innerhalb der Vollzugsanstalt, denen die per Umdruckverfahren mit Hilfe einer Matrize hergestellten Mehrausfertigungen des A-Bogens übermittelt werden. Die Bediensteten der Zugangsabteilung, der Arbeitsverwaltung, des Sicherheits- und Ordnungsdienstes, des Sozialdienstes, des psychologischen und pädagogischen Dienstes, die Verantwortlichen für die Besucher- und Prüfkartei haben auf Befragen unumwunden eingeräumt, daß sie zur Wahrnehmung ihrer Aufgaben nur einen geringen Teil der aufgeführten Informationen benötigen. Ohne Interesse ist für den Arzt die Zahl der Vorstrafen, die Namen der Tatgenossen, für den Pädagogen und die Arbeitsverwaltung die Tatgenossen und die Anschriften der nächsten Angehörigen, für die Arbeitsverwaltung Familienstand und Zahl der Kinder; für die Verwaltung der Brief- und Besucherkartei ist die Kenntnis von Geburtsort, erlerntem und ausgeübtem Beruf, Staatsangehörigkeit, zuständige Meldebehörde, Anzahl der Vorstrafen und Tatgenossen nicht erforderlich. Für alle Stellen - außer dem Seelsorger und für die Anstaltsküche im Falle von Diätpräferenzen (Mohamedaner) - ist das religiöse Bekenntnis ohne Belang. Weitere Formulare mit noch sensibleren Angaben werden
im anstaltsinternen Zugangsrundlauf Stellen zugänglich, die diese Informationen ebenfalls nicht benötigen. Der Bogen C gibt Auskunft über das Ergebnis ärztlicher Untersuchungen; der Bogen D enthält in ausführlicher Form Einzelheiten über viele Lebensbereiche des Gefangenen, die er in einem Zugangsgespräch - oftmals eine Art "Lebensbeichte" - gegenüber der Anstaltsleitung offenbart hat. Der B-Bogen enthält eine vom Arzt gefertigte Personenbeschreibung, die im Bedarfsfall - etwa bei Flucht eines Gefangenen - für Fahndungszwecke

benötigt wird. In den Bögen E und F kann der Gefangene auf freiwilliger Basis einen Lebenslauf schreiben und vorgegebene Fragen beantworten. Beamte des Sicherheits-- und Ordnungsdienstes haben erklärt, daß sie außer dem Zugangsgespräch der Anstaltsleitung die Bögen nicht benötigen. Der Anstaltsarzt möchte auf das Zugangsgespräch, den Lebenslauf des Gefangenen und den Fragebogen für den Gefangenen verzichten. Die Arbeitsverwaltung wiederum sieht keine Notwendigkeit für das Zugangsgespräch der Anstaltsleitung, den Lebenslauf und den Fragebogen für den Gefangenen. Sicherheits- und Ordnungsdienst, Sozialdienst, pädagogischer Dienst und psychologischer Dienst wiederum benötigen nach eigener Einschätzung nicht die Personenbeschreibung.Abgesehen vom anstaltsinternen Zugangsrundlauf wird schließlich der A-Bogen auch noch der Einweisungsbehörde, dem Landeskriminalamt und bei Ausländern auch dem Ausländeramt übermittelt. Der Datentransfer an externe Stellen ist in dem auf dem A-Bogen enthaltenen Umfang nicht erforderlich und deshalb unzulässig. Insofern habe ich ein kleines Zugeständnis erkämpfen können. Staatsanwaltschaft und Gerichten wird der A-Bogen nicht mehr übersandt; die Vorstrafen werden aufgrund der Angaben des Gefangenen nicht mehr erfaßt. Im übrigen findet der Datentransfer an externe Stellen jedoch wie gewohnt statt.Anstaltsleitung und Ministerium der Justiz haben zwar eingeräumt, daß die interne und externe Informationsweitergabe nicht den Anforderungen gerecht wird. Weder technische Ausstattung noch Personalausstattung seien ausreichend, um einen am Maßstab der Erforderlichkeit orientierte Informationsweitergabe innerhalb und außerhalb der Anstalt zu organisieren. Im Ergebnis bleibt festzuhalten, daß eine hoffnungslos veraltete Informationstechnik einer routinisierten

Informationsstreuung Vorschub leistet, die in gar keiner Weise den Anforderungen des Datenschutzes gerecht wird.Kernstück der Datenverarbeitung in der Strafvollzugsanstalt ist die Gefangenenpersonalakte, in der die Informationen über die Gefangenen zusammengefaßt und fortlaufend in drei verschiedenen Teilen (Heftnadeln) abgeheftet werden. Es werden dort nicht nur die bereits genannten Formblätter und Einweisungsunterlagen, sondern der gesamte, während der Haft anfallende Schriftverkehr, zum Beispiel Anträge des Gefangenen auf Vollzugslockerung, die erkennungsdienstlichen Unterlagen (Lichtbilder und Personenbeschreibungen) sowie Gutachten des psychologischen Dienstes abgelegt. Die Prüfung hat ergeben, daß sich in der Personalakte sogar teilweise ärztliche Verordnungen und Laborergebnisse zur Überwachung des Drogenmißbrauchs befinden. Diese umfassende Informationssammlung über den Gefangenen und häufig auch über Dritte (Angehörige des Gefangenen und aufgrund der Feststellungen in den Strafurteilen: Opfer, Geschädigte, Zeugen, Mittäter) wird zentral in der Vollzugsgeschäftsstelle aufbewahrt und ist praktisch jedem Bediensteten der Strafvollzugsanstalt zugänglich. Das Verfahren der Einsichtnahme durch die Vollzugsbediensteten ist förmlich nicht geregelt, insbesondere wird der Grund für die Akteneinsicht nicht dokumentiert. Lediglich der aktuelle Verbleib der Akte wird bei Mitnahme aufgezeichnet. Die schon bei dem Zugangsrundlauf beklagte Informationsstreuung findet durch die Art der Aktenaufbewahrung und die weitgehende Zugriffsmöglichkeit ihre Fortsetzung.Die Aktenhaltung und der Aktenzugriff müssen grundlegend reorganisiert werden. Die Auffassung des Ministeriums der Justiz teile ich nicht, daß alle Bedienste-

ten Zugriff auf die Personalakte haben müssen. Zwar haben alle Bediensteten eine Mitwirkungspflicht beim Strafvollzug, ihre Funktionen und Aufgaben sind gleichwohl verschieden; dies gilt auch für die Intensität des Kontaktes zu den einzelnen Strafgefangenen. Aus dem arbeitsteiligen Behandlungsvollzug folgt ein unterschiedlicher Informationsbedarf, der sich in einer differenzierten Zugriffsregelung widerspiegeln muß. Schon gar nicht muß der gesamte Inhalt der Personalakte, der auch nicht unbedingt vollzugsrelevantes Material enthält, von jedem Bediensteten eingesehen werden.Meine Forderungen lassen sich wie folgt zusammenfassen:- Der Akteninhalt muß stärker in Teilinformationsmengen aufgegliedert werden. Ansätze finden sich bereits in den sogenannten Heftnadeln, die die Akte in drei Teile gliedert. Insbesondere muß die Gefangenenpersonalakte von Routinevorgängen, die in Beiakten geführt werden sollten, entlastet werden, damit nicht bei jeder Vollzugsentscheidung die gesamte Akte eingesehen werden muß.- Nicht nur medizinische Befunde, Diagnosen und sonstige ärztliche Erhebungen - auch wenn der Gefangene die Informationen freiwillig mitteilt - sind - das ist unstreitig - beim Anstaltsarzt zu verwahren. Umstritten und daher weiter erörterungsbedürftig ist meine Forderung, daß psychologische Gutachten beim psychologischen Dienst der Anstalt aufzubewahren sind. Dafür spricht - ungeachtet aller rechtlichen Überlegungen im Hinblick auf den strafbewehrten Geheimnisschutz (§ 203 Abs. 1 Nr. 2 StGB) -, daß auf diese Weise die sensiblen Informationen nur in dem für den Vollzug erforderlichen Umfang von den an Vollzugsentscheidungen Beteiligten und den im inten-

siven Kontakt mit dem einzelnen Gefangenen stehenden Bediensteten genutzt werden. Die Vollzugsgeschäftsstelle, wo die Akten zentral verwaltet werden, ist am unmittelbaren Vollzug nicht beteiligt, so daß auch dort derartig sensible Informationen nicht aufbewahrt werden sollten.- Der Zugriff auf die Gefangenenpersonalakte ist nach dem Maßstab der Erforderlichkeit zu beschränken. Einsichtnahmen und Herausgaben der Personalakten sowie der Grund sind zu dokumentieren. Der Aktenumlauf in der Vollzugsanstalt hat in Verschlußmappen oder "von Hand zu Hand" zu erfolgen.Neben der zentralen Gefangenenpersonalakte werden noch eine Vielzahl von Karteien und Unterlagen geführt; die Überprüfung ihrer Notwendigkeit und ihres Umfangs muß noch in weiteren Kontrollbesuchen fortgesetzt werden. Zu einzelnen Punkten habe ich bereits Beanstandungen ausgesprochen.Bei der Aufnahme der Gefangenen werden erkennungsdienstliche Maßnahmen durchgeführt (§ 86 StVollZG); und zwar werden neben der Personenbeschreibung durch den ärztlichen Dienst Lichtbilder gefertigt. Im Archiv der abgelegten Personalakten wurden bis zu vier Lichtbilder vorgefunden. Die variierende Zahl der Lichtbilder läßt nur den Schluß zu, daß diese im Einzelfall zur Aufgabenwahrnehmung nicht erforderlich waren. Die im Archiv abgelegten Lichtbilder werden nach Bekundung der Bediensteten bei der späteren Neuaufnahme desselben Betroffenen nicht weiter verwendet.Jede erkennungsdienstliche Maßnahme stellt einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung dar. Inzwischen hat das Ministerium der Justiz auf meine Beanstandung hin klargestellt, daß Fotografien von Gefangenen als er-

kennungsdienstliche Unterlagen nur für den unabweisbaren Bedarf gefertigt werden dürfen. Anzahl und Verbleib werden dokumentiert. Der Gefangene wird zum Zeitpunkt der Entlassung über sein Recht, die Vernichtung der erkennungsdienstlichen Unterlagen zu verlangen, belehrt.Auf meine weitere Beanstandung hin ist inzwischen klargestellt, daß in der Kartei des Sicherheits- und Ordnungsdienstes keine Informationen über Aids gespeichert werden dürfen. Nach einem früheren Erlaß des Ministeriums der Justiz ist nur der Anstaltsleiter durch den Anstaltsarzt über den positiven Befund zu unterrichten.Auch die regelmäßige Aufbewahrungsdauer der Personalakten, die nach der Entlassung des Gefangenen im Archiv abgelegt werden, muß überprüft werden. Seit Jahren fordern die Datenschutzbeauftragten eine gesetzliche Normierung der Aufbewahrungsbestimmungen (Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25.11.1986, mein 9. TB Anlage 1 Nr. 3). Ich begrüße es, daß meine Anregungen zu der Aufbewahrungsbestimmung bei der zukünftigen Novellierung des Strafvollzugsgesetzes berücksichtigt werden sollen. Insgesamt halte ich die Aufbewahrungsfristen für zu lang bemessen. Nach den eigenen Bekundungen der Vollzugsbediensteten werden die archivierten Akten bei weiterer Inhaftierung des Betroffenen regelmäßig nicht herangezogen. Die Erforderlichkeit längerer Aufbewahrungsfristen - insbesondere bei Abschiebehäftlingen - muß deshalb bezweifelt werden.Ein besonderes Problem stellt die Speicherung von
Namen und Wohnung der Angehörigen dar. Diese Angaben werden regelmäßig, ohne daß der Betroffene überhaupt etwas davon weiß, beim Gefangenen erhoben. Es steht außer Frage, daß diese Daten für die Betreuung des

Gefangenen und seiner Resozialisierung von großer Bedeutung sind. Gleichwohl haben auch die Angehörigen das Recht, darüber zu befinden, ob ihre Daten in der Strafvollzugsanstalt gespeichert werden. Es muß grundsätzlich ihrer Entscheidung überlassen bleiben, ob sie den Gefangenen überhaupt betreuen wollen. Ihre Einwilligung ist deshalb unerläßlich. In den wenigsten Fällen kann diese jedoch von vorneherein eingeholt werden. Um dieser Problematik einigermaßen gerecht zu werden, habe ich vorgeschlagen, die Daten dieses Personenkreises bis zur Einholung der Einwilligung gesondert aufzubewahren und nicht in der Gefangenenpersonalakte mit allen anderen Unterlagen zu speichern. Nach einer noch näher festzulegenden Frist sollten Daten von Angehörigen - oder wer auch immer unter dieser Bezeichnung erfaßt wird -, die nicht erschienen, sich nicht um den Gefangenen in einer anderen Weise gekümmert haben, gelöscht werden.

5. Verfassungsschutz5.1 Prüfung des Landesamtes für Verfassungsschutz (LfV)In den Monaten Juni und Juli 1993 wurde das Landesamt für Verfassungsschutz einer Prüfung unterzogen. Das Saarländische Verfassungsschutzgesetz ist am 17.04.1993 in Kraft getreten. Die Rechtsgrundlagen für die Datenverarbeitung durch die Verfassungsschutzbehörde haben sich entscheidend verändert (vgl. meinen 14. TB S. 6 ff, Lt-Drucksache 10/1403). So dürfen etwa im Extremismusbereich personenbezogene Informationen vor der Festlegung eines Beobachtungsobjektes, die der Zustimmung des Ministeriums des Innern bedarf, nur aus allgemein zugänglichen Quellen erhoben werden. Erst nach dieser Festlegung dürfen personenbezogene Daten in Dateien gespeichert werden. Die Festlegung des Beobachtungsobjekts ist das wichtigste Steuerungselement für die Informationsverarbeitung des LfV.Mit dem gleichzeitig in Kraft getretenen Saarländischen Datenschutzgesetz ist erstmals meine Kontrollkompetenz für das Landesamt für Verfassungsschutz begründet worden. Damit wurde die in der Bundesrepublik Deutschland seit 15 Jahren bestehende einmalige Sonderstellung des Landesamtes für Verfassungsschutz im Saarland beseitigt.5.1.1 DienstanweisungenAuf unsere Prüfung hin hat das Landesamt für Verfassungsschutz die Anpassung der Dienstanweisungen an die neue Rechtslage angekündigt. Die Stellungnahmen des Landesamtes für Verfassungsschutz auf unseren Prüfbericht vom 21.10.1993 ließen allerdings nicht erkennen, inwieweit diesem Anliegen Rechnung getragen ist. Vor Erlaß von Verwaltungsvorschriften ist überdies der

Landesbeauftragte für Datenschutz zu beteiligen (§ 8 Abs. 1 SDSG). Lediglich der Entwurf einer Dienstanweisung über "nachrichtendienstliche Mittel" zur heimlichen Informationsbeschaffung etwa durch den Einsatz von V-Männern und von technischen Mitteln wurde vorgelegt, der jedoch den gesamten Bereich der Informationsbeschaffung und -auswertung nicht abdeckt. Der Entwurf entsprach nicht den Anforderungen, weil er die schon im Gesetzgebungsverfahren beklagte hinreichende Klarheit über den Einsatz der Mittel nicht herstellte. Insbesondere war nicht abschließend geregelt, welche nachrichtendienstlichen Mittel das Landesamt für Verfassungsschutz anwenden darf. Der Einsatz nachrichtendienstlicher Mittel ist besonders eingriffsintensiv, weil die heimliche Vorgehensweise regelmäßig mit Täuschung des Betroffenen verbunden ist und massenhaft Überschußinformationen anfallen können. Die Voraussetzungen, unter denen solche Handlungsmethoden angewendet werden dürfen, hat der Gesetzgeber selbst festzulegen (Gesetzesvorbehalt und Wesentlichkeitslehre). Wenigstens in der Dienstanweisung hätten deshalb möglichst konkrete Regelungen getroffen werden müssen. Klare Handlungsanweisungen können nur erreicht werden, wenn die Verwaltungsvorschrift auf einem geringeren Abstraktionsniveau als das Gesetz möglichst detaillierte Regelungen trifft. Der Verweis auf den Gesetzeswortlaut, wie stellenweise geschehen, genügt deshalb nicht den Anforderungen. Der Entwurf blieb sogar hinter den gesetzlichen Vorgaben zurück (z.B. beim Einsatz nachrichtendienstlicher Mittel gegenüber Einzelpersonen; § 5 Abs. 1 Satz 2 SVerfSchG). Die im übrigen derzeit bereits vorliegenden Dienstanweisungen für die Beschaffung und Auswertung von Informationen waren ausdrücklich lediglich als "vorläufig" oder als "Entwurf" bezeichnet, die ebenfalls die Gesetzesnovelle noch nicht berücksichtigten. Mit dem Gesetz insbesondere nicht vereinbar ist die vorläufige Anwei-

sung, daß eine verkürzte Zeitspeicherung zulässig ist, wenn lediglich ein Zweifelsfall vorliegt. Tatsächliche Anhaltspunkte für einen Verdacht sind jedoch unerläßlich (§ 7 Abs. 2 Satz 1 SVerfSchG). Auch sollten die Richtlinien und Dienstanweisungen für
alle Formen des Extremismus nach einheitlichen Rechtsgrundsätzen ausgerichtet werden. Praktische Schwierigkeiten in der Ausformulierung werden schon dadurch gemindert, daß sich die Organisationsstrukturen in den beiden Bereichen des Extremismus immer mehr angleichen (zu den neuen autonomen, rechtsextremistischen Strukturen vgl. Verfassungsschutzbericht NRW, Zwischenbericht Januar bis August 1994, Seite 6). Da jedoch außer der genannten keine weiteren Dienstanweisungen vorgelegt wurden, besteht Grund zu der Annahme, daß weder neue erarbeitet, noch die alten der neuen Rechtslage angepaßt wurden. Meiner Bitte um Stellungnahme wurde bislang nicht gefolgt.5.1.2 Bezeichnung und Festlegung der Beobachtungs-
objekteDie Förmlichkeit, eine Bestrebung oder eine Einzelperson als Beobachtungsobjekt festzulegen, die gemäß § 3 Abs. 1 Satz 4 Saarländisches Verfassungsschutzgesetz der Zustimmung des Ministeriums des Innern bedarf, war jedenfalls zu Beginn der Prüfung nicht beachtet; sie wurde - wie das Landesamtes für Verfassungsschutz selbst einräumt -, erst vor Abschluß der Prüfung förmlich nachgeholt. In keinem einzigen aktuellen Fall konnte im Verlauf der Prüfung eine Dokumentation in den Akten und Unterlagen festgestellt werden, wonach die förmliche Beteiligung des Ministeriums des Innern in der Form der Zustimmung erfolgt war. Anläßlich meiner Prüfung hat das Amt zugesichert, daß entsprechend der neuen Rechtslage, zukünftig alle Beobachtungsobjekte mit akuellem Stand unter Einschluß von

Zeitpunkt und Dauer festgelegt und dokumentiert werden. Ferner wurde auch klargestellt, daß sogenannte "militante Einzelkämpfer" in Zukunft als Beobachtungsobjekte förmlich nachgewiesen werden.Ich habe darauf gedrungen, daß die Personenzusammenschlüsse aus Gründen der rechtsstaatlich erforderlichen Begrenzung der Beobachtungsaktivität des Verfassungsschutzes eindeutig bestimmt sein müssen. Trotz aller praktischen Schwierigkeiten, die sich bei lockeren Organisationsformen ergeben können, sind alle aus der konkreten Situation herzuleitenden Anknüpfungspunkte für eine Kennzeichnung zu nutzen, um eine möglichst eindeutige Zuordnung des Personenkreises zu gewährleisten. Dies schließt keineswegs aus, daß eine Person mehreren Personenzusammenschlüssen gleichzeitig oder zu wechselnden Zeitpunkten angehört. Notfalls müssen einzelne Personen, die sich einer eindeutigen Zuordnung entziehen, als "militante Einzelkämpfer" (§ 5 Abs. 1 Satz 3 SVerfSchG) ausgewiesen werden. Es müssen alle Möglichkeiten genutzt werden, eine möglichst genaue Zuordnung und Abgrenzung der einzelnen Beobachtungsfälle zu erreichen. Andernfalls kann die Zustimmung des Ministeriums für die Festlegung des Beobachtungsobjekts ihre Steuerungsfunktion für die Informationsverarbeitung durch das Landesamt für Verfassungsschutz nicht entfalten.5.1.3 Gemeinsame Verbunddatei der Verfassungsschutzbehörden des Bundes und der LänderDas Landesamt für Verfassungsschutz verarbeitet personenbezogene Daten - wie jede andere Behörde auch - in Karteien und Dateien. Von besonderer Bedeutung ist die automatisierte Verbunddatei - NADIS - nach § 6 Bundesverfassungsschutzgesetz, die den Informationsaustausch zwischen dem Bundesamt für Verfassungsschutz und den Landesämtern für Verfassungsschutz gewährleistet. In

ihr dürfen nach der genannten, gesetzlichen Vorschrift nur Daten erfaßt werden, die zum Auffinden von Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind. Wegen Schußwaffengebrauchs auf einem Truppenübungsplatz waren zwei Personen in dieser Verbunddatei gespeichert, obwohl nach eigener Bewertung des Amtes ein extremistischer Hintergrund nicht festgestellt werden konnte. Es handelte sich um "Waffennarren"; Strafverfahren, die gegen sie eingeleitet waren, wurden eingestellt. Die Dateispeicherung, zumal in einer bundesweiten Verbunddatei, setzt "tatsächliche Anhaltspunkte" voraus; reine Zweifel reichen nicht aus. Die Verbunddatei ist kein Verdachtsverdichtungsinstrument, so daß auch eine verkürzte Zeitspeicherung mangels der gesetzlich vorgeschriebenen Voraussetzungen nicht zulässig ist. 5.1.4 "Vorkartei"Das Landesamt für Verfassungsschutz führt im Extremismusbereich eine sogenannte "Vorkartei", in der Personen erfaßt werden, die nicht in der bundesweiten Verbunddatei gespeichert sind. Auch insoweit müssen die gesetzlichen Voraussetzungen für die Dateiverarbeitung erfüllt sein. Es dürfen in Dateien nur Personen gespeichert werden, die ein festgelegtes Beobachtungsobjekt nachdrücklich unterstützen oder als militante Einzelkämpfer auftreten (§ 10 Abs. 1, § 5 Abs. 1 Satz 2 SVerfSchG). Die Stichproben haben diesen strengen, gesetzlichen Anforderungen einer Dateiverarbeitung nicht genügt. So waren Teilnehmer an öffentlichen Veranstaltungen einer extremistischen Bestrebung gespeichert, ohne daß aus ihrem sonstigen Verhalten eine nachdrückliche Unterstützung festgestellt wurde. Schon nach den bisherigen, vorläufigen Anweisungen waren lediglich Anmelder, Leiter oder aktive Teilnehmer an öffentlichen Veranstaltungen zu erfassen, wenn der Betroffene bereits als Extremist bekannt war oder sich

mit Rede- oder Diskussionsbeiträgen extremistischen Inhalts beteiligt oder sonstige Funktionen ausgeübt hat. Die neue Rechtslage, die eine "nachdrückliche Unterstützung" eines extremistischen Personenzusammenschlusses voraussetzt (§ 5 Abs. 1 Satz 2 SVerfSchG), läßt erst recht eine Speicherung nur dann zu, wenn eine über die reine Teilnahme an Demonstrationen hinausgehende Beteiligung zu erkennen ist.Hinfort will das Landesamt für Verfassungsschutz Personen in der Vorkartei nur noch speichern, wenn sie zwar bekannt, aber nicht identifiziert sind. Die gesetzlichen Voraussetzungen im übrigen sollen beachtet werden. Inwieweit unseren Beanstandungen im Einzelfall Rechnung getragen wurde, ist nicht mitgeteilt worden.In einer weiteren Datei wurden Informationen über Personen gespeichert, die aufgrund des Einsatzes nachrichtendienstlicher Mittel gewonnen wurden, ohne daß eine förmliche Festsetzung als Beobachtungsobjekt erfolgt war. Zwar ist der Einsatz nachrichtendienstlicher Mittel ausnahmweise im Einzelfall mit Genehmigung des Ministeriums, die hier vorlag, zulässig (§ 7 Abs. 3 Satz 2 SVerfSchG). Jedoch läßt der nicht weiter auslegbare Gesetzeswortlaut eine Speicherung der so gewonnenen Informationen in Dateien (abgesehen von Spionage und Sabotage) nicht zu (§ 10 Abs. 1 SVerfSchG). Diese Verarbeitungsart ist besonders eingriffsinensiv, weil sie einen schnellen Zugriff auf bestimmte Personen und Selektionen nach bestimmten Merkmalen erlaubt. Fallen beim Einsatz nachrichtendienstlicher Mittel Informationen massenhaft an, so daß eine Verarbeitung sinnvoll nur mit Hilfe von Dateien oder in automatisierten Verfahren möglich ist, dann muß sich die Behörde zu einer Festlegung als Beobachtungsobjekt entschließen und damit die Möglichkeit einer weitergehenden Informationsauswertung durch

Dateiverarbeitung eröffnen. Nur so kann die gesetzlich vorgeschriebene Steuerungsfunktion der Festlegung als Beobachtungsobjekt gewährleistet werden. 5.1.5 Löschungen und BereinigungenBei der Einzelfallbearbeitung, spätestens nach fünf Jahren ist zu prüfen, ob personenbezogene Informationen in Dateien zu löschen oder zu sperren sind; spätestens zehn Jahre nach der letzten gespeicherten, relevanten Information sind regelmäßig personenbezogene Daten aus dem Bereich des Extremismus zu löschen (§ 11 Abs. 2 SVerfSchG). Das LfV hat von vorneherein Handlungsdefizite eingeräumt. Eine umfangreiche Altfallbereinigung ist durchzuführen. Das Landesamt für Verfassungsschutz teilt meine Auffassung, daß Löschungen auch zu einem früheren Zeitpunkt als vor Ablauf der gesetzlich vorgesehenen fünf Jahre unter Berücksichtigung des Maßstabs der Erforderlichkeit durchzuführen sind. Ich stimme allerdings nicht mit dem LfV überein, daß eine solche verkürzte Zeitspeicherung nur im Einzelfall in Betracht kommt. Vielmehr dürfte die Behandlung bestimmter Altersgruppen einer allgemeinen Regelung durch Dienstanweisung zugänglich sein. Dies um so mehr, als das Landesamt aufgrund unserer Überprüfungen bereits angekündigt hat, daß Personendaten von über 70-jährigen gelöscht werden, wenn keine relevanten Aktivitäten in den letzten drei Jahren festgestellt werden. Eine Bereinigung aller Akten, Karteien und Dateien ist auch insoweit zugesagt.Übereinstimmung bestand ebenfalls in der Frage, daß in der Sach- (Indiz-)kartei, in der Fakten nach bestimmten Sachthemen geordnet gespeichert sind, grundsätz-

lich keine personenbezogenen Daten enthalten sein dürfen, weil sonst die gesetzlich vorgeschriebenen Prüf- und Löschfristen nicht eingehalten werden können. Werden Daten in der Verbunddatei gelöscht, hat das LfV zugesagt, auch die zugehörigen Daten in der Sach-(Indiz-)Kartei und in den Akten zu löschen. Damit ist jedoch das Problem der Altfälle im übrigen nicht bereinigt.In der Lichtbilder- und Adreßkartei einer Abteilung ist die Bereinigung der Altfälle ebenfalls sicherzustellen. Zudem ist eine Überprüfung der Zulässigkeit der Speicherung in diesen Dateien mit einem vertretbaren Zeitaufwand nicht möglich, weil eine begleitende Dokumentation der Begründung für die einzelnen Personen in der speichernden Organisationseinheit nicht geführt wird. Die Dokumentation der begründenden Tatsachen ist im Gesetz ausdrücklich vorgeschrieben (§ 10 Abs. 3 SVerfSchG). Der Bestand solcher Dateien muß im übrigen auf das unerläßliche Maß reduziert werden; in ein und derselben Organisationseinheit dürfen nicht zwei verschiedene Lichtbilderkarteien geführt werden, weil sonst die Gefahr einer unzulässigen Doppelerfassung besteht. Auch zur Regelung dieses Bereiches ist eine Dienstanweisung erforderlich.Einvernehmen konnte erzielt werden hinsichtlich der
Dokumentation der Verhandlungen über die Vernichtung von Verschlußsachen. Personenbezogene Daten dürfen in diesen Aufzeichnungen nicht vorgehalten werden, da sonst die Löschungsfristen unterlaufen werden. Über den Stand der Bereinigungen ist mir auch auf
meine Bitte um Stellungnahme bislang nichts mitgeteilt worden.Aufgrund des Rücklaufs von der Staatsanwaltschaft wurde - wie ich feststellte - in der Verbunddatei in

zahlreichen Fällen das Erkenntnisdatum fortgeschrieben. Dieses Datum ist maßgebend für den Lauf der Prüf- und Löschungsfristen. Das Erkenntnisdatum und damit die Löschungsfrist dürfen jedoch nicht "hochgesetzt" werden, weil für die Zulässigkeit der Speicherung relevante, neue Erkenntnisse aus den Urteilen nicht gewonnen werden. Das LfV hat eine Bereinigung zugesagt und inzwischen den Vollzug gemeldet.5.1.6 Dokumentation der Übermittlung aus dem Personal-
ausweisregisterZu beanstanden war ein Verstoß gegen § 10 Abs. 4 des
Ausführungsgesetzes zum Saarländischen Personalausweisgesetz, da die Verpflichtung zur Dokumentation jeder Übermittlung aus dem Personalausweisregister nicht eingehalten wurde. Die betreffende Bestimmung hat bereits vor Inkrafttreten des Saarländischen Verfassungsschutzgesetzes gegolten, so daß die fehlende Dokumentation nicht in Zusammenhang mit der Novellierung des Verfassungsschutzgesetzes stehen kann. Die Rechtmäßigkeit der Datenübermittlungen aus dem Personalausweisregister konnte nicht kontrolliert werden, weil prüffähige Unterlagen nicht vorhanden waren.5.2
Sicherheitsüberprüfung5.2.1 Verfahren der SicherheitsüberprüfungDas Verfahren der Sicherheitsüberprüfung bildete einen der Schwerpunkte meiner Kontrollmaßnahmen, weil in diesem Zuammenhang öffentliche Bedienstete, die an sich unverdächtig sind, in großer Zahl in die Überprüfung einbezogen werden und umfangreiches Datenmaterial anfällt.

Bedienstete in der öffentlichen Verwaltung, die Umgang mit geheimhaltungsbedürftigen Tatsachen oder Erkenntnissen haben, werden einer Sicherheitsüberprüfung unterzogen. Bei hohem Geheimhaltungsgrad (geheim, streng geheim) der Aufgaben, mit denen der Betroffene befaßt ist, führt das LfV tief in das Privatleben und die Intimsphäre eindringende Ermittlungen durch, die auch den Ehegatten, Verlobten und Lebensgefährten einbeziehen. Das Ergebnis hält das LfV in einer Sicherheitsüberprüfungsakte fest.Grundlage der Sicherheitsüberprüfung ist eine "Richtlinie für die Sicherheitsüberprüfung von Bediensteten des Saarlandes sowie der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts". Eine gesetzliche Grundlage für das Verfahren besteht im Saarland, anders als im Bund (Sicherheitsüberprüfungsgesetz vom 20. April 1994) derzeit nicht. Dieses Regelungsdefizit muß beseitigt werden, weil - abgesehen von der Einwilligung der Betroffenen - wesentliche Verfahrenselemente der Gesetzgeber festzulegen hat.Das Landesamt für Verfassungsschutz speichert in der bundesweiten Verbunddatei (NADIS) alle Personen, die nach der Sicherheitsüberprüfungsrichtlinie ermächtigt werden sollen. Schon seit Jahren melden die Ressorts die Veränderungen nicht mehr in dem gebotenen Umfang. Derzeit sind beim LfV 1.700 Personen erfaßt. Ich habe daher in den Ressorts parallele Untersuchungen durchgeführt. Nicht einmal auf ausdrückliche Anfragen des LfV haben die Ressorts in dem notwendigen Umfang reagiert.Die Grundsätze der Erforderlichkeit werden in einem nicht länger hinnehmbaren Umfang vernachlässigt. Immerhin werden die Identifikatoren der Betroffenen im bundesweiten Zugriff der Verfassungsschutzämter und sensible Informationen in den Sicherheitsüberprüfungs-

akten über Personen vorgehalten, die mangels Aktualisierung zur Wahrnehmung der Sicherheitsbelange nicht mehr benötigt werden. Der gespeicherte Personenkreis und die vorhandenen Sicherheitsakten müssen unter Berücksichtigung folgender Gesichtspunkte in einem ganz erheblichen Umfang reduziert werden:- tatsächlich erfolgte Ermächtigung;- Wegfall der Beschäftigung im sicherheitsempfindlichen Bereich;- Ausscheiden des Bediensteten aus dem Dienst.Hierbei müssen die Ressorts die notwendigen Informationen unverzüglich an das LfV geben. Obwohl das LfV bei den Sicherheitsüberprüfungen grundsätzlich nur Mitwirkungspflichten hat, trägt es für den Umfang seiner Speicherung eine Mitverantwortung, weil die Datenbestände auch in anderen verfassungsrechtlich relevanten Zusammenhängen, wenn auch nur in sehr eingeschränktem Umfang, genutzt werden können (§ 7 Abs. 2 Satz 2 SVerfSchG). Dieser Mitwirkungspflicht kann das LfV durch Speicherung des Erkenntnisdatums und einer Wiedervorlagefrist Rechnung tragen. Diese Daten sind zur Steuerung von Prüfungs- und Spätestlöschungsfristen erforderlich. Die Beteiligung des LfV an der personenbezogenen Sicherheitsüberprüfung ist nur zulässig, soweit die hiervon betroffenen Personen eingewilligt haben; dies gilt nicht nur für Ehegatten, Verlobte und Lebenspartner, sondern auch für den betroffenen Bediensteten selbst (§ 4 Satz 2 und 3 SVerfSchG). Diesen gesetzlichen Anforderungen genügt das bisher praktizierte Verfahren nicht.Das bisher verwendete Formular einer "Erklärung des Bediensteten" enthält weder eine Aufklärung über die Mitwirkungspflichten des Bediensteten (§ 7 Abs. 4

SVerfSchG) noch eine Einwilligung in die Mitwirkung des LfV im Rahmen der Sicherheitsüberprüfung. Eine genaue Beachtung der Formvorschriften des § 4 SDSG ist unerläßlich. In der Ausfüllung des Formulars allein kann jedenfalls keine verbindliche Einwilligung des Bediensten gesehen werden, die den Erfordernissen der Form und Transparenz genügt.Auch hinsichtlich der mitbetroffenen Ehegatten, Verlobten und Lebenspartner ist bisher die notwendige Einwilligung nicht in dem gebotenen Umfang eingeholt worden. Es genügt nicht den Anforderungen, wenn der Partner lediglich bei Sicherheitsermittlungen (Richtlinie vom 17.09.1986 Tz. 5.2) einwilligt. Vielmehr bedarf nach dem Wortlaut des Gesetzes die Einbeziehung in die Überprüfung durch das LfV schlechthin der Einwilligung des Betroffenen. Deshalb ist die Einwilligung der Mitbetroffenen auch bei der Sicherheitsüberprüfung der untersten Stufe, der sogenannten Karteiabfrage, notwendig. Eine verbindliche Einwilligung setzt voraus, daß Kenntnis über den Umfang der Informationsverarbeitung vermittelt wird. Die Erklärung des Bediensteten enthält Angaben über den Ehegatten, die den normalen Umfang der Kenntnisse des Dienstherrn und Arbeitgeber über den Partner des Bediensteten übersteigt (z.B. frühere Wohnanschriften). Auch insoweit sollte dafür gesorgt werden, daß der Partner Kenntnis von dem Umfang der über ihn erhobenen Daten erhält.Das zuständige Innenministerium muß dafür sorgen, daß
das Verfahren geändert, die geeigneten Formulare entwickelt werden und die notwendigen Erklärungen nachgereicht werden.

5.2.2 Durchführung in den RessortsIm Berichtszeitraum habe ich im Innenministerium, im
Ministerium für Wirtschaft, im Ministerium für Umwelt und im Ministerium für Frauen, Arbeit, Gesundheit und Soziales die Datenverarbeitung im Zusammenhang mit der Sicherheitsüberprüfung kontrolliert. Dabei mußte ich im wesentlichen folgende Mängel feststellen:- Für die Durchführung der Sicherheitsüberprüfung ist
ein Geheimschutzbeauftragter zu bestellen. Nach den Sicherheitsrichtlinien sind Geheimschutz und Personalverwaltung streng zu trennen. Es wurde festgestellt, daß dieses Trennungsgebot im Ministerium für Frauen, Arbeit, Gesundheit und Soziales nicht eingehalten wurde. Die Durchführung der Sicherheitsrichtlinien war dem Referat für Personalangelegenheiten zugewiesen. Die Funktionstrennung ist inzwischen hergestellt.- Ein Problem, das in allen überprüften Ministerien zu
bereinigen ist, ist die Aufbewahrungsdauer der Sicherheitsakten. Im Regelfall werden die Sicherheitsakten auch weiter vorgehalten, obwohl die Bediensteten die sicherheitsempfindliche Tätigkeit nicht mehr wahrnehmen, sei es wegen Ausscheidens aus dem Dienst oder Übertragung einer nichtsicherheitsempfindlichen Tätigkeit. Es gilt jedoch der Grundsatz, daß personenbezogene Daten zu löschen sind, wenn ihre Kenntnis für die speichernde Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist (§ 19 Abs. 3 SDSG). Wenn die Betroffenen im sicherheitsempfindlichen Bereich nicht mehr tätig sind, besteht nach angemessener Frist keine Notwendigkeit mehr, die Akten weiter aufzubewahren. Ich habe daher gefordert, übergangsweise bis zur
Verabschiedung der anstehenden, gesetzlichen Rege-

lung in die Sicherheitsrichtlinien eine Bestimmung über die Länge der Aufbewahrungsfristen für die Sicherheitsakten aufzunehmen. Ich habe vorgeschlagen, die Regelungen über die Aufbewahrung und Vernichtung der Unterlagen des Sicherheitsüberprüfungsgesetzes des Bundes zugrundezulegen. Danach sind die Unterlagen über die Sicherheitsüberprüfung bei der zuständigen Stelle spätestens fünf Jahre nach dem Ausscheiden aus der sicherheitsempfindlichen Tätigkeit zu vernichten, es sei denn, der Betroffene willigt in weitere Aufbewahrung ein oder es ist beabsichtigt, dem Betroffenen in absehbarer Zeit erneut eine sicherheitsempfindliche Tätigkeit zuzuweisen.- In einigen Sicherheitsakten der Ressorts fanden sich ausführliche Berichte des Landesamtes für Verfassungsschutz über das Ergebnis der Sicherheitsermittlungen. In den Stellungnahmen waren Angaben zu Charakter, Ehe, materielle Situation, Betätigung in der Öffentlichkeit und Vereinen, elterlicher Familie, Einstellung zu Staat und Verfassung enthalten. In einem Bericht lautete ein Hinweis wie folgt: "Ehe wird als harmonisch bezeichnet", "Hinweise auf abnorme Veranlagung zu Sucht- und Rauschmitteln haben sich bislang nicht ergeben", "es wird ihm nachgesagt, daß er jeglichen Extremismus auf politischer Ebene grundsätzlich ablehnt", "sie war immer gut gekleidet". Ich habe die Entfernung dieser Berichte aus den Akten verlangt. Ich kann nicht ausschließen, daß in den Berichten auch sensiblere Informationen negativer Art enthalten sein können, die kein Sicherheitsrisiko darstellen und deshalb auch nicht mitzuteilen sind. Wenn das Ergebnis der Überprüfung keine Sicherheitsrisiken erkennen läßt, hat das Landesamt für Verfassungsschutz an die Geheimschutzbeauftragten lediglich eine kurze Mitteilung des Überprüfungsergebnisses zu übersenden.

In einem Fall hatte das Landesamt für Verfassungsschutz der zuständigen Behörde Vorstrafen eines Bediensteten mitgeteilt, ohne diese im Hinblick auf ein Sicherheitsrisiko zu bewerten. Der betreffende Bedienstete wurde dessenungeachtet zum Umgang mit Verschlußsachen ermächtigt. Diese Verfahrensweise ist unbefriedigend. Teilt das Landesamt für Verfassungsschutz einzelne Tatsachen aus der Überprüfung auch dann mit, wenn sie kein Sicherheitsrisiko begründen, dann muß eine eindeutige Bewertung hinzugefügt werden. Ich bevorzuge indessen ein Berichtsverfahren, das sich auf die Mitteilung von Tatsachen beschränkt, die ein Sicherheitsrisiko eindeutig begründen.- Je nach Lage des Falles begnügt sich das Landesamt für Verfassungsschutz mit einer Karteiüberprüfung oder es werden Sicherheitsermittlungen durch Befragung von Personen, die den Bediensteten kennen (Auskunftspersonen), durchgeführt. Auf dem Vordruck, den der Bedienstete zu Beginn der Sicherheitsüberprüfung ausfüllen muß, sind auch die Namen von Auskunftspersonen anzugeben. Es wurde festgestellt, daß die Erklärungen der Bediensteten, bei denen lediglich eine Karteiüberprüfung vorgenommen wurde, fast immer auch die Angaben zu Auskunftspersonen enthielten, obwohl die Beantwortung dieser Frage bei dieser Überprüfungsart nicht erforderlich ist. Ich habe für die Karteiüberprüfung die Entwicklung eines speziellen Erklärungsbogens gefordert, in dem die Frage nach Auskunftspersonen nicht mehr enthalten ist.Die einzelnen Ministerien und das für den Geheimschutz zuständige Innenministerium haben zugesagt, meinen Beanstandungen abzuhelfen.

5.2.3 Beschränkung der Kontrollen des Landesbeauftragten für DatenschutzLeider konnte der Landesbeauftragte für Datenschutz nicht in jeder Hinsicht seinen Kontrollaufgaben nachkommen. Die Prüfung beim Landesamt für Verfassungsschutz mußte unterbrochen werden, weil die Einsichtnahme in die dortigen Sicherheitsüberprüfungsakten nicht gewährt wurde. Nach Erörterung der Rechtslage mit der Aufsichtsbehörde wurde dem Landesbeauftragten lediglich persönlich die Einsichtnahme gestattet. Bei einer derartigen Beschränkung war - angesichts des großen Umfangs des Datenbestandes - eine systematische Prüfung nicht möglich, bei der auch Erkenntnisse aus den parallel durchgeführten Kontrollen in den Sicherheitsüberprüfungsakten in den Ressorts hätten verwertet werden können. Dessen ungeachtet ist die Beschränkung des Kontrollvorgangs mit dem gesetzlichen Prüfauftrag des LfD nicht vereinbar. Nach § 26 Abs. 1 SDSG ist das Kontrollrecht des unabhängigen Datenschutzbeauftragten umfassend. Lediglich im Einzelfall kann eine Beschränkung des Einsichtsrechts auf die Person des LfD in Betracht kommen, wenn die Sicherheit des Bundes oder eines Landes dies gebietet (§ 26 Abs. 2 Satz 1 SDSG). Eine derartige Gefahr ist jedoch nicht zu erkennen. Der Gesetzgeber hat eindeutig geregelt, daß die Akten über die Sicherheitsüberprüfung der Kontrolle durch den LfD unterliegen (§ 24 Abs. 2 Satz 4 Nr. 2, Abs. 6 BDSG). Lediglich wenn der Betroffene von seinem Widerspruchsrecht Gebrauch macht, ist die Einsichtnahme nicht zuzulassen. So gesehen hat der Gesetzgeber Beschränkungen allenfalls im Interesse der schutzwürdigen Belange der Betroffenen, jedoch nicht mit Rücksicht auf Sicherheitsbedenken für notwendig gehalten. Das uneingeschränkte Kontrollrecht des Landesbeauftragten für Datenschutz nach dem Saarländischen Datenschutzgesetz (§ 26 Abs. 1) muß unbeschadet

des Widerspruchsrechts des Betroffenen gewährleistet bleiben.In diesem Zusammenhang wurde auch die unzutreffende Behauptung aufgestellt, es sei eine systematische Überprüfung der Sicherheitsakten unter der Voraussetzung angeboten worden, daß die Namen der Referenz- oder Auskunftspersonen geschwärzt würden. Abgesehen davon, daß dieses Verfahren angesichts der großen Zahl der Betroffenen nicht praktikabel gewesen wäre, hätte diese Vorgehensweise nicht im Einklang mit dem Gesetz gestanden.Eine Querschnittsprüfung war wegen der großen Zahl der Betroffenen und mit Rücksicht auf die Tatsache geboten, daß eine gleichzeitige Kontrolle der Sicherheitsüberprüfungsakten in den Ressorts durchgeführt wurde. Die Überprüfungen in den verschiedenen Bereichen konnten nur dann zu einem brauchbaren Ergebnis führen, wenn auch die Unterlagen des LfV einer Stichprobenprüfung in angemessenem Umfang unterzogen worden wären. Dies war aber nur unter Beteiligung aller Mitarbeiter/Innen meiner Dienststelle sinnvoll möglich.5.2.4 ZweckbindungDie amtsinterne Zweckbindung ist jedenfalls für die Bereiche Sicherheitsüberprüfung und Überwachungsmaßnahmen nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses gesetzlich festgeschrieben (§ 7 Abs. 2 Satz 2 SVerfSchG i.V.m. § 7 Abs. 3 G 10). Danach dürfen Erkenntnisse aus den genannten Bereichen nur in eng begrenzten Ausnahmefällen in anderen verfassungsschutzrechtlich relevanten Zusammenhängen genutzt werden. Diese enge Zweckbindung ist nicht gewährleistet, da zwei Bedienstete des LfV gleichzeitig im Bereich Sicherheitsüberprüfung und im Bereich "G 10" und ein Bediensteter gleichzeitig im Bereich Sicher-

heitsüberprüfung und Spionage tätig sind. Eine strenge organisatorische und personelle Abschottung der genannten Bereiche ist unerläßlich. Hierfür sind die geeigneten personellen und organisatorischen Maßnahmen zu treffen.5.3 Beteiligung des Landesamtes für Verfassungsschutz beim Erwerb der deutschen StaatsangehörigkeitAus Anlaß einer Umfrage des Bundesbeauftragten für Datenschutz zur Beteiligung der Landesverfassungsschutzämter im Einbürgerungsverfahren hat mir das Ministerium des Innern die erfreuliche Tatsache mitgeteilt, daß bereits im Jahre 1990 auf eine Regelanfrage zur Verfassungstreue des Einbürgerungsbewerbers verzichtet worden sei. Das LfV werde nur im Einzelfall beteiligt, wenn Hinweise auf eine politisch-extremistische Betätigung des Einbürgerungsbewerbers vorlägen.Ich begrüße diese Änderung der Verfahrensweise im Einbürgerungsverfahren um so mehr, als mir durch die Umfrageergebnisse anderer Bundesländer bekannt wurde, daß die nicht datenschutzgerechte Regelanfrage im Einbürgerungsverfahren in einigen Bundesländern beibehalten wurde. 5.4 Trennung von Polizei und Nachrichtendiensten; VerbrechensbekämpfungsgesetzDie Gesetzgebungsorgane des Bundes haben nach langwierigen Beratungen unter Einschaltung des Vermittlungsausschusses das Verbrechensbekämpfungsgesetz verabschiedet. In seinem Art. 13 sieht dieses Gesetz die Fernmeldeaufklärung durch den Bundesnachrichtendienst zur Verhinderung, Aufklärung oder Verfolgung von Straftaten vor.

Aufgrund der technischen Gegebenheiten ist in die Fernmeldeaufklärung eine große Zahl Unbeteiligter einbezogen. Da dem Bundesnachrichtendienst Befugnisse übertragen werden, die auf eine gezielte Erhebung von Daten für polizeiliche Zwecke hinauslaufen können, wird die herkömmliche und bewährte Trennung zwischen Polizei und Nachrichtendiensten unterlaufen. Die Konferenz der Datenschutzbeauftragten hat am 26./27.09.1994 hierzu eine Entschließung gefaßt (Anlage 6). Es ist insbesondere fraglich, ob es noch gelingt, gerade die Unbeteiligten und Unverdächtigen vor unverhältnismäßigen Belastungen zu schützen.

6. Wahlen6.1 Repräsentative Wahlstatistik und das WahlgeheimnisDie Wahlgesetze des Bundes und der Länder sehen im Zusammenhang mit Bundes- und Landtagswahlen eine repräsentative Wahlstatistik auf der Grundlage von Wahlunterlagen aus bestimmten Wahlbezirken vor. Differenziert nach Altersgruppen und Geschlecht wird die Wahlbeteiligung und das Wahlverhalten nach statistischen Grundsätzen untersucht (vgl. die Ergebnisse der repräsentativen Landtagswahlstatistik 1994, Pressedienst des Statistischen Landesamtes des Saarlandes vom 5.12.1994).Der Bundestag hat die Aussetzung der repräsentativen Wahlstatistik für die Bundestagswahl 1994 beschlossen. Auch das Bundesland Brandenburg hat auf die Erstellung der Statistik für die Landtagswahl 1994 ohne förmliche Aufhebung der einschlägigen Bestimmungen des Landeswahlgesetzes verzichtet. Im Saarland wurde die Landtagswahlstatistik 1994 erstellt, während die Bundeswahlstatistik - wie vom Bundestag beschlossen - unterblieben ist. Die unterschiedliche Verfahrensweise hat mich veranlaßt, den Vorgang zu untersuchen. Insbesondere war zu prüfen, ob das Wahlgeheimnis voll gewahrt bleibt.Wahlunterlagen, nämlich die Wählerverzeichnisse und die Stimmzettel bestimmter Wahlbezirke übersenden die Gemeindewahlleiter dem Statistischen Amt, das die statistische Erhebung im einzelnen durchführt.Statistische Erkenntnisse über die Wahlbeteiligung werden allein auf der Grundlage der Wählerverzeichnisse mit Hilfe einer Strichliste festgestellt. Das Wahlverhalten wird auf der Basis der Stimmzettel ausgezählt. Zur Plausibilität wird das Wahlverhaltensergeb-

nis mit der Anzahl der Urnenwähler abgeglichen, die ebenfalls auf der Grundlage des Wählerverzeichnisses festgestellt wird.Ich habe die Zählergebnisse aller 58 Stichproben-Wahl-
bezirke des Saarlandes auf der Grundlage der Strichlisten überprüft. Hinsichtlich des Wahlverhaltens habe ich festgestellt, daß in vier ausgezählten Altersgruppen mit der geringsten Wahlbeteiligung nur zwei Parteien gewählt wurden und in allen vier Altersgruppen nur jeweils ein Wähler eine andere Partei gewählt hat. Ich darf ausdrücklich festhalten, daß insoweit das Wahlgeheimnis voll gewahrt blieb. Hätten jedoch alle Wähler einer Altersgruppe nur eine Partei gewählt, wäre im Zusammenhang mit dem Wählerverzeichnis, das die Wahlberechtigten namentlich mit Adresse aufführt, ohne weiteres feststellbar gewesen, welche Partei der einzelne Bürger gewählt hat. Unsicherheitsfaktoren, die die Anzahl der Personen in den einzelnen Altersgruppen (geringste festgestellte Beteiligung zwischen 8 und 13 Wählern) reduzieren und damit die Gefahr einer Identifizierung des Wählers erhöhen können, sind die Briefwähler, die in der Statistik überhaupt nicht erfaßt werden, die Nichtwähler und die unterschiedliche Verteilung der Geschlechter in den Altersgruppen.Wegen der somit durchaus bestehenden Gefahren für das
Wahlgeheimnis im Zusammenhang mit der statistischen Erhebung über das Wahlverhalten habe ich im Vorfeld der Wahl gegenüber dem Statistischen Landesamt angeregt, die Strichlisten auf der Grundlage des Wählerverzeichnisses und auf der Grundlage der Stimmzettel getrennt zu erstellen, um einer eventuellen Reidentifizierung auf der Grundlage der Wählerverzeichnisse vorzubeugen. Das Statistische Amt ist meiner Anregung gefolgt und hat für die getrennte Bearbeitung die Zuständigkeiten festgelegt und die Zugriffe Unbefugter untersagt. Auch die Landeshauptstadt hat für die zu-

sätzlichen, kommunalen Wahlbezirke, die in die repräsentative Wahlstatistik einbezogen waren, entsprechende Anordnungen getroffen.Diese Maßnahmen konnten allerdings keine vorbeugende
Wirkung im Hinblick auf die Feststellung der Wahlbeteiligung entfalten, die allein auf der Grundlage des Wählerverzeichnisses ausgezählt wird. Dieses Verzeichnis, das über die Tatsache, ob eine Person von ihrem Stimmrecht Gebrauch gemacht hat, Auskunft gibt, sei es als Urnenwähler, sei es als Briefwähler, fällt unter das Wahlgeheimnis (vgl. v. Münch, Grundgesetz-Kommentar, Art. 38 Rdnr. 53; Maunz-Dürig, Grundgesetz-Kommentar, Art. 38 Rdnr. 54). Auf der Stufe der Wahlvorbereitung sind Einschränkungen des Wahlgeheimnisses nach übereinstimmender Meinung zulässig, "soll die Wahl ordnungsgemäß ablaufen" (BVerfGE 12,35). Es bestehen deshalb keine Bedenken, daß das Wählerverzeichnis dem Wahlvorstand mit den genannten Hinweisen vorliegt. Die repräsentative Statistik ist indessen ein Vorgang, der mit der Durchführung der Wahl und ihrem ordnungsgemäßen Ablauf nicht im Zusammenhang steht. Daraus ist zu folgern, daß die Bekanntgabe der Teilnahme oder Nichtteilnahme an der Wahl gegenüber staatlichen Stellen verfassungswidrig ist, da selbst in der Unterlassung der Stimmabgabe eine politische Entscheidung liegen kann.Hinzu kommt noch, daß Zweifel bestehen, ob die derzeitigen gesetzlichen Regelungen eine hinreichend normenklare, gesetzliche Ermächtigung für die Durchführung der repräsentativen Wahlstatistik darstellen. Dies mag dazu beigetragen haben, daß der Bundestag die repräsentative Wahlstatistik für die Bundestagswahl 1994 ausgesetzt hat.

Meine Überprüfungen im Anschluß an die Wahlen haben ergeben, daß bereits für die Anlieferung der Wahlunterlagen durch die Gemeindewahlleiter keine ausreichenden technisch-organisatorischen Datensicherungsmaßnahmen ergriffen wurden. So erfolgte die Übersendung der Stimmzettel zwar in Briefumschlägen, jedoch waren diese häufig nicht versiegelt. Die noch sensibleren Wählerverzeichnisse waren größtenteils überhaupt nicht verschlossen. Transportbegleitscheine, die die Art und die Anzahl der übergebenen Wahlunterlagen dokumentieren, wurden nicht gefertigt, so daß eine Vollständigkeitskontrolle unmöglich war.6.2 Öffentliche Auslegung des Wählerverzeichnisses bei

Landes- und KommunalwahlenDie öffentliche Auslegung sowie der Umfang der auszulegenden Daten waren bereits Gegenstand mehrerer Tätigkeitsberichte (vgl. 1. TB Tz. 1.1, 6. TB Tz. 10.1, 10. TB Tz. 11.2). Nach wie vor ist aus datenschutzrechtlicher Sicht mit der Auslegung des Wählerverzeichnisses zu bemängeln, daß der Tag der Geburt offenbart wird. Lediglich auf Antrag des Betroffenen ist das Geburtsdatum unkenntlich zu machen. Dieses Datum ist nicht nur deshalb besonders schützenswert, weil es das genaue Alter einer Person offenbart, sondern weil es mit dem Namen die Identifizierung einer Person mit hoher Treffsicherheit erlaubt und damit den Aufbau von Datenbeständen und deren Nutzung - z.B. zur Bildung von Persönlichkeitsprofilen - erheblich erleichtert. Deshalb erscheint es datenschutzrechtlich geboten, auf das Geburtsdatum bei dem auszulegenden Wählerverzeichnis gänzlich zu verzichten. Ebenso ist zu fordern, daß die Daten der Wahlberechtigten, für die eine Auskunftssperre wegen Gefahr für Leib und Leben nach § 34 Abs. 5 Meldegesetz besteht,

bei Kommunalwahlen nicht in das auszulegende Wählerverzeichnis aufzunehmen sind. Diese Forderung ist bei der Landeswahlordnung bereits verwirklicht (§ 14 Abs. 3 Landeswahlordnung). Inzwischen hat Baden-Württemberg die Kommunalwahlordnung entsprechend geändert. An den Beschluß des Ausschusses für Datenschutz des Saarländischen Landtags vom 30. September 1988 (Anlage 9 zu meinem 10. TB) muß erinnert werden. Danach darf der Schutz von Bürgern, deren Meldedaten wegen Gefahren für Leib und Leben einer Auskunftssperre unterliegen, bei Wahlen nicht durch Eintragung in das öffentlich auszulegende Wählerverzeichnis in Frage gestellt werden.Der Hinweis des Ministeriums des Innern, die gleichzeitige Durchführung der Kommunal- und Europawahl würde eine Änderung der Kommunalwahlordnung nicht zulassen, verfängt nicht. Es ist Vorsorge dafür zu treffen, daß die schutzwürdigen Belange der Betroffenen wenigstens bei alleiniger Durchführung der Kommunalwahl berücksichtigt werden können. Nicht zuletzt werden mit Änderungen in den Kommunal-
wahlordnungen auch Signale für das zu ändernde Bundesrecht gesetzt.6.3 Geheimhaltung der Gründe für die Beantragung der

BriefwahlWer sich an einer Wahl per Brief beteiligen will, muß die hierfür erforderlichen Unterlagen beantragen. Ein Formular für diesen Antrag (Wahlscheinantrag) erhielt der Wähler für die Europa- und Kommunalwahl 1994 als Anhang zur Wahlbenachrichtigung. Der Inhalt dieses Antrages ist in der Europa- und Kommunalwahlordnung durch den Verordnungsgeber festgelegt. Beide Verordnungen enthalten unter anderem die Vorgabe, daß der Wahl-

scheinantrag so zu kennzeichnen ist, daß er nur in verschlossenem, frankiertem Umschlag zurückgesandt werden soll. Ein Gemeindewahlleiter hat dagegen den Antrag als Postkarte ausgestaltet. Ein Hinweis auf die verschlossene Zurücksendung fehlte. Auf der Postkarte sollten neben Identifizierungsdaten wie Geburtsdatum auch die Gründe, die zur Durchführung der Briefwahl berechtigen, angegeben werden: Verlegung der Wohnung, Krankheit, Alter, körperliche Gebrechen. Wenn der Wähler einen Wahlschein für die Briefwahl erhalten will, muß er die genannten Gründe vortragen. Der Gemeindewahlleiter betrachtet indessen den Hinweis auf die verschlossene Zurücksendung nicht als wesentlichen Bestandteil des durch Rechtsverordnung vorgegebenen Antrages, da dies nach seiner Auffassung eine unzumutbare Gängelung des mündigen Bürgers bedeutet hätte. Die Unterlassung der Unterrichtung verstößt gegen
ausdrückliche Vorschriften der Wahlordnung. Die betreffenden Wähler - dazu gehören vor allem gebrechliche alte Leute und Kranke, die sich in der Wahlzelle überfordert fühlen - werden dazu verleitet, Angaben zu ihrer Person offen mitzuteilen. Oft können sie nicht mehr selbst zur Post gehen und offenbaren sich auf diese Weise anderen gegenüber. Wegen der Förmlichkeiten, die bei einer Briefwahl zu
beachten sind, dürften sich die Wähler um eine Ungültigkeit ihrer Wahl nicht zu riskieren, genau an das halten, was von ihnen verlangt wird. Es ist deshalb davon auszugehen, daß die Wähler sensible Informationen über sich selbst offen weitergeben, statt durch Versendung in einem verschlossenen Umschlag sich des strafrechtlichen Schutzes des Briefgeheimnisses zu versichern.

Ich habe deshalb gefordert, daß bei künftigen Wahlen nicht nur der entsprechende Vermerk auf dem Antrag zur Erteilung eines Wahlscheines anzubringen ist, sondern daß der Antrag darüber hinaus auf keinen Fall als Postkarte ausgestaltet werden darf, da dadurch der Wille des Verordnungsgebers, das Verfahren datenschutzgerecht zu gestalten, unterlaufen würde.

7. Melderecht7.1 Novellierung des Melderechtsrahmengesetzes und des LandesmeldegesetzesNach langjährigen Erfahrungen mit den Regelungen des Melderechtsrahmengesetzes (MRRG) aus dem Jahre 1980 hat der Bundesgesetzgeber im Jahre 1994 das Erste Gesetz zur Änderung des Melderechtsrahmengesetzes verabschiedet. Die zwangsweise Erhebung der teilweise recht sensiblen Meldedaten, der sich kein Bürger entziehen kann, erfordert eine sorgfältige Abwägung der öffentlichen Interessen und der schutzwürdigen Belange der Betroffenen.Die Hotel- und Krankenhausmeldepflicht wurden schon sehr frühzeitig als verfassungsrechtlich bedenklich angesehen.- Im Rahmen der Zusammenarbeit zwischen den Schengen-- Staaten hat die Bundesrepublik Deutschland sich verpflichtet, die Hotelmeldepflicht in der Form sicherzustellen, daß beherbergte Ausländer Meldevordrucke ausfüllen und unterschreiben sowie sich gegenüber dem Leiter der Beherbergungsstätte oder seinem Beauftragten ausweisen. Wegen der zu befürchtenden praktischen Schwierigkeiten bei der Beschränkung der Hotelmeldepflicht auf Ausländer hat das MRRG die Hotelmeldepflicht auch weiterhin für alle beherbergten Personen festgeschrieben und für Ausländer um die Ausweispflicht erweitert. Die durch den Landesgesetzgeber umzusetzende Regelung stellt einen datenschutzrechtlichen Rückschritt dar.

- Die Krankenhausmeldepflicht ist zwar nicht entfallen, hat aber eine datenschutzfreundliche Modifizierung erfahren, so daß aus den in Krankenhäusern und ähnlichen Einrichtungen geführten Verzeichnissen Auskunft an die Meldebehörde oder die Polizei nur noch in Einzelfällen erteilt werden darf, wenn dies zur Abwehr einer erheblichen und gegenwärtigen Gefahr, zur Verfolgung von Straftaten oder zur Aufklärung des Schicksals von Vermißten und Unfallopfern erforderlich ist. Eine Einsichtnahme ist nicht mehr zulässig. Insofern ist ein datenschutzrechtlicher Fortschritt zu verzeichnen.Der mir vorgelegte Entwurf eines Gesetzes zur Änderung des Landesmeldegesetzes war in mehreren Punkten, in denen der Gesetzgeber noch einen Regelungsspielraum hat, nicht zufriedenstellend:- Die Übermittlung von Meldedaten von Kindern, die in einem Adoptionspflegeverhältnis stehen, an öffentlich-rechtliche Religionsgesellschaften sollte nicht zugelassen werden. Es muß den Pflegeeltern selbst überlassen bleiben, inwiefern sie Dritte informieren.- In Anlehnung an die Regelung im Ausländerzentralregistergesetz sind nicht nur Auskunftssperren gegenüber privaten Dritten sondern auch Übermittlungssperren im Einzelfall gegenüber anderen öffentlichen Stellen, insbesondere bei Gefahr für Leib und Leben eines Meldepflichtigen, vorzusehen. Bei solchen Gefahrenlagen müssen die Risiken so weit wie möglich gemindert werden.- Die Gruppenauskunft aus dem Melderegister an politische Parteien, Wählergruppen und andere Träger von Wahlvorschlägen im Zusammenhang mit Wahlen ist in Eingaben problematisiert worden. Die nach Lebensal-

tersgruppen zusammengefaßten Wahlberechtigten (z.B. Jungwähler) dürfen nach der bisherigen Regelung ohne Angabe des Geburtsdatums den genannten privaten Stellen in den sechs der Wahl vorangehenden Monaten zur Verfügung gestellt werden. Die Informationen über den Wähler dürfen jedoch nur für Wahlwerbezwecke verwendet und müssen deshalb spätestens nach dem Wahlgang vernichtet werden; eine Nutzung etwa zur Mitgliederwerbung ist nicht zulässig. Eine Kontrolle dieser Zweckbindung ist nur auf der Grundlage des Bundesdatenschutzgesetzes in sehr eingeschränktem Umfang zulässig, nämlich wenn hinreichende Anhaltspunkte dafür vorliegen, daß Rechtsvorschriften verletzt sind (§ 38 Abs. 1 BDSG). Ob eine Einhaltung insbesondere der Zweckbindung stets gewährleistet ist, kann man angesichts des weit gefaßten Kreises der Auskunftsberechtigten, die alle Träger von Wahlvorschlägen umfaßt, bezweifeln. Deshalb werden immer wieder Stimmen laut, die das Privileg in Frage stellen und darauf verweisen, daß eine Notwendigkeit angesichts der Möglichkeiten, die die modernen Medien für die Wahlwerbung zur Verfügung stellen, nicht mehr gegeben ist. Der Entwurf sieht jedoch vor, den Betroffenen die

Gelegenheit einzuräumen, der Übermittlung zu widersprechen. Ergänzend hierzu sollte jedoch eindeutiger als in dem geltenden Gesetz die Zweckbindung und damit die Voraussetzungen der Strafbewehrung (§ 38 MG) geregelt werden. Diese Vorkehrungen stellen jedoch aus datenschutzrechtlicher Sicht nur die zweitbeste Lösungsmöglichkeit dar. Die meisten Meldepflichtigen dürften von einer eventuellen Widerspruchsmöglichkeit schon deshalb keinen Gebrauch machen, weil sie von der Veröffentlichung des Hinweises auf dieses Recht wegen der Informationsüberflutung keine Kenntnis erhalten.

- Eine schon in früheren Jahren vorgetragene Forderung geht dahin, dem Bürger solle auf Verlangen nicht nur Auskunft über die gespeicherten Daten, sondern auch über die Stellen erteilt werden, an die regelmäßig Daten übermittelt werden. Transparenz ist eines der wichtigsten Prinzipien des Datenschutzes. Der betroffene Bürger soll stets wissen können, wer was wann über ihn weiß.- Der Vollzugspolizei ist der automatisierte Zugriff auf das Melderegister in beschränktem Umfang eingeräumt (§ 31 Abs. 5 MG). Der Gesetzgeber hat mehr als früher auch organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken (BVerfGE 65,1 ff, 44). Im Landesmeldegesetz ist deshalb vorzusehen, daß das Abrufverhalten der Polizei durch eine automatisierte Protokollierung überprüft werden kann. Ebenso sollte das Verwendungsverbot der Protokolldaten für andere als Kontrollzwecke gesetzlich abgesichert werden.Der Innenausschuß des Landtages des Saarlandes hatte bereits in seinen Beratungen zu meinem 7. Tätigkeitsbericht u. a. zur Rechtsmaterie des Melderechts einen Beschluß gefaßt (10. TB Anlage 9, Tz. 4).7.2 Regelmäßige Datenübermittlungen an die öffentlich--rechtlichen Rundfunkanstalten und die Gebühreneinzugszentrale (GEZ) zur Sicherstellung des Gebühreneinzugs

Die Regierungschefs der Länder haben sich mit der Thematik "Meldedatenübermittlungsverordnungen und Rundfunkgebühreneinzug" befaßt. Zum Zeitpunkt der Behandlung des Themas bestanden lediglich in Hessen und Nordrhein-Westfalen Regelungen, nach denen regel-

mäßig Daten aus dem Melderegister an die GEZ aus Anlaß der Anmeldung, Abmeldung und des Todes eines Einwohners übermittelt werden. Der zuständige Arbeitskreis II der Innenministerkonferenz hat einen entsprechenden Musterentwurf für eine Vorschrift der Meldedatenübermittlungsverordnungen der Länder erarbeitet. Der Entwurf sieht vor, daß künftig alle Meldebehörden im Falle einer Anmeldung, Abmeldung oder des Todes eines volljährigen Einwohners bis zu acht Kerndaten an die GEZ übermitteln dürfen.Hiergegen bestehen grundsätzliche Bedenken, die in einer Entschließung von Datenschutzbeauftragten des Bundes und der Länder zusammengefaßt wurden (Anlage 7).Der Entwurf wurde insbesondere deshalb abgelehnt, weil er zu einem bundesweiten Melderegister für Volljährige führen kann. Den Rundfunkanstalten stünde der unkontrollierte Zugriff auf Millionen personenbezogener Daten volljähriger Einwohner der Bundesrepublik zu, obwohl es für die Rundfunkanstalten nur von Interesse ist, welcher Einwohner bei ihnen gebührenpflichtig ist und bislang seine Gebührenpflicht nicht angemeldet hat. Das vorgesehene generelle Übermittlungsverfahren kennt keine Unterscheidung zwischen erforderlichen und nicht erforderlichen Daten, sondern überläßt diese Unterscheidung der GEZ. Über die Frage, ob ein Volljähriger überhaupt gebührenpflichtig ist, geben die Meldedaten keine Auskunft. Das muß nach wie vor im herkömmlichen Verfahren durch Befragung ermittelt werden. Der Entwurf verstößt gegen den Verfassungsgrundsatz der Verhältnismäßigkeit.Trotz grundsätzlicher Bedenken einiger Bundesländer hat die Innenministerkonferenz den vom Ausschuß erarbeiteten Vorschlag als Musterentwurf einer Meldedatenübermittlungsverordnung empfohlen.

Es ist nicht verständlich, daß der Beschluß der Innenministerkonferenz sich über den eindeutigen Wortlaut des § 4 Abs. 6 des Rundfunkgebührenstaatsvertrages hinwegsetzt, der eine Erhebung beim Betroffenen sowie tatsächliche Anhaltspunkte für das "Schwarzsehen und Schwarzhören" voraussetzt. Aus datenschutzrechtlicher Sicht dürfen solche bereichsspezifischen Regelungen durch die allgemeinen Bestimmungen des Melderechts nicht umgangen werden.7.3 Offenlegung privater Verhältnisse durch ein

Straßen- und HausnummernverzeichnisDurch eine Eingabe wurde ich auf die Herausgabe des nach Straßen und Hausnummern sortierten Adressenverzeichnisses einer Gemeinde, das im Amtlichen Bekanntmachungsblatt veröffentlicht wurde, aufmerksam gemacht. Neben den Namen und Anschriften der Einwohner waren weitere sensible personenbezogene Angaben ersichtlich. So hat die Gemeinde gekennzeichnet, ob die Einwohner einen Haupt- oder einen Nebenwohnsitz im Gemeindegebiet begründet haben. Des weiteren enthielt das Verzeichnis genaue Angabe über Baulücken sowie Häuser mit der Bezeichnung "unbewohnt", "Neubau", "Wochenendhaus" und "Rohbau". Ferner waren alle gewerblichen Betriebe der Gemeinde sowie Personen unter der Adresse eines Alten- und Pflegeheims und eines therapeutischen Kinder- und Jugendheims aufgeführt. Die Gemeinde hatte zuvor im Amtlichen Bekanntmachungsblatt darauf hingewiesen, daß sie Straßen, Hausnummern, Namen veröffentlichen werde und die Einwohner dem widersprechen können.Die Gemeinde hat sich zur Rechtfertigung der Veröffentlichung des Verzeichnisses auf § 35 Abs. 3 Saarländisches Meldegesetz (MG) berufen, wonach die Meldebehör-

de Auskunft über personenbezogene Daten an Adressbuchverlage erteilen darf.Ich habe darauf hingewiesen, daß nach der genannten Bestimmung lediglich Auskunft über Namen, akademische Grade und Anschriften sämtlicher Einwohner, die das 18. Lebensjahr vollendet haben, erteilt werden darf. Aus gutem Grund dürfen ausschließlich diese melderechtlichen Angaben veröffentlicht werden. Soweit die Merkmale aus anderen Quellen herrührten, beeinträchtigte ihre Bekanntgabe gleichfalls die schutzwürdigen Belange der Betroffenen, zumal die Gemeinde in ihrer Vorankündigung und mit ihrem Hinweis auf ein Widerspruchsrecht diese Angaben nicht erwähnt und damit die Bürger über den Umfang getäuscht hatte. Die Veröffentlichung folgender Angaben war unzulässig:- "Haupt- und Nebenwohnsitz" schon wegen der gesetzlich abschließenden Aufzählung des freigegebenen Datenkatalogs.- Die Angaben zu den Gewerbebetrieben ist nur zulässig, soweit die Gewerbetreibenden schriftlich in der Gewerbeanzeige zugestimmt haben.- Bei den unter der Adresse des Alten- und Pflegeheims angegebenen Personen lag der Schluß nahe, daß es sich hier um Untergebrachte handeln könnte. Bei den Personen unter der Adresse des Therapeutischen Kinder- und Jugendheims konnte es sich - wenn nicht ebenfalls um Untergebrachte - um dort Beschäftigte handeln, deren Beschäftigungsverhältnis nicht offenbart werden durfte.Die folgenden Angaben waren zwar nicht namensbezogen, dennoch verursacht die Herstellung ihrer Personenbeziehbarkeit durch Rückfragen keinen außergewöhnlichen

Aufwand, so daß die schutzwürdigen Belange beeinträchtigt sind:- "Wochenendhaus", "unbewohnt" wegen der geradezu provozierten Gefahr von Einbrüchen, ohne daß es auf die Personenbeziehbarkeit ankommt;- "Baulücke", "Neubau", "Rohbau" wegen der vom Eigentümer möglicherweise nicht beabsichtigten Einladung an Firmen und Makler, mit entsprechenden Angeboten vorstellig zu werden.Die Veröffentlichung, sortiert nach Straßen- und Hausnummern, stellt ebenfalls eine stärkere Beeinträchtigung der schutzwürdigen Belange der Betroffenen dar. Bei der Sortierung nach Straßen und Hausnummern ist leicht ersichtlich, wer allein ein Haus bewohnt, wer mit wem im gleichen Haus wohnt, ob in einem Haus lebende Personen verheiratet sind (Namensungleichheit), ob bei verheirateten Personen auch der Ehegatte für die Wohnung gemeldet ist. Des weiteren kann im Einzelfall bei einer Einrichtung festgestellt werden, wer bei dieser beschäftigt ist. Der Meldebehörde obliegt es der Beeinträchtigung schutzwürdiger Belange der Einwohner vorzubeugen (§ 7 MG). Stehen mehrere Möglichkeiten der Veröffentlichung zur Verfügung, so hat sie das schonendste Mittel im Interesse der Betroffenen zu wählen. Dies wäre ein rein alphabetisches Verzeichnis gewesen. Die Umsortierung nach Straßen und Hausnummern ist für ein Adressbuch nicht erforderlich und belastet die Betroffenen unverhältnismäßig. Die Veröffentlichung hat somit nicht den Anforderungen entsprochen.Die Gemeinde hat ihren Willen bekundet, die angesprochenen Datenschutzverstösse zukünftig vermeiden zu wollen.

7.4 Auskunft aus dem Melderegister7.4.1 Auskunft über gesperrte PersonendatenNach dem Melderecht hat der Meldepflichtige die Möglichkeit, das Vorliegen von Tatsachen glaubhaft zu machen, die die Annahme rechtfertigen, daß ihm oder einer anderen Person aus einer Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange erwachsen kann (§ 34 Abs. 5 MG). Im Melderegister wird sodann eine Auskunftssperre zum Schutze des Betroffenen eingetragen.Der Personenkreis der Betroffenen kann zum Beispiel umfassen: verdeckte Ermittler, nicht offen ermittelnde Polizeibeamte, Auskunftspersonen, Hinweisgeber aus bestimmten Gesellschaftskreisen. Geben die Meldebehörden die Auskunft, es sei eine Auskunftssperre eingerichtet, hat ein Petent die Befürchtung geäußert, liege die Schlußfolgerung nahe, der Betroffene wohne in der Gemeinde dieser Behörde. Damit seien Gefährdungen insbesondere in kleineren Gemeinden nicht auszuschließen, weil der Betroffene leicht ermittelt werden könne.Das zuständige Ministerium des Innern hat mitgeteilt, daß selbst bei der Auskunft, es sei eine Auskunftssperre eingerichtet, die Schlußfolgerung, der Betroffene wohne in dieser Gemeinde, nicht zwingend sei. Auch die Meldebehörden des vorherigen und weiteren Wohnsitzes sind zu unterrichten (§ 30 Abs. 3 MG), so daß auch die Nichtwohnsitzgemeinde zur Auskunftsverweigerung verpflichtet ist. Für den tatsächlichen Aufenthalt einer Person können
zwar im Einzelfall mehrere Gemeinden in Betracht kommen. Ob damit ein ausreichender Schutz der gefährdeten

Person in allen Fällen gegeben ist, halte ich für zweifelhaft.Da die meisten Betroffenen lediglich eine Wohnung haben dürften, habe ich empfohlen, Formulierungen zu wählen, die nicht auf eine Registrierung des Betroffenen bei der um Auskunft ersuchten Meldebehörde schließen lassen (gegebenenfalls "Fehlanzeige", "der Betroffene ist in der Gemeinde nicht gemeldet").Das Grundrecht auf Leben und körperliche Unversehrtheit (Art. 2 Abs. 2 Satz 1 GG) ergibt nicht nur einen Abwehranspruch des einzelnen gegen staatliche Maßnahmen, die sein Leben bedrohen, sondern zugleich eine objektive, rechtliche Verpflichtung aller staatlichen Gewalt, das Leben - auch gegen Gefährdungen von dritter Seite - zu schützen.7.4.2 Auskunft über EG-AusländerMeldebehörden haben mich darüber informiert, daß eine oberste Landesbehörde aus Anlaß der Europawahl alle Meldebehörden des Saarlandes um Mitteilung der Adressen von in der Gemeinde ansässigen EG-Ausländern gebeten hat. Als Verwendungszweck wurde angegeben, die bei uns lebenden ausländischen Mitbürger zu ermuntern, im Interesse einer hohen Wahlbeteilung von der erstmaligen Möglichkeit im Gastland mitzuwählen, Gebrauch zu machen.Dieses an sich wünschenswerte Ziel konnte jedoch die Melderegisterauskunft nicht rechtfertigen. Es war zunächst zu bezweifeln, ob die Erforderlichkeit der Melderegisterauskunft bejaht werden kann, weil die Unterrichtung der EG-Ausländer über ihr Wahlrecht auch durch allgemeine Veröffentlichungen in den Medien hätte erfolgen können und auch erfolgt ist.

Im Zusammenhang mit der Wahl dürfen Melderegisterauskünfte in beschränktem Umfang allenfalls Parteien und Wählergruppen gegeben werden (§ 35 MG). Aber auch insoweit ist die Selektion und Mitteilung der Staatsangehörigkeit und/oder EG-Staatsangehörigkeit aller EG-Ausländer nicht zugelassen. Meldedaten dürfen im übrigen nur, soweit sie zur rechtmäßigen Erfüllung der in die Zuständigkeit der datenempfangenden Behörde liegenden Aufgaben erforderlich sind, übermittelt werden (§ 31 MG). Unter den obersten Landesbehörden obliegt die Durchführung von Wahlen jedoch nur dem Landeswahlleiter im Ministerium des Innern. Eine konkrete durch Gesetz zugewiesene Zuständigkeit der datenanfordernden Stelle war nicht zu erkennen; eine allgemeine lediglich politische Aufgabenstellung einer öffentlichen Stelle ist für die Datenübermittlung nicht ausreichend. Lediglich den Parteien hat der Gesetzgeber für Zwecke der Wahlwerbung ein zeitlich und inhaltlich beschränktes Auskunftsrecht eingeräumt. Die Verwendung von Melderegisterdaten, die von jedem Bürger zwangsweise erhoben werden, darf nur in dem engen durch das Gesetz vorgegebenen Rahmen erfolgen.Ich habe die oberste Landesbehörde darum gebeten, die Meldebehörden zu verständigen und Melderegisterdaten, die bereits vorliegen, zu vernichten.7.4.3 Auskunft über GUS-BewohnerEine Meldebehörde hat angefragt, ob das Ersuchen eines Vereins um Übermittlung aller Namen und Adressen der in der Gemeinde wohnenden Aussiedler und ehemaligen GUS-Bewohner zulässig sei. Der an dem kulturellen Ziel der Integration des Personenkreises ausgerichtete

Verein beabsichtige, eine Einladung zu einer Kunstausstellung zu versenden.Ich habe darauf hingewiesen, daß zur Auskunftserteilung (Gruppenauskunft) nur die im Meldegesetz aufgezählten Daten, zu denen auch die Staatsangehörigkeit zählt, herangezogen werden dürfen (§ 34 Abs. 3 MG). Es war jedoch zweifelhaft, ob dieses Kriterium die Möglichkeit eröffnet, eine Aussage darüber zu treffen, welche Personen zu dem Kreis der rußlanddeutschen Aussiedler gehörten. Die Staatsangehörigkeit läßt jedenfalls nicht auf Herkunft und Volkszugehörigkeit schließen.Da zudem die gesetzliche Voraussetzung des "öffentlichen Interesses" an der Gruppenauskunft zweifelhaft erschien und auch der Schluß nahe lag, ehemalige GUS--Bewohner könnten durch eine Übermittlung gefährdet werden, habe ich der Meldebehörde empfohlen, Adressierung und Versendung der von dem Verein gelieferten Schreiben gegen Erstattung des Kostenaufwandes in Erwägung zu ziehen. Auf diese Weise kann eine Datenübermittlung an eine private Stelle unterbleiben und den schutzwürdigen Belangen der Betroffenen sowie nicht auszuschließende Eigeninteressen an der Teilnahme zu dieser Veranstaltung Rechnung getragen werden.

8. Änderungsgesetz zur Abgabenordnung 1994Das Bundesministerium der Finanzen hat vielversprechende Referentenentwürfe zur Novellierung der Abgabenordnung (AO) mit besonderem Schwerpunkt bei den datenschutzrechtlich relevanten Bestimmungen erarbeitet. Im Mittelpunkt stand die Neufassung der Bestimmung über das Steuergeheimnis (§ 30 AO), die die neuere Datenschutzgesetzgebung und die Rechtsprechung des Bundesverfassungsgerichts sowie des Bundesfinanzhofes zum informationellen Selbstbestimmungsrecht umsetzen sollte. Trotz langjähriger Beratung dieses Entwurfes bereichsspezifischer Datenschutzbestimmungen wurde dieses Regelungsvorhaben unverständlicherweise zurückgestellt.Der Bedarf an konkretisierenden, datenschutzrechtlichen Regelungen in der AO ist auch nicht annähernd vollständig durch das Gesetz zur Bekämpfung des Mißbrauchs und zur Bereinigung des Steuerrechts (Mißbrauchsbekämpfungs- und Steuerbereinigungsgesetz - StMBG) gedeckt worden. Vor allem ist durch die Bezugnahme dieses Gesetzes auf die zentrale Regelung der AO zum Steuergeheimnis (§ 30 AO), der datenschutzrechtlich ergänzungsbedürftig ist, der unbefriedigende Rechtszustand fortgeschrieben worden.So fehlt insbesondere eine ausreichend normenklare Rechtsgrundlage für die Speicherung personenbezogener Daten und ihre Übermittlung in eine bundesweite Fahndungsdatei.Bislang ist es auch nicht gelungen, die bereits in meinem 13. Tätigkeitsbericht (Lt-Drucksache 10/941, Tz. 4.1) dargestellten Defizite der AO abzubauen (z. B. mangelnde Berücksichtigung der traditionellen Berufs- und Amtsgeheimnisse - wie das Arztgeheimnis - bei der Verpflichtung öffentlicher Stellen zur Aus-

kunfts- und Vorlagepflicht gegenüber den Finanzbehörden sowie zur Anzeige von Steuerstraftaten - § 105 und § 116 AO -).

9. Sparkassen9.1 Datenschutzklausel der BausparkasseIn den letzten Jahren wurden von den Banken und Versicherungsgesellschaften bundesweit sogenannte Allfinanz-Konzepte entwickelt. Auch im Saarland haben sich die Sparkassen, die Landesbausparkasse (LBS), die Saarländische Landesbank Girozentrale sowie die Saarland Versicherungen AG zu einem Verbund (S-Finanzgruppe) zusammengeschlossen. Ihr Ziel ist die umfassende Beratung in Bauspar-, Geld-, Finanzierungs- und Versicherungsangelegenheiten.Ein vollständiger Verbund ist jedoch nicht verwirklicht. Die Sparkassen und die Landesbausparkasse (evtl. später auch die anderen Verbundmitglieder) kooperieren in der Weise, daß die ersteren die Sparverträge lediglich vermitteln; alleiniger Vertragspartner ist die Landesbausparkasse.Für die Beratung und Vermittlung durch die Sparkasse wurde mit meiner Unterstützung eine Einwilligungserklärung (Datenschutzklausel) entwickelt. In Verbindung mit einem Merkblatt "Erläuterungen zur Datenschutzklausel" wird der LBS-Kunde über den Informationsaustausch der Verbundpartner aufgeklärt.Den Sparkassen werden bei der Beratung und Vermittlung Informationen aus dem Bausparvertrag bekannt, die sie sonst nicht erhalten hätten. Es war also dafür Sorge zu tragen, daß die Zweckbindung dieser Informationen grundsätzlich sichergestellt ist und ihrer Verwendung für Werbezwecke durch die Sparkassen für eigene oder Produkte der anderen Verbundteilnehmer nur mit ausdrücklicher Einwilligung des Sparers erfolgt (etwa das Angebot von Darlehen bei Fälligkeit des Bausparvertrages zur Verbesserung der Liquidität oder von Ver-

sicherungen zur Minderung des Risikos einer Darlehensaufnahme).Die Einwilligung für die Vermittlung und Beratung einerseits sowie für die Werbung mit eigenen oder Verbundprodukten andererseits wird getrennt abgefragt. Der LBS-Kunde ist somit der Werbung nicht völlig ausgeliefert; die Entscheidungsfreiheit des Verbrauchers ist gewährleistet.Schließlich mußte die Zweckbindung auch im Hinblick
auf den zentralen, zur Abwicklung der Bausparverträge bei der Landesbausparkasse gespeicherten Datenbestand gesichert werden. Durch angemessene technisch-organisatorische Maßnahmen ist gewährleistet, daß der automatisierte Direktzugriff der Sparkassen nur auf Verlangen des Betroffenen erfolgt. Für die Abfrage der Bauspardaten muß die vollständige Bausparnummer einschließlich einer Prüfziffer eingegeben werden. Dadurch wird die Selektion von Bauspardaten durch die Eingabe des Namens praktisch ausgeschlossen. Zugriffsberechtigt sind im übrigen nur bestimmte Mitarbeiter der Sparkassen; Benutzerkennung und persönliches Paßwort sind selbstverständlich verbindlich vorgegeben; die Zugriffe werden aufgrund von Protokollen wenigstens stichprobenweise überprüft.Der Bausparer wird im übrigen schon bei Vertragsab-
schluß darüber unterrichtet, daß ein bestimmter Datensatz aus einem Anlaß, der eine sachkundige Beratung erfordert, der vermittelnden Bank in konventionellem Wege mitgeteilt wird (z. B. bei Zuteilungsreife des Bausparvertrages).

9.2 Beschränkung des bankinternen Zugriffs auf Kontoinformationen

Im Berichtszeitraum ist der Wunsch von Sparkassenkunden laut geworden, nur von ihrer kontoführenden Sparkassenfiliale betreut zu werden, so daß andere am Informationssystem angeschlossene Filialen keinen Zugriff auf ihre Konten und Depots haben. Mit diesem Anliegen habe ich mich an den Sparkassen- und Giroverband Saar gewandt mit der Bitte um Überprüfung, inwieweit der Zugriff auf Kontoinformationen im Interesse des Kunden beschränkt werden kann. Der Sparkassen- und Giroverband hat mir mitgeteilt, daß betriebsstellenbezogene Beschränkungen EDV-technische Aufwendungen erfordern würden, die nicht mehr in angemessenem Verhältnis zu dem angestrebten Schutzzweck stünden. Zudem legten die Kunden Wert darauf, nicht nur die Dienstleistungen bei einer bestimmten sondern bei jeder Zweigstelle in Anspruch nehmen zu können. Zur Sicherung der Zugriffsbeschränkung kämen sogenannte Kontrollschlüssel zur Anwendung, die bewirkten, daß die Abfrage oder Eingabe nicht durch einen Mitarbeiter allein vorgenommen werden könne, sondern ein zweiter Mitarbeiter herangezogen werden müsse (Vier-Augen-Prinzip). Die Diskussion über die Gestaltung des Vertragsverhältnisses unter Berücksichtigung des Willens des Kunden nach Beschränkung seiner Daten auf eine Bankfiliale dauert derzeit noch an. Die Prüfung der Argumente des Sparkassen- und Giroverbandes setzt vor allem auch eine Untersuchung darüber voraus, in welchem Umfang EDV-technische Aufwendungen für diese Vertragsgestaltung aufzubringen wären. Verbraucherfreundlich wären jedenfalls Vorkehrungen, die sicherstellen, daß der

Zugriff auf Kontoinformationen innerhalb der Sparkassenorganisationen nur in dem vom Kunden gewünschten Umfang möglich ist.

10. EG-StatistikverordnungDer erste Entwurf der EG-Statistikverordnung datiert bereits aus dem Jahre 1989. Er war ein Beispiel dafür, wie der Standard des Datenschutzes in der Bundesrepublik Deutschland durch unmittelbare Maßnahmen der EG-Kommission unterschritten werden kann (vgl. meinen 11. TB Seite 12).Im Rahmen des sogenannten EUROFARM-Projektes, das der Durchführung von Erhebungen der Gemeinschaft über die Struktur der landwirtschaftlichen Betriebe im Zeitraum 1988 bis 1997 dient, hat die deutsche Sonderregelung zunächst vorgesehen, Individualdaten beim Statistischen Bundesamt zu belassen, das bisher die notwendigen Tabellen aufbereitete und an das Europäische Statistische Amt - EUROSTAT - weiterleitete. Nunmehr sollen die Individualdaten unmittelbar an EUROSTAT weitergeleitet werden.Dieses Verfahren kann erst dann akzeptiert werden, wenn das Statistikrecht der Europäischen Union die notwendigen datenschutzrechtlichen Regelungen getroffen hat. Die EG-Statistikverordnung ist bislang immer noch nicht verabschiedet.Die Datenschutzbeauftragten des Bundes und der Länder haben sich daher erneut mit der Problematik in einer Entschließung vom 25.8.1994 befaßt (Anlage 8). Sie haben betont, daß als zuständige Gemeinschaftsdienststelle unmißverständlich das Statistische Amt der Europäischen Gemeinschaften benannt werden und einen den Statistischen Ämtern in der Bundesrepublik vergleichbaren organisationsrechtlich selbständigen Status erhalten muß. Hierin ist eine Grundvoraussetzung für die Zweckbindung der zu statistischen Zwecken erhobenen Daten sowie für die statistische Geheimhaltung zu sehen.

Der zentrale Begriff der "statistischen Geheimhaltung" selbst bedarf einer dem nationalen Recht entsprechenden neuen, präzisen Definition.Im Entwurf der Verordnung sind datenschutzgerechtere Verfahrensvorkehrungen festzulegen, die Zuständigkeiten zu klären und die Trennung und Aufbewahrung von Erhebungs- und Hilfsmerkmalen zu regeln.Grundlegende Entscheidungen über die den Bürger belastenden Datenerhebungen sollten dem Rat mit Zustimmung des Europäischen Parlaments vorbehalten bleiben.Nicht zuletzt fehlt es bis heute an einer unabhängigen und effektiven Datenschutzkontrollinstanz für die Organe der Europäischen Union.

11. Soziales

11.1 Föderales Konsolidierungsprogramm - Bekämpfung des Mißbrauchs von Sozialleistungen

Im Berichtszeitraum hat die Bundesregierung ein Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms (FKPG) vorgelegt. Ziel des Gesetzes soll die Konsolidierung der öffentlichen Haushalte, unter anderem durch Bekämpfung der mißbräuchlichen Inanspruchnahme von Sozialleistungen sein. In das Bundessozialhilfegesetz ist eine Regelung aufgenommen worden, die einen automatisierten Datenabgleich zwischen Sozialhilfeträgern sowie zwischen diesen und anderen Sozialleistungsträgern, nämlich mit der Bundesanstalt für Arbeit sowie den gesetzlichen Renten- und Unfallversicherungen, erlaubt. Einen konkreten Anhaltspunkt für einen unberechtigten Leistungsbezug setzt das Gesetz nicht voraus (§ 117 Abs. 1, Abs. 2 BSHG). Mit anderen öffentlichen Stellen als den genannten ist ein Datenabgleich nur nach dem Maßstab der Erforderlichkeit vorgesehen (§ 117 Abs. 3 BSHG).Soweit der Datenabgleich voraussetzungslos stattfinden darf, wird die Glaubwürdigkeit aller Sozialhilfeempfänger in Zweifel gezogen. Selbst wenn es zutreffen sollte, daß ein erheblicher Anteil der Sozialhilfeempfänger der schon jetzt bestehenden Verpflichtung nicht nachkommt, den Sozialhilfeträgern Leistungen der Bundesanstalt für Arbeit und das Eingehen von Beschäftigungsverhältnissen mitzuteilen, bestehen Zweifel an der Zwecktauglichkeit eines solchen Abgleichs. Jedenfalls Nebeneinkünfte von Sozialhilfeempfängern, für die keine Sozialabgaben entrichtet werden, sind den Trägern der Sozialversicherung nicht bekannt und können deshalb nicht einbezogen werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung vom 9./10. März 1994 ihrer Besorgnis über die Entwicklung Ausdruck verliehen, die zu einem dichteren Datenverbindungssystem im Sozialleistungsbereich und einem Abbau des Sozialdatenschutzes gerade der großen Mehrzahl der rechtstreuen Leistungsbezieher führt (Anlage 9). Kurz nach Inkrafttreten des Gesetzes wurde aus anderen Bundesländern die Absicht dortiger Sozialhilfeträger bekannt, ihre Datenbestände über Sozialhilfeempfänger mit den Datenbeständen der Kfz-Zulassungsstellen abzugleichen. Der automatisierte Datenabgleich sollte dazu dienen, Sozialhilfeempfängern auf die Spur zu kommen, die in ihrem Sozialhilfeantrag verschwiegen haben, daß sie Halter eines Kraftfahrzeuges sind.Ein solcher automatisierter Abgleich aller Sozialhilfeempfänger, ohne daß im konkreten Fall der Verdacht einer rechtswidrigen Inanspruchnahme von Sozialhilfe besteht, findet im Gesetz keine Stütze (§ 117 Abs. 3 BSHG). Das Ministerium für Frauen, Arbeit, Gesundheit und Soziales hat hierzu in einem Schreiben an die örtlichen Träger der Sozialhilfe auf unsere Veranlassung hin ausdrücklich klargestellt, daß eine Datenüberprüfung nur zulässig ist, wenn im Einzelfall der Verdacht einer rechtswidrigen Inanspruchnahme von Sozialhilfe besteht.11.2 Prüfung der Landesversicherungsanstalt für das

Saarland (LVA)Die LVA ist der Träger der gesetzlichen Rentenversicherung der Arbeiter im Saarland. Die Zahl der Versicherten beläuft sich auf etwa 220.000, die der Rentenempfänger auf etwa 124.000. Bei der LVA sind über 500 Mitarbeiter beschäftigt. Kernstück sind die Abteilun-

gen, die die Versicherungskonten zum Nachweis von Anwartschaften und Ansprüchen führen und Anträge auf Leistung der Renten sowie für die Maßnahmen der Rehabilitation bearbeiten. Diese Organisationseinheiten - Abteilungen für Versicherungen/Rente, Hüttenknappschaftliche Zusatzversicherung, Rehabilitation - werden unterstützt durch die Abteilungen für Verwaltung, Datenverarbeitung, Rechnungsprüfung und Recht sowie den Ärztlichen Dienst. Medizinische Befunde, Diagnosen und Therapien werden in großem Umfang gespeichert, weil sie für die Entscheidungen über Rentenansprüche im Falle der Berufs- oder Erwerbsunfähigkeit sowie bei Rehabilitationsmaßnahmen benötigt werden. Für die Abwicklung des Massengeschäfts ist die Automation besonders wichtig. Schwerwiegende Mängel mußten im Verfahrensablauf beim
Umgang mit medizinischen Daten festgestellt werden.Ein Rehabilitationsantrag, dem von Anfang an ein Bericht des behandelnden Arztes beigefügt ist, durchläuft von der Posteingangstelle bis zur Versendung des Bescheids immerhin zehn verschiedene Stellen der LVA. Auf diesem langen Weg wird der Antrag durch weitere sensible Unterlagen des Ärztlichen Dienstes der LVA und weitere Stellungnahmen externer ärztlicher Gutachter angereichert. Ähnlich verhält es sich auch im Rentenbereich bei Anträgen auf Gewährung einer Erwerbsunfähigkeits- oder Berufsunfähigkeitsrente. Der Verwaltungsakte wird ein besonderes Heft mit den ärztlichen Gutachten und sonstigen medizinischen Unterlagen beigefügt, das mit der Gesamtakte zu den verschiedenen Bearbeitungsstationen wandert. Damit haben viele Mitarbeiter einschließlich der Boten die Möglichkeit, in die unverschlossenen Arztunterlagen Einsicht zu nehmen.

Ein anderes Beispiel kann den unangemessenen Umgang mit den medizinischen Angaben veranschaulichen: Kureinrichtungen und Heilstätten, in denen Krankheiten aller Art, auch Drogen-, Alkohol- und Medikamentenabhängigkeit behandelt werden, berichten umfassend über Verlauf und Ergebnis einer Rehabilitationsmaßnahme (Zitat aus einer Anamnese: "Patient hatte mit 16 Jahren sexuellen Kontakt mit gleichaltriger Partnerin"). Die Rehabilitationsabteilung prüft, ob die Maßnahme wie bewilligt durchgeführt wurde und welche Maßnahmen der Nachsorge oder sogar die Rentengewährung veranlaßt ist. Nach eigener Bekundung der Bediensteten wird für diese Prüfung nicht der gesamte Inhalt des Entlassungsberichts benötigt; die Entscheidung gründet allein auf einigen Eckpunkten aus diesem Bericht. Der Entlassungsbericht wird in zweifacher Ausfertigung geliefert und in der Rehabilitationsabteilung sowie im Archiv der Rentenabteilung, in leicht zugänglicher Weise (Klarsichthülle) abgelegt.Den externen Gutachtern und Ärzten, von denen sonstige
Unterlagen angefordert werden, gibt die LVA den irreführenden Hinweis, daß die Sendungen an den Leiter des Ärztlichen Dienstes zu richten sind und erweckt damit den nicht zutreffenden Eindruck, daß sie die sensiblen Informationen in besondere Verwahrung nimmt. Der organisatorische Ablauf sollte in der Weise geändert werden, daß sämtliche ärztlichen Unterlagen verschlossen beim Ärztlichen Dienst eingehen und nur dort geöffnet werden. Dieser trägt die Verantwortung, in welchem Umfang medizinische Daten offen im internen Verwaltungsablauf in Akten vorgehalten werden. Umfangreiche Unterlagen und Berichte mit Anamnesen, Epikrisen und Einzelbefunden sollten in einem Umschlag verschlossen zu den Akten genommen werden. Der Aktenin-
halt im übrigen sollte auf Ergebnisse medizinischer Untersuchungen und zusammenfassende ärztliche Bewertun-

gen beschränkt sein. Der verschlossene Umschlag sollte nur von den dazu besonders befugten Bediensteten der Leistungsabteilungen im Bedarfsfall geöffnet werden dürfen. In einer Vielzahl von Fällen dürften die unverschlossen in den Akten vorhandenen medizinischen Feststellungen für die Entscheidungsfindung ausreichen.Durch technisch-organisatorische Maßnahmen, die der Ärztliche Dienst sicherzustellen hat, ist ein unbemerktes Auswechseln des Umschlags und unbefugtes Öffnen zu verhindern (z.B. Klebeetikette mit Namen und Versicherungsnummer des Betroffenen, Unterschrift). Den externen Ärzten sollten Rückumschläge mit dem Aufdruck "Arztsache" zur Verfügung gestellt werden, um bei der Rücksendung eine eindeutige Adressierung für den internen Ablauf innerhalb der LVA zu erreichen.Der Vorschlag soll dazu beitragen, daß im Interesse der Persönlichkeitsrechte der Betroffenen mit den medizinischen Informationen möglichst schonend umgegangen wird und ihre Verwendung von dazu befugten Bediensteten nach dem Maßstab der Erforderlichkeit gewährleistet ist. Ziel muß sein, den Intimbereich und das soziale Umfeld der Betroffenen gegen unangemessene Ausspähung zu schützen. Auch innerhalb des Leistungsträgers ist sicherzustellen, daß die Daten nur Befugten zugänglich sind (§ 35 Abs. 1 SGB I).Mängel mußten auch bei der automatisierten Datenverarbeitung festgestellt werden.Die Zugriffsrechte einschließlich der Befugnisse zur Änderung von Daten sind in der Spitze des hierarchisch gegliederten Verwaltungsaufbaus der LVA besonders zahlreich. Insoweit ist ein Bedarf nur in eingeschränktem Umfang erkennbar. Die elektronische Datenverarbeitung der LVA ist in traditioneller Großrechnerorganisation ausgelegt; sie ist daher lediglich ein unterstüt-

zendes Element für die aktenmäßige Verarbeitung von Vorgängen. Die Erfassung und Veränderung im Massengeschäft vollzieht sich nicht auf der Ebene der Führung (keine Kumulation der Zugriffsberechtigung entsprechend der Hierarchie). Eine Beschränkung wenigstens auf den lesenden Zugriff ist angezeigt. Referenten und Abschnittsleiter sollten nur in Ausnahmefällen erfaßte Daten ändern dürfen. Auch auf der Ebene der Massenabwicklung ist eine Beschränkung nach der jeweiligen, arbeitsteiligen Zuständigkeit notwendig. Jeder Sachbearbeiter sollte nur auf die Daten der Versicherten zugreifen können, die er zur Aufgabenwahrnehmung in seinem Zuständigkeitsbereich benötigt. Die Zuständigkeiten der Bediensteten in den Abteilungen für Renten und Rehabilitation sind nach den Geburtstagen der Versicherten festgelegt. Der automatisierte Zugriff auf die Daten der Versicherten ist jedoch allen Bediensteten innerhalb jeweils einer der genannten Abteilungen möglich.Die umfassende Zugriffsmöglichkeit in den Leistungsabteilungen ist für den Betroffenen gerade mit Rücksicht auf die medizinischen Angaben äußerst belastend. Der einheitliche Diagnoseschlüssel der Renten- und Krankenversicherung, der der automatisierten Speicherung zugrunde liegt, reicht von den infektiösen, parasitären Erkrankungen, den bösartigen Neubildungen bis hin zu den psychiatrischen Anomalien (sexuelle Verhaltensabweichungen und Störungen, Medikamenten-/Drogen-/Alkoholabhängigkeit). Die Diagnosen werden in dieser Form auch für die Statistik genutzt und personenbezogen dauerhaft gespeichert. Daten über eine Erkrankung dürfen in automatisierten Verfahren jedoch nur den Bediensteten zugänglich sein, die sie zur Erfüllung ihrer Aufgaben benötigen (§ 148 Abs. 2 SGB VI). Die Zugriffsmöglichkeiten sind entsprechend der Zuständigkeitsverteilung zu reduzieren. Statistikdaten

dürfen nach Feststellung der statistischen Ergebnisse nicht mehr personenbeziehbar und auf längere Zeit gespeichert bleiben. Ist die Statistik erstellt, sind personenbezogene Angaben zu diesem Zweck nicht mehr erforderlich und sind deshalb in den Statistikdateien zu löschen.Die technisch-organisatorischen Maßnahmen der Datensicherung beim Rechnereinsatz entsprechen auch im übrigen nicht den Anforderungen. Ein Bediensteter der LVA hat in einem unbewachten Augenblick ein betriebsbereites Terminal genutzt und sich in strafbarer Weise einen Vermögensvorteil verschafft. Dieser Vorfall belegt, daß eine Verbesserung der Datensicherungsmaßnahmen insbesondere durch Verbesserung der Zugriffskontrolle notwendig ist. Von den zahlreichen Vorschlägen und Anregungen seien nur folgende erwähnt:- Jedem Mitarbeiter sollte zur Klarstellung der Verantwortlichkeit ein eigenes Terminal zur Verfügung gestellt werden;- die Zugriffskontrolle für die Terminals ist durch automatische Abschaltung oder durch einen chipkartengesicherten Gerätezugang gegen mißbräuchliche Zugriffe zu gewährleisten;- eine Einzel- bzw. Gruppenzugangsberechtigung auf bestimmte Terminals - insbesondere im Bereich der Systemtechnik und EDV-Verbindungsstellen - sollte festgelegt und eine EDV-gestützte Kontrolle eingerichtet werden;- Zugriffsbefugnisse sind nur aufgrund schriftlicher Anordnung und im System kontrollierbar zuzuweisen und zu entziehen; Anordnung und Kontrolle sind vom Vollzug personell zu trennen;

- um die Richtigkeit von Daten und die datenschutzgerechte Handhabung bei der automatisierten Datenverarbeitung zu gewährleisten, wird empfohlen, das ohnehin schon bestehende Prinzip weiter zu vervollständigen, an besonders kritischen Stellen den Vorgang durch eine zweite Person zwingend überprüfen zu lassen (Vieraugenprinzip). Dies gilt vor allem für die Reha-Abteilung und die EDV-Koordinierungs- und Verbindungsstellen;- die Funktionstrennung zwischen Systemtechnik und Anwendungsprogrammierung ist im Interesse eines ordnungsgemäßen Ablaufs der Automation und der Verfahrenssicherheit zu realisieren;- zur Kontrolle der Systemtechnik ist eine edv-gestützte Auswertung der Protokolle einzuführen;- eine interne, verselbständigte Revisionsstelle ist einzurichten, die aufgrund der Protokolle im Systembereich und bei der Abwicklung des Massengeschäfts die automatisierte Informationsverarbeitung (welche Daten sind zu welcher Zeit, von wem im Verfahren eingegeben worden) kontrolliert.Zur bürgernahen Beratung von Versicherten - in den Gemeinden sind an bestimmten Tagen regelmäßig Informationsstunden eingerichtet - werden sogenannte "Laptop", tragbare Computer, eingesetzt, mit deren Hilfe über einen Fernzugriff die Versichertendaten des Betroffenen abgerufen und ausgewertet werden können. Diese Geräte eröffnen über das Telefonnetz einen Zugang zu allen Versichertendaten. Diese sensible Leitungsverbindung bedarf eines besonderen Schutzes. Hierzu habe ich gefordert, daß der Verbindungsaufbau durch ein Rückruf- und Identifizierungssystem gesichert und der Zugriff auf den Laptop selbst besser geschützt wird.

Eine Achillesferse ist der Mangel einer ausreichenden Sicherung der in Bearbeitung befindlichen Akten. Abschließbare Behältnisse sind vielfach nicht vorhanden; die Büroräume sind nicht mit Sicherheitsschlössern versehen. Die Zugangssicherung des Gebäudes ist unzureichend. Sogar das Betreten des Hauses zwischen 6.30 Uhr und 8.30 Uhr war unkontrolliert. Auch die Zugangssicherung zu den Archiven muß verbessert werden.Ein Problempunkt war auch die Entsorgung, die datenschutzgerechter zu gestalten ist.Auf unsere Anregung ist die LVA dazu übergegangen, die Untersuchungen von eigenen Bediensteten auf dauernde Dienstunfähigkeit nicht mehr durch den eigenen Ärztlichen Dienst sondern durch den Amtsarzt durchführen zu lassen.Die LVA hat alle unsere Anregungen positiv aufgenommen und ist bemüht, Abhilfe zu schaffen. Die Behandlung der ärztlichen Unterlagen, Stellungnahmen und Berichte im Verwaltungsablauf soll in einer Arbeitsgruppe untersucht werden. Die Umstellungen im Bereich der Automation dürften größtenteils kurzfristig nicht zu bewältigen sein. Die LVA ist nämlich Kooperationspartner des Verbandes der Deutschen Rentenversicherungsträger (VDR), der die erforderlichen Programme arbeitsteilig bei den Verbundpartnern nach gemeinsam erarbeiteten Vorgaben erstellen läßt und die Ergebnisse im Verbund zur Verfügung stellt. Die LVA hat jedoch zugesichert, die Anregungen und Vorschläge im Bereich des VDR vorzutragen und zu unterstützen.

11.3 Angaben von Heilstätten gegenüber ArbeitgeberWenn einem Arbeitnehmer eine Kur bewilligt wird, hat er für die Dauer von sechs Wochen einen Anspruch auf Fortzahlung des Arbeitsentgeltes gegenüber seinem Arbeitgeber (früher § 7 Abs. 1 i.V.m. § 1 Lohnfortzahlungsgesetz; seit 01.06.1994 § 9 Abs. 1 i.V.m. § 3 Entgeltfortzahlungsgesetz). Der Arbeitnehmer muß seinem Arbeitgeber den Zeitpunkt des Kurantritts und den Entlassungstag mitteilen. Dies geschah in der Weise, daß der Arbeitnehmer seinem Arbeitgeber das Einberufungsschreiben und die Entlassungsmitteilung der Behandlungsstätte vorlegte. Die datenschutzrechtliche Problematik dieser Verfahrensweise lag darin begründet, daß der Arbeitnehmer mit der Vorlage dieser Unterlagen seinem Arbeitgeber die Art seiner Erkrankung offenbarte. Da die meisten Kliniken auf die Rehabilitation bestimmter Krankheiten spezialisiert sind, war es für die Personalsachbearbeiter ein leichtes, aus der Art der Kureinrichtung auf die Art der Krankheit des Arbeitnehmers zu schließen.Ich bin deshalb an die Landesversicherungsanstalt für das Saarland herangetreten, um eine Änderung des Verfahrens zu erreichen. Folgende Lösung wurde gefunden: Die Landesversicherungsanstalt stellt den Arbeitnehmern auf Wunsch eine neutrale Bescheinigung über den Beginn und das Ende der Kur aus. In einem Merkblatt wird der Arbeitnehmer über diese Möglichkeit ausdrücklich informiert.Durch dieses Verfahren wird den berechtigten Interessen der Arbeitnehmer auf Schutz ihrer Sozialdaten gegenüber ihrem Arbeitgeber Rechnung getragen.

11.4 Methadon-SubstitutionSeit einiger Zeit besteht im Saarland für Drogensüchtige unter bestimmten Voraussetzungen die Möglichkeit der Behandlung mit dem Ersatzmittel "Methadon".Die Indikationen zur Substitutionsbehandlung, die Qualifikation der Ärzte und die Maßnahmen während der Substitutionsbehandlung hat der Bundesausschuß der Ärzte und Krankenkassen in Richtlinien im einzelnen geregelt. Diese Richtlinien sehen u. a. vor, daß der Arzt den Beginn und die Beendigung der Substitutionsbehandlung mit weiteren Angaben der kassenärztlichen Vereinigung und der zuständigen Krankenkasse anzuzeigen hat. Diese Meldungen sollen der Vermeidung von Mehrfachsubstitutionen, der Einhaltung der Höchstgrenze der Anzahl substituierter Patienten beim einzelnen Arzt und der Sicherstellung der psychosozialen Begleitbetreuung dienen.Diese Meldungen erfolgten ohne Beteiligung des Patienten. Ich habe die Befugnis der kassenärztlichen Vereinigung und der Krankenkasse zur Erhebung dieser Daten in Frage gestellt. Denn es handelt sich um Daten, die der ärztlichen Schweigepflicht unterliegen und deshalb nicht ohne gesetzliche Grundlage oder die Einwilligung des betreffenden Patienten weitergegeben werden dürfen. Im 5. Buch des Sozialgesetzbuches, das in einem eigenen Abschnitt regelt, welche Daten im Rahmen der kassenärztlichen Versorgung vom Arzt an die kassenärztlichen Vereinigungen und die Krankenkassen weitergegeben werden dürfen, ist eine gesetzliche Befugnis zur Übermittlung der fraglichen Daten nicht enthalten. Da auch die kassenärztliche Vereinigung keine Rechtsgrundlage für die Substitutionsmeldungen angeben konnte, wurde unter meiner Beteiligung ein Merkblatt mit einer Erläuterung der einzelnen Datenverarbeitungsvorgänge und eine Einverständniserklärung

zur Weiterleitung der Daten an die kassenärztliche Vereinigung und die zuständige Krankenkasse entwickelt. Mittlerweile wurden auch die bundesweiten Richtlinien um den Hinweis ergänzt, daß die Datenübermittlungen der Einwilligung des Patienten bedürfen. Das Formular einer Einwilligungserklärung ist Bestandteil der Richtlinien. 11.5 Abrechnungsvordrucke - Gefahr für das Arztgeheim-

nisWenn ein Arzt in einem Notfall tätig wird oder die Urlaubs- bzw. Krankheitsvertretung für einen anderen Arzt wahrnimmt, hat er für die Abrechnung seiner ärztlichen Leistungen gegenüber Kassenärztlicher Vereinigung und Krankenkasse ein besonderes Abrechnungsformular zu verwenden. In dem Vordruck waren auch Angaben zu machen, die für den weiterbehandelnden Arzt wichtig, für die Abrechnung allerdings nicht erforderlich waren (z. B. Angaben über Befunde und durchgeführte Therapie). Die routinisierte Durchbrechung des Arztgeheimnisses war zu unterbinden.Der Vordruck wurde mittlerweile geändert. In dem für die Abrechnung bestimmten Durchschlag sind bestimmte Felder geschwärzt, diese Felder können nur auf dem Durchschlag ausgefüllt werden, der für den weiterbehandelnden Arzt bestimmt ist.11.6 Sozialhilfe: Offenbarungspflicht über die Einkom-

mensverhältnisse des Schwiegersohns?Der Träger der Sozialhilfe kann seine Leistungen an den Sozialhilfeempfänger in bestimmtem Umfang von den unterhaltspflichtigen Personen (z.B. Kindern) zurückverlangen. Die Unterhaltspflichtigen sind deshalb

verpflichtet, dem Träger der Sozialhilfe über ihre Einkommens- und Vermögensverhältnisse Auskunft zu geben (§ 116 Abs. 1 BSHG). Auf dem entsprechenden Fragebogen wurde allerdings nicht nur nach den Einkommens- und Vermögensverhältnissen des Unterhaltspflichtigen, sondern auch nach den wirtschaftlichen Verhältnissen des Ehegatten des Unterhaltspflichtigen (Schwiegersohn, Schwiegertochter) gefragt. Eine solche Pflicht zur Auskunftserteilung durch den nicht unterhaltspflichtigen Ehegatten des Unterhaltspflichtigen besteht jedoch nach dem eindeutigen Gesetzeswortlaut nicht (§ 116 Abs. 1 BSHG). Das Bundesverwaltungsgericht (Urteil vom 21.1.1993 -5 C 22.90-) hat deshalb entschieden, daß der Sozialhilfeträger nicht ermächtigt ist, Auskunft über die Einkommens- und Vermögensverhältnisse des nicht unterhaltspflichtigen Ehegatten zu verlangen. Da Angaben über die Einkommensverhältnisse des Ehegatten des Unterhaltspflichtigen sich auch in der Weise auswirken können, daß die Höhe des zu erstattenden Betrages gemindert wird, können solche Angaben auf freiwilliger Basis erhoben werden.Das Ministerium für Frauen, Arbeit, Gesundheit und
Soziales, mit dem ich die Problematik erörtert habe, teilt die Auffassung, daß die Einkommens- und Vermögensverhältnisse der selbst nicht unterhaltspflichtigen Ehegatten nur auf freiwilliger Basis erfragt werden dürfen. Keine Übereinstimmung bestand allerdings anfangs in der Frage, in welcher Form die Betroffenen auf die Freiwilligkeit ihrer Angaben hingewiesen werden müssen. Das Ministerium meinte zunächst, es sei ausreichend, wenn die nicht unterhaltspflichtigen Ehegatten bei Rückfragen hinsichtlich des Auskunftsersuchens des Sozialamtes auf die Freiwilligkeit ihrer Angaben hingewiesen werden. Ich habe dagegen die Auffassung vertreten, daß bereits in dem Erhebungsformular schriftlich auf die Freiwilligkeit der fraglichen Angaben hingewiesen werden muß. Das Ministerium hat

sich mittlerweile meiner Auffassung angeschlossen und die örtlichen Träger der Sozialhilfe im Saarland gebeten, den betreffenden Fragebogen mit einem Hinweis auf die Freiwilligkeit der Angaben über die Einkommens- und Vermögensverhältnisse des nicht unterhaltspflichtigen Ehegatten zu versehen.11.7 "Vorladung" des Sozialhilfeempfängers per Post-

karteEin Petent hat sich darüber beschwert, daß ihm die Einladung zu einer Vorsprache beim Sozialamt auf einer Postkarte zugestellt worden ist. Als Absender war auf der Postkarte das Sozialamt angegeben. Der Petent hat sich dagegen verwahrt, daß auf diese Art und Weise der Briefträger Kenntnis davon erhält, daß er Kontakt zum Sozialamt hat. Der Petent hat darüber hinaus darauf hingewiesen, daß nicht auszuschließen war, daß auch andere Mitbewohner Kenntnis von seiner sozialen Situation erhielten.Die Beschwerde des Petenten ist berechtigt. Die Absen-

derangabe "Sozialamt" auf einem an einen Bürger adressierten Schriftstück stellt eine Verletzung des Sozialgeheimnisses (§ 35 SGB I) dar. Nach dieser Vorschrift hat jeder Anspruch darauf, daß Einzelangaben über seine persönlichen und sachlichen Verhältnisse von den Leistungsträgern als Sozialgeheimnis gewahrt werden. Dazu gehört, daß der Sozialleistungsträger alle geeigneten Maßnahmen ergreift, um zu verhindern, daß Dritte Kenntnis davon erlangen, daß eine Person Kontakt zum Sozialamt hat.

11.8 Der Sozialleistungsberechtigte - primäre Informationsquelle der SozialverwaltungEin Sozialhilfeempfänger hat sich bei mir über die Art der Datenbeschaffung durch das Sozialamt bei der Bearbeitung seines Sozialhilfeantrages beschwert. Das Sozialamt hat zur Berechnung der Hauslasten die Verbrauchsdaten unmittelbar bei den Stadtwerken erfragt. Der Petent meint, es habe ihm Gelegenheit gegeben werden müssen, die Angaben selbst zu liefern. Außerdem sei von dem Sozialamt zur Ermittlung des Verkaufswertes seines Einfamilienhauses ein Mitarbeiter des Bauamtes beauftragt worden, ein Gutachten zu erstellen. Dabei sei auch die Höhe der Sozialhilfe mitgeteilt worden. Durch die Angabe der Höhe der Sozialhilfe an das Bauamt hat das Sozialamt das Sozialgeheimnis (§ 35 Abs. 1 SGB I) verletzt. Eine Offenbarung personenbezogener Daten an Dritte durch die Sozialleistungsträger ist nur zulässig, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist (§ 69 Abs. 1 Nr. 1 SGB X a. F.). Die Angabe der Höhe der Sozialhilfe war für den Zweck der Erstellung eines Wertgutachtens unerheblich und damit unzulässig. Das Sozialamt hat seinen Fehler freimütig eingestanden.Nicht geklärt werden konnte dagegen, ob das Sozialamt dem Petenten vor seiner Anfrage bei den Stadtwerken Gelegenheit gegeben hatte, die erforderlichen Unterlagen selbst vorzulegen. Der Fall gibt mir Gelegenheit, darauf hinzuweisen, daß Sozialdaten grundsätzlich beim Betroffenen zu erheben sind (§ 67 a Abs. 2 Satz 1 SGB X). Ohne Mitwirkung des Antragsstellers dürfen Daten bei dritten Personen oder Stellen nur im Ausnahmefall in den gesetzlich bestimmten Fällen (§ 67 a Abs. 2 Satz 2 SGB X) erhoben werden. Wer Sozialhilfe beantragt, ist zur Mitwirkung verpflichtet und berech-

tigt (§§ 60 ff. SGB I). Die Behörde darf sich grundsätzlich nicht über den Kopf des Betroffenen hinweg die Daten beschaffen.11.9 Zusammenwirken von freier Scheidungsberatung mit
der FamiliengerichtshilfeDurch eine Presseveröffentlichung aufmerksam geworden,
habe ich mich mit der Problematik der gleichzeitigen Wahrnehmung der Trennungs- und Scheidungsberatung einerseits und der Mitwirkung im familiengerichtlichen Verfahren andererseits durch die öffentliche und freie Jugendhilfe auseinandergesetzt. Nach dem Kinder- und Jugendhilfegesetz (KJHG) hat die Jugendhilfe die Aufgabe, Eltern in Fragen der Partnerschaft, Trennung und Scheidung Beratung anzubieten. Im Falle der Trennung oder Scheidung sollen Eltern bei der Entwicklung eines einvernehmlichen Konzepts für die Wahrnehmung der elterlichen Sorge unterstützt werden, das als Grundlage für die richterliche Entscheidung über das Sorgerecht nach der Trennung oder Scheidung dienen kann (§ 17 Abs. 2 KJHG). Es handelt sich hier um ein Beratungsangebot der Jugendhilfe, das von den Beteiligten auf freiwilliger Basis in Anspruch genommen werden kann. Das Jugendamt hat daneben die Aufgabe, im Verfahren
vor dem Familiengericht mitzuwirken, um dem Gericht die sachgerechte Entscheidung über die elterliche Sorge und das Umgangsrecht zu ermöglichen (§ 50 KJHG).Aus datenschutzrechtlicher Sicht ergibt sich die Problematik, eine Organisationsstruktur zu finden, die sicherstellt, daß Informationen, die die Betroffenen im Rahmen der freiwilligen Trennungs- und Scheidungsberatung gegeben haben, ohne ihre Einwilligung nicht für Aufgaben der Familiengerichtshilfe verwandt werden. Denn lediglich für den Fall, daß das Jugendamt zur

Abwendung einer Gefahr für das Wohl des Kindes oder des Jugendlichen das Tätigwerden des Vormundschafts- oder Familiengerichts für erforderlich hält, ist eine Offenbarung gegenüber dem Gericht auch ohne Einwilligung der betroffenen Eltern zulässig (§ 65 Nr. 2 SGB VIII). Für nicht akzeptabel halte ich es, wenn beide Aufgaben durch ein und dieselbe Person wahrgenommen werden. Dies gilt zumindest dann, wenn die Scheidungsberatung zu keinem Ergebnis führt. Denn ich halte es für kaum vorstellbar, daß in den Bericht an das Familien- oder Vormundschaftsgericht keine Informationen Eingang finden, die im Rahmen der freiwilligen Trennungs- und Scheidungsberatung offenbart wurden.Eine institutionelle Trennung zwischen Trennungs- und
Scheidungsberatung und Familiengerichtshilfe wäre aus datenschutzrechtlicher Sicht zweifellos die sicherste Lösung. Ich räume allerdings ein, daß im Interesse der Einheit des Beratungsprozesses dieser Konzeption nicht unbedingt der Vorzug zu geben ist. Für akzeptabel halte ich die von einem Jugendhilfeträger erarbeitete Konzeption, wonach in dem Fall, daß die Scheidungsberatung zu keinem Ergebnis führt, der Fall an einen anderen Kollegen weitergegeben wird.Um das für eine erfolgreiche Beratung erforderliche
Vertrauensverhältnis herzustellen, muß den betroffenen Eltern zu Beginn der Beratung erklärt werden, daß ohne ihre Einwilligung grundsätzlich keine Informationen aus der Beratung an das Familien- oder Vormundschaftsgericht weitergegeben werden. Sie müssen ferner darüber aufgeklärt werden, daß im Interesse des Wohles des Kindes in Ausnahmefällen eine Weitergabe von Informationen auch ohne Einwilligung zulässig ist. Schließlich sollte darauf hingewiesen werden, daß im Falle der ergebnislosen Beratung der Bericht an das Familien--

oder Vormundschaftsgericht durch einen anderen Mitarbeiter erstattet wird. 11.10 Offenlegung des Adoptionsverhältnisses beim KindergeldAdoptivkinder sind leiblichen Kindern gleichgestellt.
Deshalb hat der Gesetzgeber das Adoptionsverhältnis gegen Ausforschung und Offenbarung besonders geschützt, um die völlige Integration des adoptierten Kindes in die Familie zu gewährleisten. Behörden, Arbeitgebern oder anderen Stellen ist aus diesem Grund die Frage nicht erlaubt, ob ein Kind ein leibliches oder ein angenommenes ist.Mehrere Eltern haben sich gegen einen Erklärungsvordruck der Zentralen Besoldungs- und Versorgungsstelle Saar (ZBS) zur Überprüfung des Kindergeldanspruchs gewandt. Auf diesem Vordruck wurde die Beziehung eines jeden Kindes zum Kindergeldberechtigten und zum Ehegatten erfragt. Unter anderem war anzugeben, ob es sich um ein Adoptivkind oder ein leibliches Kind handele.Das Ministerium des Innern hat in seiner Stellungnahme darauf verwiesen, daß das zuständige Bundesministerium den im gesamten Bundesgebiet verwendeten Vordruck herausgegeben habe. Die beanstandeten Angaben seien nur bei Adoptionen Volljähriger und bei solchen nach ausländischem Recht notwendig gewesen. Diese Einschränkung war aus dem Formular jedoch nicht zu erkennen. Die Betroffenen haben in einer Vielzahl von Fällen die Fragen, wie nach dem objektiven Erklärungswert des Vordrucks verlangt, beantwortet und damit auch Angaben über ein gegebenenfalls bestehendes Adoptionsverhältnis gemacht. Wie das Ergebnis zeigt, steht der Vordruck nicht im Einklang mit dem gesetzlich verankerten Schutz des Adoptionsverhältnisses. Ich habe gefordert,

daß die ZBS in diesen Fällen die Befragung in korrekter Form wiederholt und das vorliegende ausgefüllte Exemplar vernichtet. Das Ministerium des Innern hat sich lediglich bereit
erklärt, die ZBS anzuweisen, die entsprechenden Angaben "zu löschen". Diese Anweisung ist dahin zu verstehen, daß die Angaben geschwärzt oder überklebt werden. Diese nachträgliche Veränderung ist unbefriedigend, weil sie den Rückschluß auf das Adoptionsverhältnis erlaubt.11.11 Sozialdatenschutz der Bediensteten eines Sozialleistungsträgers

Eine Mitarbeiterin des Landesamtes für Versorgung und
Soziales hat bei diesem Amt einen Antrag auf Anerkennung als Schwerbehinderte gestellt. Der Antrag wurde abgelehnt; gegen den ablehnenden Bescheid hat die Petentin Widerspruch eingelegt. Sie hat sich bei mir darüber beschwert, daß über diesen Widerspruch ein Abteilungsleiter des Landesamtes für Versorgung und Soziales entschieden hat. Dazu muß man wissen, daß die Abteilungsleiter im Landesamt für Soziales und Versorgung in die Vertretungsregelung des Amtsleiters einbezogen sind und im Vertretungsfall vorbereitende Personalmaßnahmen zur Aufrechterhaltung des Dienstbetriebes treffen können. Die Petentin wollte nicht akzeptieren, daß ein mit Personalangelegenheiten befaßter Mitarbeiter im Rahmen des Widerspruchsverfahrens Kenntnis von ihren gesundheitlichen Verhältnissen erlangt.Die Beschwerde der Petentin war berechtigt. Sozialdaten der Beschäftigten und ihre Angehörigen dürfen Personen, die Personalentscheidungen treffen oder daran mitwirken können, weder zugänglich sein noch vom

Zugriffsberechtigten weitergegeben werden (§ 35 Abs. 1 Satz 3 SGB I). Interessenkollisionen in der Person des Vorgesetzten muß entgegengewirkt werden. Der Sozialdatenschutz der Bediensteten muß auch im Rahmen des Dienstbetriebs eines Sozialleistungsträgers gewährleistet sein.Mit dem Landesamt für Soziales und Versorgung wurde eine Lösung für das Problem gefunden: Die Amtsleitung hat im einzelnen geregelt, welche Bediensteten für die Antragsbearbeitung ihrer Kollegen zuständig sind. Dabei wurde darauf geachtet, daß kein Abteilungsleiter in die Bearbeitung einbezogen ist. Die Akten der Bediensteten werden gesondert in einem verschlossenen Stahlschrank aufbewahrt. Nur die mit der Sachbearbeitung betrauten Bediensteten verfügen über den entsprechenden Schlüssel. Der für die automatisierte Bearbeitung der Vorgänge Amtsangehöriger zuständige Bedienstete besitzt eine eigene Kennung, so daß den übrigen Mitarbeitern Zugriffe auf die automatisiert gespeicherten Daten von Bediensteten nicht möglich sind. 11.12 Behördenkatalog zur Vereinfachung der Entscheidung über die Weitergabe der Daten zur Gefahrenabwehr

Durch das am 18. Juni 1994 in Kraft getretene 2. Gesetz zur Änderung des Sozialgesetzbuches ist der Kreis der Behörden, denen die Sozialbehörde im Rahmen der allgemeinen Amtshilfe personenbezogene Angaben über Namen, Zeitpunkt und Ort der Geburt, derzeitige Adresse und Arbeitgeber übermitteln darf, eingeschränkt worden (§ 68 SGB X). Als Empfänger von Sozialdaten kommen danach in Betracht: Polizeibehörden, Staatsanwaltschaften, Gerichte, Behörden der Gefahrenabwehr, Justizvollzugsanstalten sowie Institutionen, die einen öffentlich-rechtlichen Anspruch von mindestens 1.000

DM geltend machen. Zur Vereinfachung der Entscheidung, ob eine anfragende Stelle als "Behörde der Gefahrenabwehr" anzusehen ist, beabsichtigt der Verband deutscher Rentenversicherungsträger bundesweit ein Verzeichnis dieser Behörden zu erstellen.Gegenüber der Landesversicherungsanstalt habe ich die Auffassung vertreten, daß die Erstellung eines solchen Verzeichnisses nicht im Interesse des Datenschutzes liegen dürfte. Ich habe die Befürchtung, daß das Verzeichnis der Behörden der Gefahrenabwehr einer Routinisierung des Vorgangs Vorschub leistet und Sozialdaten an diese Behörden übermittelt werden, ohne daß im konkreten Einzelfall die Daten zur Abwehr von Gefahren benötigt werden. Denn es gibt Behörden, die sowohl Aufgaben der Gefahrenabwehr als auch sonstige Aufgaben wahrnehmen (z.B. Landratsämter und sonstige untere Verwaltungsbehörden). Sozialdaten können an diese Behörden aber nur insoweit mitgeteilt werden, als sie diese zur Erfüllung von Gefahrenabwehraufgaben benötigen und kein Grund zur Annahme besteht, daß dadurch schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Es ist also in jedem Einzelfall eine Güterabwägung zu treffen.Ich hoffe im Interesse des Datenschutzes, daß die Erstellung des geplanten Verzeichnisses unterbleibt.

12. Gesundheit12.1 Krankenversicherungskarte (KVK), Wegbereiter für
maschinenlesbare Patientenkarten?Mit dem Gesundheitsstrukturgesetz ist die Krankenversicherungskarte eingeführt worden, die spätestens bis zum 1.1.1995 den Krankenschein ersetzen soll. Die KVK ist ein Teil der im Gesundheitsreformgesetz und im Gesundheitsstrukturgesetz vorgesehenen Maßnahmen, um Transparenz des Leistungsgeschehens und Kostenbegrenzung im Gesundheitswesen zu erreichen. Es handelt sich um eine Speicher(Chip-)Karte, die nur dazu verwendet werden darf, die Anspruchsberechtigung des Versicherten gegenüber den Kassen nachzuweisen und die automatische Abrechnung unter Einsatz maschinenlesbarer Formulare durchzuführen. Den Inhalt der Karte hat der Gesetzgeber genau vorgegeben (§ 291 SGB V); medizinische Angaben dürfen auf ihr nicht gespeichert werden. Neben den Identifikatoren des Versicherten ist vor allem die Krankenversichertennummer als Sortierkriterium für die Automation bedeutsam. Die Angaben auf der KVK werden mit Hilfe von Lesegeräten, die den Ärzten von der kassenärztlichen Vereinigung zur Verfügung gestellt werden, auf maschinenlesbare Formulare übertragen. Auf dem automatisierten Wege dürfen jedoch den Kassen im weiteren Verlauf des Abrechnungsvorgangs keine versichertenbezogene Daten zu Abrechnungszwecken zur Verfügung gestellt werden (§ 295 Abs. 2 SGB V).Die Karte enthält zusätzliche Speicherbereiche, die
für die gesetzlich vorgegebenen Datenarten nicht benötigt und derzeit lediglich mit überschreibbaren Füllzeichen belegt sind. Hier wird deutlich, daß mit der Einführung der KVK und der Zurverfügungstellung der Lesegeräte für die Ärzte eine Infrastruktur geschaffen wurde, die weitgehende Möglichkeiten der Speicherung

und Verwendung von medizinischen Daten eröffnet. Das technisch Machbare drängt nach gesetzlicher Umsetzung.Die KVK ist eine "einfache" Speicherkarte, die keine Sicherheitslogik enthält. Der Sicherheitsmechanismus bewegt sich insgesamt auf einem Niveau, das zwar den technischen Anforderungen des Abrechnungsverfahrens genügt. Bei der Benutzung dieser Speicherkarten wird jedoch nicht einmal eine benutzeridentifizierende Kennzahl (PIN) abgeprüft. Gerade mit Rücksicht auf die Gefahr des Kartenmißbrauchs kann diesem Aspekt bereits derzeit Bedeutung zukommen. Ferner wird nicht geprüft, zu welchen Funktionen (Schreib-, Lesezugriff) das Arztgerät berechtigt ist (Authentifizierung und Autorisierung). Des weiteren ist eine Verschlüsselung, die für Chipkarten derzeit erst erprobt wird, nicht möglich. Die durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten Arztlesegeräte sind ebenfalls nicht dahin überprüft, ob sie keinen Schreibzugriff, sondern lediglich einen Lesezugriff haben. Wichtig ist die Beschränkung auf den Lesezugriff aber gerade mit Rücksicht auf die lediglich mit Füllzeichen belegten Speicherbereiche der KVK, die etwa auch mit medizinischen Daten überschrieben werden könnten. Wegen dieser Sicherungsdefizite wird man den Umfang der Datenspeicherung auf der KVK und die Zugriffe durch Ärzte und gesetzliche Krankenkassen im Auge behalten müssen. Festzuhalten ist jedenfalls, daß die derzeit vorhandenen Sicherheitsmechanismen nicht ausreichen, wenn medizinische Daten auf der Chipkarte gespeichert würden.Gerade weil die Krankenversicherungskarte einen Einstieg in die Verwendung eines neuen Kartentyps zur Speicherung und Nutzung medizinischer Daten darstellt, ist es notwendig, sich mit Chancen und Risiken dieser Entwicklung auseinanderzusetzen. Die Speicherkapazität und die Verarbeitungsintelligenz der Chipkarten wird

sich in absehbarer Zeit in einem Ausmaß verbessern, daß technisch gesehen auch die gesamte Krankengeschichte eines Patienten - ja sogar Röntgenbilder - abgespeichert werden können. Inzwischen zeichnen sich bereits verschiedene Kartentypen ab, die unterschiedliche Zielsetzungen verfolgen:- Notfallkarten, die z. B. Risikofaktoren wie Allergien, aktuelle Medikationen etwa bei Diabetikern oder Impfungen auf schnellem und einfachem Wege verfügbar halten;- Karten für besondere Patientengruppen z. B. zur verbesserten Nachsorge Krebskranker und von Transplantationspatienten;- Patientenkarten mit medizinischen Informationen über die gesamte Krankengeschichte einschließlich Röntgenaufnahmen und Medikationen zur generellen Verwendung durch mit- oder nachbehandelnde Ärzte;- Apothekerkarten insbesondere zur Beratung bei Selbstmedikation.Abgesehen von den verschiedenen, speziellen Zwecksetzungen, vor allem zur Behandlung von Notfallpatienten, sollen die verschiedenen Kartentypen die Kommunikation zwischen den Ärzten (z. B. Hausärzten, Fachärzten, Fachabteilungen eines Krankenhauses) verbessern und die Kosten infolge von Mehrfachuntersuchungen mindern helfen. Die praktischen Schwierigkeiten dürfen nicht übersehen werden, die sich allein dadurch ergeben, daß größere Transparenz für Ärzte und Kassen nur erreicht wird, wenn die Dokumentation standardisiert und strukturiert ist. In diesem Zusammenhang dürften sich noch einige Probleme in der Diskussion unter Fachleuten ergeben.

Die Vorteile solcher Patientenkarten liegen zwar auf der Hand. Mit ihrer Verwendung steigen jedoch die Gefahren für die Persönlichkeitsrechte und das Arztgeheimnis, weil nicht nur die Mißbrauchsmöglichkeiten etwa bei Verlust, Diebstahl und infolge unbefugten Zugriffs wachsen. Der Datenschutz muß auch als das verfassungsmäßige Recht des einzelnen verstanden werden, über den Umgang mit seinen Daten selbst so zu verfügen und bestimmen zu können, wie über sein Eigentum. Es gibt kaum andere Daten, die dem Betroffenen so sehr zu eigen sind, wie Angaben über seine Gesundheit. Deshalb muß er sicher sein, daß medizinische Daten, die er für bestimmte Zwecke anderen überläßt oder vielleicht auch überlassen muß, nur für diese Zwecke genutzt werden.Besitz, Inhalt und Nutzung einer solchen Karte stehen
mit Rücksicht auf das Persönlichkeitsrecht des Bürgers - oder wie das Bundesverfassungsgericht es ausdrückt im Hinblick auf sein "informationelles Selbstbestimmungsrecht" - in seiner freien Entscheidung.Fraglich ist zunächst, ob die Freiwilligkeit der Entscheidung für oder gegen die Gesundheitskarte in der Praxis stets gewährleistet ist. So kann ein faktischer Zwang auf die Entscheidungsfreiheit des Betroffenen ausgeübt werden, wenn ein Krankenversicherungsunternehmen oder eine Krankenkasse mit der Einführung Vorteile oder Nachteile verbindet oder auch nur das Verfahren der Abwicklung ändert; z. B. den Schriftwechsel erschwert oder den Zugang zu Leistungen Karteninhabern erleichtert. Zur Freiwilligkeit gehört, daß mit der Nichtteilnahme keine Nachteile verbunden sein dürfen. Die schriftliche Einwilligung des Betroffenen nach umfassender Aufklärung über Zweck, Inhalt und Verwendung der Gesundheitskarte ist unabdingbar.

Da aber damit gerechnet werden muß, daß aus dem Trend hin zu großen Informationssystemen ein beinahe unausweichlicher Druck für die Patienten entsteht, muß der Gesetzgeber im voraus die Rahmenbedingungen für die Patientenkarten eindeutig festschreiben und die organisatorisch-technischen Maßnahmen der Datensicherung festlegen.Gefahren für die Selbstbestimmung des Patienten ergeben sich im übrigen allein schon daraus, daß Chipkarten bisher nur mit technischen Hilfsmitteln gelesen werden können, die der Betroffene in der Regel nicht besitzt. Er kann also regelmäßig nicht kontrollieren, daß der Aussteller der Karte und sein Arzt nur die mit ihm vereinbarten Daten im Chip speichern, das Lesegerät auch wirklich alle gespeicherten Daten anzeigt und die Karte keine oder nur eindeutig vereinbarte Verarbeitungsprogramme enthält.Zu den Details, die im einzelnen noch nicht voll übersehen werden können, dürfte es beispielsweise auch gehören, daß der Betroffene im Einzelfall frei und ohne Benachteiligung entscheiden kann, ob er die Gesundheitskarte vorzulegen bereit ist. Es ist seine freie Entscheidung, welche Daten er wann, wem offenbart. Seinem Selbstbestimmungsrecht zufolge muß es ihm möglich sein, darüber zu befinden, welche Informationen auf der Chipkarte jeweils den Benutzern zur Kenntnis gelangen dürfen (Segmentierung des Zugriffs). Der Patient muß bei einem Arztwechsel nicht den gesamten Karteninhalt offenbaren müssen. So kann er beispielsweise daran interessiert sein, daß der nachbehandelnde Arzt von der bisherigen Medikation nichts erfährt, weil er eine neue, von der Behandlung unbeeinflußte Diagnose und Therapie erreichen will. Hierzu trägt vor allem auch die Entscheidungsfreiheit des Betroffenen bei, selbst zu bestimmen, welche Daten erfaßt, geändert oder gelöscht werden.

Eine ganz erhebliche Verschlechterung könnte darin liegen, daß die Daten auf einer Gesundheitsdatenkarte, die der Patient in eigener Verfügung hat, nicht mehr der ärztlichen Schweigepflicht unterliegen. Es ist also nicht nur an Mißbrauchsgefahren durch Diebstahl zu denken, sondern auch an zulässige Beschlagnahme. Eine Anpassung der gesetzlichen Vorschriften dürfte unerläßlich sein.Es geht hier nicht darum, die technische Entwicklung
und ihre Vorteile für die Menschen zu verhindern. Vielmehr ist eine Güterabwägung zwischen dem Datenschutz und der Qualität der ärztlichen Versorgung notwendig. Wenn der Gesetzgeber davon überzeugt ist, daß die Vorteile die stets möglichen Nachteile überwiegen, kann er durch gesetzliche Maßnahmen den Trend unterstützen. Voraussetzung ist jedoch, daß die Position des Betroffenen durch angemessenen Datenschutz ausreichend gesichert ist. Eine fundierte Technikfolgenabschätzung ist unerläßlich.Die Datenschutzbeauftragten haben anläßlich ihrer
Konferenz vom 9./10.3.1994 die als Anlage 10 beigefügte Entschließung gefaßt. 12.2 Defizite des Saarländischen ÄrztekammergesetzesDie Aufgaben der Ärztekammer, die Berufsausübung und
Weiterbildung der ihr angehörenden Ärzte sowie die Berufsgerichtsbarkeit sind im Saarländischen Ärztekammergesetz geregelt. Die Ärztekammer verarbeitet personenbezogene Daten ihrer Mitglieder, also die Daten von Ärzten, Zahnärzten und Medizinialassistenten. Das Ärztekammergesetz weist hier ein Regelungsdefizit auf, denn Umfang, Zweck und Voraussetzungen der Datenverarbeitung sind im Gesetz nicht geregelt. Spätestens seit

dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 steht fest, daß Eingriffe in das grundgesetzlich geschützte Recht auf informationelle Selbstbestimmung nur auf der Grundlage einer bereichsspezifischen gesetzlichen Regelung zulässig sind.Ich habe deshalb das zuständige Ministerium aufgefordert, das Ärztekammergesetz zu ergänzen:- Umfang und Zweck der Verarbeitung personenbezogener Daten über die Kammerangehörigen müssen für die Betroffenen transparent und klar festgelegt sein. Zumindest in einer Satzung muß festgelegt werden, welche Daten die Kammerangehörigen angeben müssen, unter welchen Voraussetzungen Daten an andere Stellen weitergegeben werden dürfen sowie wie lange die Daten über die Kammerangehörigen gespeichert werden dürfen.- Festgelegt werden muß, wie lange die Unterlagen über berufsgerichtliche Verfahren aufbewahrt werden dürfen.- Soweit personenbezogene Patientendaten verarbeitet werden, müssen die Voraussetzungen im Gesetz klar festgelegt werden, da die Patienten keine Kammerangehörigen sind.Eine Reaktion des zuständigen Ministeriums auf meinen Vorstoß zur Änderung und Ergänzung des Ärztekammergesetzes ist bisher leider nicht erfolgt. 12.3 Änderung der Berufsordnung für ÄrzteSchon im Jahre 1991 hat der Bundesgerichtshof (Urteil vom 11.12.1991, Az. VIII ZR 4/91) entschieden, daß die Weitergabe der Patientenkartei beim Verkauf einer

Arztpraxis nur mit ausdrücklicher Zustimmung der einzelnen Patienten zulässig ist. Nach Auffassung des Bundesgerichtshofes verletzt die Übergabe der Kartei ohne Einwilligung der Patienten deren "informationelles Selbstbestimmungsrecht" und verstößt gegen die ärztliche Schweigepflicht. Die Zustimmung der Patienten müsse in "eindeutiger und unmißverständlicher Weise" eingeholt werden.In der Folgezeit wurden verschiedene praktische Möglichkeiten diskutiert, um den Anforderungen des Urteils gerecht zu werden (z.B. Verbleib der Unterlagen beim Verkäufer oder bei der Ärztekammer; gesonderte Verwahrung in einem Schrank, zu dem der Praxisübernehmer nur zusammen mit einem weiteren Praxismitarbeiter Zugang hat, sogenanntes Zwei-Schlüssel-Verfahren). Die Ärztekammer im Saarland beabsichtigte, in ihre Berufsordnung eine Regelung aufzunehmen, wonach der übernehmende Arzt, dem bei einer Praxisaufgabe oder Praxisübergabe ärztliche Aufzeichnungen über Patienten in Obhut gegeben werden, diese Aufzeichnung unter Verschluß halten muß und sie nur mit Einwilligung des Patienten einsehen oder weitergeben darf.Das Ministerium für Frauen, Arbeit, Gesundheit und Soziales hat mich speziell zu dieser Frage anläßlich einer aufsichtsrechtlichen Überprüfung der Berufsordnung beteiligt.Ich habe darauf hingewiesen, daß der ärztlichen Schweigepflicht nur dann Genüge getan wird, wenn die Patientenunterlagen dem Praxisübernehmer verschlossen übergeben werden. Eine entsprechende Klarstellung in der Berufsordnung habe ich empfohlen. Leider mußte ich feststellen, daß die Berufsordnung entgegen der ursprünglichen Absicht der Ärztekammer in diesem Punkt unverändert geblieben ist.

12.4 Pflegedienstprogramm MediCareEiner Informationsschrift mußte ich entnehmen, daß die
Unikliniken im Rahmen eines Pilotprojekts die Software "MediCare" zur EDV-Unterstützung der täglichen Stationsarbeit in der Inneren Medizin II erproben; das Verfahren soll später auf die gesamte Uniklinik ausgedehnt werden. Die Anwendung basiert auf einem Netzwerk mit Rechner (Server), Personalcomputern in Stationszimmern und bei den Leistungserbringern wie z.B. Labor und Radiologie. Eingesetzt werden tragbare Computer ohne Tastatur, die mit Hilfe von Stifteingabe und Handschrifterkennung (sogenannten Notepads) anstelle von herkömmlichen Krankenblättern unmittelbar am Krankenbett bei der Visite bedient werden können.Auf dem Notepad werden die Patientenstammdaten, die
Vitalwerte, die Aktivitäten des täglichen Lebens, die Pflege- und Arztanamnese, die Leistungsanforderungen, die Verordnungen und Befunde gespeichert. Bei Bedarf werden die Daten zwischen Notepad und Serverrechner mit Hilfe einer Datenübertragung aktualisiert.Das Pflegedienstprogramm MediCare soll schrittweise die herkömmliche Krankenakte vollständig ersetzen. Als Hauptvorteile der Unterstützung des Pflegepersonals durch die EDV werden genannt, die Reduzierung der Schreibarbeiten auf ein Minimum, eine übersichtlichere Gliederung der Krankenakten, eine schnellere und übersichtlichere Befundpräsentation, eine erhebliche Vereinfachung bei der Pflegeanamnese, Pflegeplanung und Pflegedokumentation, eine einfache, schnelle und papierlose Erstellung von Leistungsanforderungen, eine schnellere und vereinfachte Terminplanung und Terminkontrolle sowie eine übersichtlichere Darstellung aller Stationsdaten. Man erhofft sich von dem Einsatz

des Systems eine erhebliche Zeiteinsparung bezüglich der pflegerisch-verwaltenden Tätigkeiten, so daß das Pflegepersonal mehr Zeit für die Patientenbetreuung hat. So wichtig diese Ziele auch sind, muß darauf geachtet werden, daß die Persönlichkeitsrechte der Patienten durch Einsatz dieses automatisierten Verfahrens mit seinen speziellen Risiken nicht auf der Strecke bleiben.Ich habe eine Reihe von Verbesserungen im Bereich der organisatorisch-technischen Maßnahmen der Datensicherung gefordert:- Der Rechner (Server) muß in einem besonders gesicherten Raum aufgestellt werden. Zutritt zu diesem Raum dürfen lediglich berechtigte Personen haben. Der Kreis dieser Personen muß genau festgelegt und diese müssen auf ihre Verantwortung im Rahmen des Datenschutzes hingewiesen werden.- Die auf dem Notepad erfaßten Daten müssen verschlüsselt werden.- Die Paßwortlänge ist auf sechs Stellen zu erweitern.

Ein Programmabbruch nach drei falschen Paßworteingaben ist vorzusehen.- Der Zugang zum Betriebssystem über Notepad ist zu sperren.- Die Systemkomponente zur Eintragung neuer Benutzer muß auf dem Notepad gelöscht werden; diese Funktionen dürfen nur am besonders geschützten Rechner ausgeführt werden.- Nach Absturz der MediCare-Software und Neustart muß die Benutzerkennung und das Paßwort neu abgefragt werden.

- Jedem Datensatz ist außer der Kennung des angemeldeten Benutzers das Datum und die Uhrzeit der Eingaben anzuhängen.Nicht befriedigend geregelt ist bisher die Löschung der gespeicherten Patientendaten. Das Saarländische Krankenhausgesetz (§ 29 Abs. 5 Satz 1) schreibt mit gutem Grund vor, daß Patientendaten, die im automatisierten Verfahren mit der Möglichkeit des Direktabrufes gespeichert sind, unmittelbar nach Abschluß der Behandlung in MediCare zu löschen sind. Lediglich Daten, die zur Auffindung archivierter Daten erforderlich sind, dürfen auskunftsfähig gespeichert bleiben.Die Funktionstrennung war nicht in ausreichendem Maße gewährleistet, da Betriebssystemverwaltung und Anwendungssystembetreuung in einer Hand liegen (zur Problematik der Funktionstrennung vgl. auch Tz. 15.2.2).Die Verhandlungen mit den Universitätskliniken zur Umsetzung der von mir geforderten technisch-organisatorischen Maßnahmen der Datensicherung waren bei Redaktionsschluß noch nicht abgeschlossen.12.5 Studie zur Verbesserung der KrankenhaushygieneIm Berichtszeitraum ist im gesamten Bundesgebiet eine Studie zur Qualitätssicherung in der Krankenhaushygiene angelaufen. Bei der Studie geht es darum, die Ursachen von Krankenhausinfektionen zu erkennen und Grundlagen für ihre Minimierung zu gewinnen.Aus den Krankenunterlagen der Krankenhauspatienten werden medizinische Daten in einen Erhebungsbogen eingetragen, an das Klinikum Freiburg weitergeleitet, dort automatisiert gespeichert und ausgewertet. Ärzte

der Hygiene-Institute der Freien Universität Berlin und der Universität Freiburg übertragen die Daten aus den Krankenunterlagen in die Erhebungsbögen. Dieser Vorgang ist datenschutzrechtlich als Übermittlung personenbezogener Daten und als Durchbrechung der ärztlichen Schweigepflicht zu werten, da dabei nicht mit der Behandlung und Versorgung der Patienten im Krankenhaus beauftragte Dritte Kenntnis von personenbezogenen und unter die ärztliche Schweigepflicht fallenden Angaben erhalten. Das Saarländische Krankenhausgesetz läßt aber eine Übermittlung von Patientendaten an Personen und Stellen außerhalb des Krankenhauses grundsätzlich nur zu, wenn die Einwilligung der Patienten eingeholt wird (§ 31 Abs. 2 SKHG). Die Projektleitung sah zunächst erhebliche praktische
Schwierigkeiten. Man scheute nicht nur den Verwaltungsmehraufwand, sondern befürchtete auch eine negative Selektion durch Verweigerung der Einwilligung. Schließlich erarbeitete die Projektleitung eine Einwilligungserklärung, in der die Patienten über das Ziel des Forschungsvorhabens sowie Art und Umfang der Datenverarbeitung aufgeklärt werden.Wie die Projektleitung mitteilt, hat sich das Verfah-
ren der Einholung von schriftlichen Einwilligungserklärungen bei Durchführung der Studie bewährt. Ich sehe hierin einen Beweis, daß die Anforderungen des Gesetzgebers im Interesse der Transparenz der Informationsverarbeitung und der freien Entscheidung des Betroffenen nicht überhöht und der Praktikabilität im Alltag nicht entgegenstehen.

12.6 Modellvorhaben zur Prüfung der Notwendigkeit der Krankenhausbehandlung

Die Krankenkassen müssen in jedem Land die Notwendigkeit der Krankenhausaufnahmen durch den Medizinischen Dienst der Krankenversicherung als Modellvorhaben prüfen lassen (§ 275 a Abs. 1 SGB V). Die näheren Modalitäten dieser Prüfungen haben im Saarland die Saarländische Krankenhausgesellschaft und die Krankenkassen im Saarland ausgehandelt. Der Vertragsentwurf wurde mir zur datenschutzrechtlichen Prüfung vorgelegt. Einige datenschutzrechtlichen Verbesserungen konnten erreicht werden:

- Der Vertrag sieht modellbegleitende Arbeitsgruppen im Krankenhaus und auf Landesebene vor. Auf meine Anregung hin wurde in den Vertragstext das Verbot aufgenommen, in den Arbeitsgruppen Einzelfälle in personenbezogener Form zu erörtern.
- In den Vertrag wurde eine Zweckbindungregelung aufgenommen, wonach im Zusammenhang mit dem Modellvorhaben bekanntgewordene personenbezogene Daten nur für Zwecke des Modellvorhabens genutzt werden dürfen. Es wurde im Vertrag klargestellt, daß durch organisatorisch-technische Maßnahmen sichergestellt werden muß, daß auf personenbezogene Daten des Modellvorhabens nur Bedienstete des Medizinischen Dienstes Zugriff haben, die mit der Aufgabe förmlich betraut sind.
- Falls der Medizinische Dienst Patienten untersuchen muß, ist dies nur mit schriftlicher Einwilligung des betreffenden Patienten zulässig.

In dem Vertrag ist vorgesehen, daß die beteiligten Krankenhäuser dem Medizinischen Dienst zum Zwecke der Auswahl der zu prüfenden Fälle eine Liste mit den

Daten aller in dem Prüfzeitraum aufgenommenen Patienten zur Verfügung stellen. Die Liste soll neben den Personalien des Patienten Angaben zur sozialen Situation des Patienten (Altenheim, Pflegeheim, kein fester Wohnsitz) enthalten. Da die fraglichen Angaben aber nicht zu den Informationen gehören, die der Patient bei einer Krankenhausaufnahme zum Zwecke der Behandlung anzugeben verpflichtet ist, müßten diese Daten speziell für die Durchführung des Modellvorhabens erhoben werden. Dies halte ich nicht für zulässig. Eine Befugnis für den Medizinischen Dienst, zum Zwecke der Durchführung des Modellvorhabens personenbezogene Daten zusätzlich zu erheben, ist im Gesetz nicht vorgesehen. 12.7 Warnmeldungen bei KrankenhauswanderernSaarländische Krankenhäuser informierten sich gegenseitig über Personen, bei denen die Kostenübernahme durch die Krankenkassen Schwierigkeiten bereitete. Ich habe deutlich gemacht, daß ich dieses Verfahren für datenschutzrechtlich nicht zulässig halte. Denn eine entsprechende Befugnis für diese Datenübermittlungen enthält das Saarländische Krankenhausgesetz (§ 29 Abs. 4) nicht.Abgesehen davon halte ich solche Warnmeldungen für kein geeignetes Mittel, Mißbräuche zu verhindern, weil eventuelle frühere Betrügereien eine Ablehnung der Krankenhausbehandlung nicht rechtfertigen, wenn später tatsächlich einmal eine akute Behandlungsbedürftigkeit besteht. Außerdem steht der Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen, die von der Speicherung nichts wissen und damit auch keine Möglichkeit der eventuellen Richtigstellung haben, in keinem Verhältnis zu dem gewünschten Erfolg. Denn wie

mir berichtet wurde, verlassen die Betroffenen das Krankenhaus in der Regel schon vor der eingehenden ärztlichen Untersuchung. Der Schaden, den solche Personen den Krankenhäusern zufügen, dürfte also allein schon wegen der kurzen Aufenthaltsdauer nicht besonders hoch zu veranschlagen sein. Hinzu kommt, daß die Warnmeldungen breit gestreut werden, ohne daß überhaupt Anhaltspunkte dafür bestehen, daß der Betreffende diese Krankenhäuser aufsucht. Ich halte solche Warnmeldungen deshalb für einen unverhältnismäßigen Eingriff in das Persönlichkeitsrecht des Betroffenen. Das Ministerium teilt meine Auffassung, daß nach der gegenwärtigen Rechtslage das praktizierte Verfahren der Warnmeldungen unzulässig ist, will allerdings im Rahmen einer späteren Novellierung des Saarländischen Krankenhausgesetzes eventuell eine entsprechende Befugnisnorm schaffen. 12.8 Die Todesbescheinigung und ihre Nutzung für wis-

senschaftliche ZweckeIn der Todesbescheinigung - auch Leichenschauschein
oder Totenschein genannt - stellt der Arzt den Tod, den Todeszeitraum, die Todesart und die Todesursache fest. Die Bescheinigung wird nach der Beurkundung des Sterbefalles vom Standesamt an das Gesundheitsamt zum Zwecke der Bekämpfung übertragbarer Krankheiten weitergeleitet. Von dort gelangt sie zum Statistischen Landesamt zur Erstellung der Todesursachenstatistik. Schließlich wird sie beim Gesundheitsamt aufbewahrt. Nähere Regelungen zu der Todesbescheinigung sollen in einem Friedhofsgesetz getroffen werden, zu dem das zuständige Ministerium einen Entwurf vorgelegt hat.Wegen der Sensibilität der Angaben über die Todesart
und Todesursache (Unfall, Vergiftung, Suizid, Behand-

lungsfehler) und die eventuelle Ursächlichkeit früherer Krankheitszustände, die in den vertraulichen Teil der Todesbescheinigung aufzunehmen sind, habe ich darauf gedrungen, daß die Personen und Stellen abschließend benannt werden, denen die Bescheinigung auszuhändigen ist und die Verantwortung für die Weiterleitung an die zuständigen öffentlichen Stellen zu übernehmen haben. Abschließend festzulegen waren auch die Personen, die Einsicht in den vertraulichen Teil nehmen dürfen und die genaue Reihenfolge, in der die verantwortlichen und berechtigten Angehörigen die Todesbescheinigung erhalten dürfen.Aus zahlreichen Eingaben in der Vergangenheit ist mir
bekannt, daß eine erhebliche rechtliche Unsicherheit darüber besteht, ob und in welchem Umfange die Angaben in der Todesbescheinigung für wissenschaftliche Zwecke verwendet werden dürfen. So hat beispielsweise im letzten Jahr das Deutsche Krebsforschungszentrum in Zusammenarbeit mit einem Institut für Präventionsforschung und Sozialmedizin für eine epidemiologische Studie Angaben zur Todesursache zahlreicher früherer Gießereiarbeiter erbeten. In einer anderen Studie des Deutschen Krebsforschungszentrums sollte über die Todesursache von Arbeitnehmern in der Glasfaserindustrie Auskunft gegeben werden. Ich habe daher vorgeschlagen, im Friedhofsgesetz Regelungen zur Nutzung der Todesbescheinigung für wissenschaftliche Zwecke zu treffen. Eine bereichsspezifische Regelung halte ich insbesondere für notwendig, weil auch die schutzwürdigen Belange der Hinterbliebenen tangiert sein können.Darüber hinaus habe ich Anfragen von Angehörigen Ver-
storbener erhalten, die - etwa zur Klärung von Versicherungsleistungen - Einsicht in die Todesbescheinigungen nehmen wollten. Es sollte eine Regelung in das Gesetz aufgenommen werden, daß Angehörigen, die ein berechtigtes Interesse nachweisen, auf Antrag unent-

geltlich Auskunft aus der Todesbescheinigung erteilt oder eine Kopie zur Verfügung gestellt wird.12.9 Anonymität der Pflichtberatung vor dem Schwanger-
schaftsabbruch und Wahrung des Sozialgeheimnisses
bei der KostenübernahmeIn dem Urteil des Bundesverfassungsgerichts zum Schwangerschaftsabbruch vom 28. Mai 1993 hat das Gericht festgestellt, daß die schwangere Frau bei Inanspruchnahme der Beratung auf ihren Wunsch gegenüber der sie beratenden Person anonym bleiben kann. Gemeinsam mit dem zuständigen Ministerium habe ich Überlegungen angestellt, wie diese Forderung des Bundesverfassungsgerichts in die Praxis umgesetzt werden kann. Das Ergebnis wurde in einem Papier "Datenschutzrechtliche Hinweise im Zusammenhang mit der Beratung" zusammengefaßt, das den einzelnen Beratungsstellen zur Verfügung gestellt wurde. Folgende Punkte aus diesem Papier erscheinen mir besonders wichtig:- Die bei der Beratungsstelle verbleibenden Beratungs-
bescheinigungen dürfen den Namen der Frau nicht enthalten.- In dem von der Beratungsstelle über die Beratung zu fertigenden Protokoll wird der Name der Frau ebenfalls nicht festgehalten. - Nach Abschluß der Beratung soll eine andere Person
als diejenige, die die Beratung durchgeführt hat, die namentliche Beratungsbescheinigung ausstellen.Bei aller Übereinstimmung im grundsätzlichen habe ich Kritik üben müssen. Die Beratungsbescheinigung muß stets von einer anderen Person ausgestellt werden.

Dies ist in den Hinweisen nicht deutlich genug zum Ausdruck gekommen. Mir ist zwar bewußt, daß diese Forderung in Beratungenstellen mit geringem Personalbestand auf praktische Schwierigkeiten stößt. Es müssen jedoch alle Vorkehrungen getroffen werden, daß dem Wunsch der Schwangeren gegenüber der/dem sie Beratenden anonym bleiben zu können, Rechnung getragen wird. Ich habe deshalb vorgeschlagen, daß Beratungsstellen, in denen den notwendigen organisatorischen Maßnahmen nicht Rechnung getragen werden kann, die Frauen darauf hingewiesen werden und ihnen anheim gestellt wird, sich in einer größeren Beratungsstelle, die die Anonymität gewährleisten kann, beraten zu lassen.Bei Frauen, die aufgrund ihrer Einkommens- und Vermögensverhältnisse nicht in der Lage sind, den Schwangerschaftsabbruch zu bezahlen, übernimmt das Land diese Kosten. Zuständige Behörde ist das Landesamt für Soziales und Versorgung. Die Antragsformulare wurden auf meine Anregung hin
überarbeitet. Das Bundesverfassungsgericht hat für Leistungen der Sozialhilfe bei Schwangerschaftsabbruch besondere Kriterien aufgestellt. So ist etwa ein Rückgriff auf Familienangehörige nicht zulässig. Bei der Gestaltung der Formulare hat mich das zuständige Ministerium beteiligt. Eine zentrale Frage bei der datenschutzrechtlichen
Beurteilung von Fragebögen ist, ob sämtliche in dem Antrag von dem Antragsteller verlangten Angaben zur Aufgabenerfüllung der Behörde tatsächlich erforderlich sind. Eine abschließende Prüfung dieser Frage war mir nicht möglich, da Richtlinien des Ministeriums über die Voraussetzungen der Hilfegewährung im einzelnen nicht existierten und bis heute nicht erlassen sind. Der Hinweis des Ministeriums auf die entsprechende Anwendung des Bundessozialhilfegesetzes macht solche

Richtlinien nicht entbehrlich, da es gerade notwendig gewesen wäre, die Abweichungen von der normalen Sozialhilfegewährung festzuhalten.Abgesehen von diesem Mangel konnte ich erreichen, daß der in dem ursprünglichen Fragebogenentwurf vorgesehene Datenumfang erheblich reduziert wurde. So haben eine Vielzahl von Fragen zu den persönlichen Verhältnissen und den Einkommensverhältnissen der Antragstellerin keinen Eingang in den Fragebogen gefunden. Ursprünglich war auch vorgesehen, daß das Landesamt für Soziales und Versorgung beim Einwohnermeldeamt einen Meldeauszug anfordern kann, um den Wohnort der Antragstellerin zu überprüfen. Ich habe die Befürchtung geäußert, daß bei Anforderung solcher Melderegisterauszüge durch das Landesamt für Soziales und Versorgung es für den zuständigen Sachbearbeiter beim Meldeamt naheliegend ist, daß hier die Daten einer Frau angefordert werden, die eine Abtreibung plant. Das Landesamt für Soziales und Versorgung verzichtete nach meiner Intervention auf die Anforderung von Melderegisterauszügen.Im Berichtszeitraum habe ich außerdem die Verfahrensweise bei der Kostenübernahme für Schwangerschaftsabbrüche vor Ort überprüft. Da es hier um die Verarbeitung äußerst sensibler Daten geht, habe ich mein Hauptaugenmerk darauf gerichtet, ob die Daten auch innerhalb des Landesamtes für Soziales und Versorgung vor dem Zugriff Unbefugter geschützt sind. Positiv möchte ich vermerken, daß sämtliche Schriftstücke in diesem Zusammenhang ungeöffnet der zuständigen Sachbearbeiterin vorgelegt werden. Den Beratungsstellen hat das Landesamt Formularanträge mit der genauen Adressierung (zuständige Sachbearbeiterin) zur Verfügung gestellt.Ein Punkt ist mir allerdings aufgefallen, der aus datenschutzrechtlicher Sicht dringend verbesserungsbe-

dürftig ist. Neben dem eigentlichen Antrag übersenden die Beratungsstellen einen sogenannten Kurzantrag mit den Personalien der Antragtellerin per Telefax. Nach Darstellung des Landesamtes für Soziales und Versorgung ist eine Kostenzusage nur möglich, wenn der Antrag, zumindest in Kurzform, vor Durchführung des Abbruchs bei dem Amt eingegangen ist. Das Telefaxgerät, auf dem die Kurzanträge eingehen, steht im Vorzimmer des Amtsleiters; die sensiblen Dokumente werden in das offene Fach der zuständigen Sachbearbeiterin gelegt und dort einmal täglich abgeholt. Bei dieser Verfahrensweise scheint mir eine Kenntnisnahme durch unzuständige Mitarbeiter nicht ausgeschlossen. Dem Gebot zur Wahrung des Sozialgeheimnisses innerhalb des Sozialleistungsträgers (§ 35 Abs.1 Satz 2 SGB I) kann nur dadurch Rechnung getragen werden, daß ein weiteres Telefaxgerät angeschafft und im Büro der zuständigen Sachbearbeiterin aufgestellt wird. Angesichts der Sensibilität der Daten scheint mir diese Datensicherungsmaßnahme nicht außer Verhältnis zu den Anschaffungskosten für ein solches Gerät zu stehen.Für nicht erforderlich halte ich es, daß eine Kopie
des Personalausweises bei den Akten vorgehalten wird. Denn der Personalausweis enthält neben dem Lichtbild weitere Daten, die für die Antragsbearbeitung nicht erforderlich sind. Ich habe daher gefordert, daß die Kopie des Personalausweises vernichtet wird, wenn sich das Landesamt davon überzeugt hat, daß die Antragstellerin ihren Wohnsitz im Saarland hat. Auch bei persönlich vorsprechenden Antragstellerinnen begnügt sich das Landesamt mit einer Vorlage des Personalausweises und dem Vermerk in den Akten, daß der Personalausweis vorgelegen habe. Schließlich habe ich eine sicherere Unterbringung der Unterlagen in einem Stahlschrank und die Festlegung von Aufbewahrungsfristen für die Akten verlangt.

13. Schulen und Hochschulen13.1 Professoren auf dem PrüfstandDurch Presseveröffentlichungen habe ich erfahren, daß der ASTA (Allgemeiner Studierendenausschuß) der Universität des Saarlandes eine Fragebogenaktion zum Thema Qualität der Lehre plant. Mehrere tausend Studenten sollten Didaktik, Betreuung und Rahmenbedingungen der Vorlesung bewerten. So wurde beispielsweise gefragt, wie oft sich der Dozent/ die Dozentin vertreten lasse, ob die Lehrveranstaltung sorgfältig vorbereitet sei, ob sich der Dozent/ die Dozentin klar, verständlich und präzise ausdrücke, ob er/sie offen sei für Kritik oder Verbesserungsvorschläge. Zusätzlich konnten noch eigene Anregungen und Kommentare zur Vorlesung abgegeben werden. Die Ergebnisse der Befragung - ausgenommen etwaige unsachliche oder beleidigende Äußerungen von Studierenden - sollten in der ASTA-Zeitschrift veröffentlicht werden. Mit der Beurteilung von Lehrveranstaltungen entstehen
Informationen, die den Dozenten zugeordnet werden können; es handelt sich folglich um personenbezogene Daten. Jedermann hat einen Anspruch auf Schutz gegen die "unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten" (BVerfGE 65,1 ff, 43). Insbesondere kann das Verfügungsrecht über die Darstellung der eigenen Person berührt sein. Nicht zuletzt ist das wissenschaftliche Personal einem faktischen Zwang ausgesetzt, weil es sich einer Befragung durch die Studenten kaum entziehen kann. Beschränkungen durch zwangsweise Informationsverarbeitung bedürfen jedoch einer verfassungsmäßigen gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkung klar ergeben (BVerfGE a.a.O. 44). Mangels einer speziellen gesetzlichen Ermächtigung für eine solche Befragung war die Einwilligung der Dozen-

ten erforderlich. Ihre Verbindlichkeit setzt allerdings voraus, daß die Bedingungen der Befragung und Auswertung sowie die sonstigen Kautelen klar und verbindlich festgelegt und die Betroffenen umfassend - etwa in einem Merkblatt - über die Verfahrensweise unterrichtet wurden. Die Betroffenen müssen wissen, daß sie ihre Einwilligung mit Wirkung für die Zukunft widerrufen können (§ 4 SDSG). Der ASTA beabsichtigte, den Dozenten das Ergebnis des sie betreffenden Umfrageteils zuzuleiten. Diese Information sollte so rechtzeitig erfolgen, daß die Dozenten noch vor der Veröffentlichung von ihrem Widerrufsrecht Gebrauch machen können. Die Erhebungsbögen waren beim ASTA unter Verschluß zu halten und spätestens einen Monat nach Veröffentlichung des Umfrageergebnisses zu vernichten.Engegen einer Pressedarstellung (Saarbrücker Zeitung
vom 15.09.1994) habe ich nicht gefordert, daß die Erhebung nicht namensbezogen durchgeführt werden dürfe. Die Unterdrückung des Namens macht keinen Sinn, wenn die Durchführung der Befragung nur unter der Voraussetzung zulässig sein soll, daß die betroffenen Dozenten ihre Einwilligung geben. Transparenz des Verfahrens für die Betroffenen hat auch zur Folge, daß die Bewertungsergebnisse den Betroffenen zugeordnet werden können.13.2 LehrerbarometerSchüler eines Saarbrücker Gymnasiums hatten in einer
Befragung die Lehrer ihrer Schule mit Werten von eins bis zehn benotet und das Ergebnis in einer aus Anlaß des Abiturs erscheinenden "Abi-Zeitung" verbreitet. Die Saarbrücker Zeitung hat dies aufgegriffen und die

ersten fünfundzwanzig Lehrer der "Beliebheitsskala" mit Namen, Platzziffern und Noten veröffentlicht. Die presserechtlichen Fragen, die im Hinblick auf den Zeitungsbericht auftreten, müssen hier außer Betracht bleiben, da die Medien nicht in den Anwendungsbereich der Datenschutzgesetze fallen (§ 41 BDSG). Wie die Befragung im einzelnen durchgeführt wurde und welche Kriterien zugrunde gelegt wurden, ist nicht bekannt geworden. Es sollen allerdings nicht nur die Beliebtheit des Lehrers, sondern auch andere Maßstäbe - wie pädagogisches Engagement, Fachkompetenz und Einsatzbereitschaft - in die Befragung einbezogen und zu einer Gesamtbewertung zusammengefaßt worden sein. Eine gewisse Seriosität der Befragung könnte sich dem Außenstehenden sogar aufdrängen, weil die einzelnen Noten in der Skala bis auf zwei Stellen hinter dem Komma errechnet waren.Die Lehrer hatten - im Gegensatz zu der oben dargestellten Aktion bei der Universität - keine Chance, die Rahmenbedingungen der Befragung und die Grundlagen der Bewertung kennenzulernen, um dann selbst entscheiden zu können, ob sie in die Befragung einbezogen werden wollen (Einwilligungslösung). Persönlichkeitsrechte der betroffenen Lehrer sind insofern tangiert, als ihre personenbezogenen Daten verarbeitet und veröffentlicht wurden. Die Betroffenen konnten sich dieser Erhebung und Bewertung nicht entziehen; sie hatte deshalb Zwangscharakter. Angesichts der Verbreitung des Umfrageergebnisses, wie auch immer es zustande gekommen ist, fällt es schwer, dem Vorgang Harmlosigkeit zu bescheinigen.Lehrer, Schüler und Erziehungsberechtigten gestalten das "Leben der Schule" gemeinsam (§ 17 Abs. 1 Schulordnungsgesetz). Jeder Schüler ist verpflichtet, "die

Regeln des Zusammenlebens in der Schule einzuhalten" (§ 30 Abs. 4 SchoG). Im Konsens den Ausweg zu finden, müssen sich alle Beteiligten bemühen. Dies setzt Verfahrenstransparenz, für die die Schüler zu sorgen haben, voraus. Den Lehrern fällt der pädagogische Auftrag zu, Verständnis bei den Schülern für Toleranz und Fairneß zu wecken. 13.3 Datenschutzprüfung im BerufsbildungszentrumIn das Schulordnungsgesetz sind bei einer Novellierung vor einigen Jahren (vgl. 5. TB Tz. 6.1) Vorschriften über die Verarbeitung von Daten der Schüler und Erziehungsberechtigten eingefügt worden. Nähere Regelungen trifft die Verordnung vom 03.11.1986 (Amtsblatt Seite 990), der mehrere Anlagen beigefügt sind, die den höchstzulässigen Inhalt von Datenträgern (Schülerkartei, Klassenbuch usw.) festlegen. Das von ca. 1.500 Schülern besuchte technisch-gewerbliche Berufsbildungszentrum wurde überprüft.Konventionelle DatenverarbeitungIn den Klassenbüchern waren auch die Zeugnisnoten vermerkt, obwohl diese Daten nach der Verordnung nur in einer besonderen Zeugnisnotenübersicht erfaßt werden dürfen. Die Karteikarten der ehemaligen Schüler wurden nicht - wie in der o.a. Verordnung vorgeschrieben - getrennt von den akuellen Karten, sondern im gleichen Karteischrank aufbewahrt. Die Informationen über ehemalige Schüler werden weniger häufig benötigt; sie sollten insbesondere durch gesonderte Aufbewahrung dem Zugriff im normalen, täglichen Verwaltungsablauf entzogen werden. Die in der Verordnung festgelegten Aufbewahrungsfristen waren bei einigen Unterlagen weit überschritten.

Prüfungsakten, Prüfungsarbeiten und Klassenbücher sind fünf Jahre nach Entlassung des Schuljahrgangs zu vernichten - soweit die Unterlagen nach einem entsprechenden Anbieten nicht durch das zuständige Archiv übernommen werden. Da Aussonderungen bisher nicht stattgefunden haben, waren die Vorgänge seit Bestehen der jeweiligen Schulform, teilweise seit 1946, vorhanden. Das Bildungsministerium verweist darauf, daß die Verordnung nur eine Kann-Vorschrift und keine Verpflichtung zur Vernichtung enthält. Dennoch will das Ministerium "anregen, daß die Schule davon im Sinne einer regelmäßigen Aktenpflege auch Gebrauch macht und ihr Schriftgut nach Fristablauf - soweit keine Archivübernahme erfolgt - tatsächlich der Vernichtung zuführt". Die Kann-Vorschrift steht im Widerspruch zur höherrangigen Norm des Saarländischen Datenschutzgesetzes (§ 19 SDSG), nach der Daten zu löschen sind, wenn ihre Kenntnis für die speichernde Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist.PC-EinsatzDer Schulträger (Stadtverband Saarbrücken) hat dem Schulzentrum einen PC und ein Schulverwaltungsprogramm zur Verfügung gestellt, damit die Daten der Schüler, Erziehungsberechtigten und Lehrer automatisiert verarbeitet werden können. Das automatisierte Verfahren war weder von der datenverarbeitenden Stelle schriftlich freigegeben (§ 8 SDSG) noch waren technische und organisatorische Datensicherungsmaßnahmen getroffen, um den beim PC-Einsatz entstehenden, bereits vielfach beschriebenen Risiken zu begegnen (vgl. 10. TB Tz. 4). Außerdem war ein Erlaß des Bildungsministeriums aus dem Jahre 1988, der unter anderem die Verwendung einer geeigneten Datensicherungssoftware vorschreibt, nicht beachtet worden. Auch beim Einsatz eines PC in der Schule ist ein Mindestmaß an Funktionstrennung zu verwirklichen. So sind Betriebssystem, die Datensiche-

rungssoftware und die freigegebenen Anwendungen von einem Systemverwalter zu installieren und zu betreuen, der nicht gleichzeitig Anwender sein darf. Das Ministerium hat sich zwischenzeitlich bereit erklärt, die Freigabe des Verfahrens, das in mehreren beruflichen Schulen eingesetzt werden soll, in die Wege zu leiten und dazu auch eine Dienstanweisung zu erlassen.Personalnebenakten der LehrerDie Schulleitung führt über jeden Lehrer eine Personalnebenakte. In diesen zum Teil jahrzehntealten und deshalb häufig recht umfangreichen Vorgängen sind insbesondere abgeheftet: Personalbogen mit Paßfoto, Kopien der beamtenrechtlichen Entscheidungen des Ministeriums wie Einstellung, Ernennungen, Beförderungen, Genehmigungen nebenamtlichen Unterrichts, Dienstreisegenehmigungen; Bewerbungsschreiben, Lehrproben mit Beurteilung bei Stellenausschreibungen; Berichte über Unterrichtsbesuche des Schulleiters einschließlich Unterrichtsvorbereitung; Jubiläumsmitteilungen, Anträge auf Dienstbefreiung. Die Akten werden bis zum Ausscheiden des Lehrers aus dem Dienst aufbewahrt und dann vernichtet. Bei Versetzungen werden die Unterlagen an die dann zuständige Schule weitergeleitet. Personalnebenakten dienen nicht wie die - im Ministerium geführte - Personal(haupt)akten der Dokumentation aller das Dienstverhältnis betreffenden Vorgänge. Sie dürfen nur solche Unterlagen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerfüllung der Schule erforderlich ist (vgl. § 56 Abs. 2 Satz 3 BRRG). Personalnebenakten dürfen daher kein Spiegelbild der eigentlichen Personalakte sein; ihr Inhalt muß sich darauf beschränken, was zur Wahrnehmung von Vorgesetztenfunktionen unerläßlich ist. Der Erforderlichkeitsgrundsatz gebie-

tet es zudem, daß - im Gegensatz zur Personalakte - Unterlagen, die "vor Ort" nicht mehr benötigt werden, etwa weil sie überholt sind, ausgesondert und vernichtet werden. Nur so kann gewährleistet werden, daß Vorgänge, die aus der Personalakte zu entfernen sind (z.B. Hinweise auf Disziplinarverfahren oder unbegründete Beschwerden) nicht noch in der Personalnebenakte vorgehalten werden. Der Personalbogen ist ständig zu aktualisieren und in seinem Umfang auf die tatsächlich notwendigen Angaben zu reduzieren. Um eine einheitliche Führung der Personalnebenakten in den Schulen sicherzustellen, sollte das Bildungsministerium den erforderlichen Inhalt der Akte und die Aussonderung nicht mehr benötigter Unterlagen durch Erlaß festlegen. Das Ministerium hat zugesagt, hierzu eine schulformübergreifende Regelung zu treffen. Ein Entwurf liegt bisher noch nicht vor. 13.4 Datenübermittlung an Berufsförderungsdienst der BundeswehrEin Soldat, dessen Fachausbildung durch die Bundeswehr gefördert wird, mußte feststellen, daß sich der Berufsförderungsdienst ohne sein Wissen bei der Schule über seine Leistungen erkundigte und diese Auskünfte auch erhielt. Meine Nachfrage bei der Fachschule ergab, daß der Berufsförderungsdienst in solchen Fällen Formblätter übersendet, in denen anzukreuzen ist, ob der Schulbesuch regelmäßig erfolgt, ob die Leistungen zufriedenstellend sind und ob die Erreichung des Ausbildungsziels gewährleistet oder gefährdet ist. Es soll nicht bezweifelt werden, daß solche Angaben zur Überprüfung der Leistung benötigt werden. Sie dürfen jedoch nicht über den Kopf des Betroffenen hinweg unmittelbar bei der Ausbildungsstätte erfragt

werden. Personenbezogene Daten sind grundsätzlich beim Betroffenen, mit seiner Kenntnis zu erheben (§ 12 Abs. 1 SDSG, § 13 Abs. 2 BDSG). Es war ein wichtiges Anliegen des Bundesverfassungsgerichts in seinem Urteil zum Volkszählungsgesetz, daß der Bürger wissen soll, wer was wann über ihn an Daten sammelt, speichert und verarbeitet. Der Auszubildende kann als mündiger Bürger ohne weiteres selbst durch Vorlage von Schulbescheinigungen dem Berufsförderungsdienst die notwendigen Nachweise liefern. Er kann dann auch reagieren, in dem er zum Beispiel seine Anstrengungen verstärkt, oder darlegt, aus welchen Gründen die Leistungen unzureichend sind. Ich habe in der Angelegenheit Kontakt mit dem Bundes-
beauftragten für den Datenschutz aufgenommen, weil dieser für die Datenschutzkontrolle bei der Bundeswehr zuständig ist. Das Bundesverteidigungsministerium hat daraufhin den Fall zum Anlaß genommen, die zuständigen Stellen seines Geschäftsbereichs nochmals darauf hinzuweisen, daß die Betroffenen verpflichtet seien, selbst die erforderlichen Nachweise beizubringen. Meine spätere Rückfrage bei der Fachschule hat jedoch
ergeben, daß sich an der Verfahrensweise des Berufsförderungsdienstes bisher nichts geändert hat. Es scheint nicht einfach zu sein, eine eingefahrene Verwaltungspraxis zu ändern. Die Schule beantwortet allerdings die Anfragen nicht mehr.13.5 Einsatz von Tonbandgeräten bei PrüfungenBeim mündlichen Teil der Heilpraktikerüberprüfung, die das Gesundheitsamt Saarbrücken zentral für das Saarland durchführt, werden die Fragen der Prüfer und die Antworten des Prüflings zu Protokollzwecken mit einem Tonbandgerät aufgezeichnet. Der Prüfling wird darüber

unterrichtet. Die Aufzeichnung wird im Falle des Widerspruchs gegen den Ablehnungsbescheid der zuständigen Behörde zur Fertigung einer Niederschrift verwendet. Tonbandaufzeichnungen stellen einen Eingriff in die Persönlichkeitsrechte dar, die ohne gesetzliche Grundlage nicht zulässig sind. Mangels solcher bereichsspezifischen Regelungen sind solche Aufzeichnungen nicht zulässig.Aber auch im übrigen begegnet die Informationsbeschaffung mit Hilfe technischer Mittel aus Anlaß einer Prüfung schwerwiegenden Bedenken. An die Protokollierung und Begründung von Prüfungsentscheidungen sind nach neuerer Rechtsprechung des Bundesverfassungsgerichts höhere Anforderungen zu stellen als bisher. Dies bedeutet jedoch nicht, daß die Protokollierungen lückenlos und in allen Einzelheiten erfolgen müssen. Unzureichende Protokollierungen können allenfalls Beweisnachteile im Falle einer Prüfungsanfechtung bringen. Diese sind jedoch angesichts der Nachteile, die dem Prüfling durch ein Tonbandmitschnitt entstehen, hinzunehmen. Das Bewußtsein, daß alle Äußerungen festgehalten werden, ist geeignet, psychologische Hemmnisse aufzubauen, die zu einem schlechteren Prüfungsergebnis führen können. Tonbandaufzeichnungen haben für das Verhalten der Betroffenen erhebliche Wirkungen, weil sie jede Nuance der Rede, einschließlich der rhetorischen Fehlleistungen, der sprachlichen Unzulänglichkeiten und der Gemütsbewegungen des Redners, dauerhaft und ständig reproduzierbar konservieren.Darüber hinaus ist die Speicherung der Artikulationsfähigkeit, des Sprachverhaltens und etwa der Wortwahl bei der Prüfung, bei der es um die Abfrage von Wissen und Kenntnisse geht, nicht erforderlich. Gerade bei

einer Heilpraktikerprüfung, die nur feststellen soll, ob vom Prüfling eine Gefahr für die Volksgesundheit ausgehen könnte, gehört die Beurteilung des persönlichen Auftretens und der Sprachgewandheit nicht zur Aufgabe der Prüfer.Keine Lösung würde es darstellen, die ausdrückliche
Einwilligung der Prüflinge einzuholen. Von einer wirklichen Freiwilligkeit kann keine Rede sein. Es entspricht der Lebenserfahrung, daß sich viele Kandidaten bei ihrer Entscheidung von der Sorge leiten lassen, die Nichteinwilligung könnte das Prüfungsergebnis negativ beeinflussen.

14. Öffentlicher Dienst14.1 Personalaktenrecht Das am 01.01.1993 in Kraft getretene Beamtenrechtsrahmengesetz hat mit der Neuordnung des Personalaktenrechts wichtige, bereichsspezifische, datenschutzrechtliche Regelungen getroffen (vgl. 14. TB Tz. 8.2.3). Inzwischen hat bereits die Mehrzahl der Bundesländer diese rahmenrechtlichen Bestimmungen in Landesrecht umgesetzt; in anderen Ländern sind Gesetzentwürfe in den parlamentarischen Beratungen. Im Saarland liegt ein Referentenentwurf vor. Der Entwurf folgt im wesentlichen den bundesrechtlichen Vorgaben. Ich habe in meiner Stellungnahme Vorschläge unterbreitet, die geeignet sind, im Interesse des Datenschutzes den durch das Rahmengesetz gegebenen Spielraum stärker zu nutzen. 14.2 BeihilfeNeue rechtliche SituationDie Beihilfebearbeitung bleibt ein Dauerthema in der Datenschutzdiskussion. Dies ist nicht verwunderlich, erhält doch der Dienstherr durch die bei der Beihilfestelle vorzulegenden Rechnungen für Arztbehandlung, Arzneimittel, medizinische Hilfsmittel, psychotherapeutische Behandlung Kenntnis von Krankheitsdaten, die bei sonstigen Arbeitnehmern nicht dem Arbeitgeber, sondern nur der Krankenkasse bekannt werden. Das zum 01.01.1993 in Kraft getretene Beamtenrechtsrahmengesetz bekräftigt die seit Jahren vertretene Forderung nach Abschottung der Beihilfestelle, um Interesenkollisionen zum Nachteil des Bediensteten in den Personalverwaltungen auszuschließen. Zusätzlich zu

der in der Beihilfeverordnung festgelegten Zweckbindung der Beihilfedaten, soll die Beihilfe in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden (§ 56 a BRRG). Nur Beschäftigte dieser Organisationseinheit dürfen Zugang zu Beihilfevorgängen erhalten. Die traditionelle Bearbeitung der Beihilfe in Personalabteilungen, -referaten oder -ämtern wird daher aufgegeben werden müssen. Übertragung der BeihilfebearbeitungDa vor allem kleinere Verwaltungen Schwierigkeiten
haben, die gesetzlich geforderte Abschottung der Beihilfe zu gewährleisten, sollte die Möglichkeit eingeräumt werden, die Bearbeitung an eine andere öffentliche Stelle abzugeben. Die Ruhegehaltskasse des Saarlandes wäre bereit, diese Aufgabe zu übernehmen. Das Ministerium des Innern lehnt es aus grundsätzlichen Erwägungen des Beamtenrechts ab, daß der Dienstherr derartige Aufgaben an eine andere juristische Person des öffentlichen Rechts mit für ihn befreiender Wirkung überträgt. Keine ministeriellen Bedenken bestehen, wenn die andere öffentliche Stelle lediglich die Berechnung durchführt. Wenn jedoch bei der Beihilfeberechnung außer Haus die Sachentscheidung im Organisationsbereich des Dienstherrn ohne ausreichende Abschottung verbleibt, ist aus der Sicht des Datenschutzes keine Verbesserung zu erkennen. In anderen Bundesländern sind beamtenrechtliche Bedenken, die einer datenschutzfreundlichen Beihilfebearbeitung im Wege stehen, nicht gesehen worden. So haben meines Wissens in Baden--Württemberg etwa 90 % der Kommunen die Beihilfegewährung an einen kommunalen Versorgungsverband übertragen.

PrüfungsfeststellungenBeihilfestellen habe ich aus unterschiedlichem Anlaß überprüft: Mehrfach wurde ich von Personalräten um eine Beurteilung gebeten; in einem Fall hat ein Arzt in einer Eingabe Sorgen eines Patienten vorgetragen; bei der LVA habe ich das Personalreferat bei der generellen Prüfung (vgl. Tz. 11.2) einbezogen.Im Vordergrund stand immer wieder die unzureichende organisatorische, personelle und räumliche Abschottung der Beihilfestelle. Es dürfte ohne weiteres einleuchten, daß die Probleme z.B. beim Medizinischen Dienst der Krankenversicherung wegen der geringen Größe dieser Organisationseinheit nicht innerhalb dieser Einrichtung gelöst werden können, sondern nur eine Verlagerung der Bearbeitung auf eine andere Stelle in Betracht kommen kann. Aber auch größeren Verwaltungen fällt es schwer, eine kollisionsfreie Abwicklung sicherzustellen. Bei der Universität erfolgt die Beihilfebearbeitung in der Personalabteilung zwar nicht im Zusammenhang mit der eigentlichen Personalsachbearbeitung, aber auch die Zuordnung zum Amt für Personalbezüge entspricht nicht den Anforderungen des Beamtenrechtsrahmengesetzes, das eine von der übrigen Personalverwaltung getrennte Bearbeitung für notwendig hält. Auch bei der LVA ist die Bearbeitung eng mit der Personalsachbearbeitung verflochten. Bei Verwaltungen dieser Größenordnung wird es keinen anderen Ausweg geben, als die Beihilfe organisatorisch vollständig aus dem Personalbereich herauszulösen. Dies bereitet Schwierigkeiten, so daß die externe Lösung immer stärker in das Blickfeld rückt.Darüber hinaus wurde bei einer Beihilfestelle festgestellt, daß die Vorgänge unbefristet aufbewahrt werden, obwohl eine Aussonderung nach fünf Jahren aufgrund des Rundschreibens des Ministeriums des Innern

zur Personalaktenführung möglich und nach den Löschungsvorschriften des SDSG (§ 19 Abs. 3) geboten ist. Ferner wurden nicht alle Belege dem Antragsteller mit dem Bescheid zurückgegeben. In den Akten fanden sich ärztliche Verordnungen für Hilfsmittel, Massagen, Krankengymnastik, ärztliche Bescheinigungen über die Anerkennung von Kuren und psychotherapeutischen Maßnahmen, ärztliche Schlußberichte von Kuren usw. Auch diese Unterlagen sind wie die übrigen Belege dem Antragsteller mit dem Bescheid zurückzugeben. 14.3 Information der kommunalen Vertretungsgremien bei

PersonaleinstellungenImmer wieder erhalte ich Anfragen aus dem kommunalen
Bereich, teils von Mitgliedern des Gemeinderates oder Kreistages, teils von der Verwaltung, welche Bewerberdaten bei Personaleinstellungen den Vertretungsgremien zur Verfügung zu stellen sind. Während bei den Kommunalverwaltungen zum Teil Unsicherheit darüber besteht, in welchem Umfange personenbezogene Daten weitergeleitet werden dürfen, fühlen sich die ehrenamtlichen Mitglieder der Entscheidungsgremien oftmals nur unzureichend informiert. Zuletzt hat sich ein Mitglied des Stadtverbandstages
an mich gewandt, nachdem die Stadtverbandsverwaltung dazu übergegangen ist, die persönlichen und beruflichen Daten der Bewerber nur noch den Fraktionsvorsitzenden zur Verfügung zu stellen und den übrigen Mitgliedern des Stadtverbandstages lediglich den Namen des zur Einstellung vorgeschlagenen Bewerbers mitzuteilen.Grundlage für die datenschutzrechtlichen Beurteilung ist das Saarländische Datenschutzgesetz (SDSG). Personenbezogene Daten dürfen von einer öffentlichen Stelle

an eine andere öffentliche Stelle übermittelt werden, wenn sie zur Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich sind (§ 14 SDSG). Für die Datenweitergabe innerhalb einer öffentlichen Stelle gelten die gleichen Anforderungen (§ 14 Abs. 5 SDSG). Ob die personenbezogenen Daten der Bewerber zur Aufgabenerfüllung des Stadtverbandstages oder -ausschusses erforderlich sind, richtet sich nach der kommunalverfassungsrechtlichen Zuständigkeitsregelung.Der Stadtverbandstag beschließt über alle Selbstverwaltungsangelegenheiten des Stadtverbandes (§ 208 KSVG). Dazu gehören auch die Personaleinstellungen. Der Stadtverbandspräsident hat die Einstellungen nach den Beschlüssen des Stadtverbandstages und des Stadtverbandsausschusses vorzunehmen (§ 213 Abs. 4 Satz 2 KSVG).Da nach diesen Vorschriften dem Stadtverbandstag oder -ausschuß die originäre Entscheidungsbefugnis bei Personaleinstellungen zusteht, sind ihm die zur Entscheidungsfindung erforderlichen Daten aller Bewerber zur Verfügung zu stellen. Eine Beschränkung auf solche Bewerber, die der Stadtverbandspräsident für geeignet hält, dürfte das Entscheidungsrecht des Stadtverbandstages in unzulässiger Weise einengen. Es dürfte allenfalls vertretbar sein, Daten von Bewerbern, die offensichtlich die Einstellungsvoraussetzungen nicht erfüllen, dem Gremium vorzuenthalten.Dagegen würde es eine unverhältnismäßige Belastung des Bewerbers darstellen, wenn dem zuständigen Beschlußgremium alle der Verwaltung vorliegenden personenbezogenen Daten der Bewerber übermittelt würden. Weiterzugeben sind lediglich die Angaben, die für die Entscheidungsfindung benötigt werden. Weil je nach Art der zu besetzenden Stelle mehr oder weniger Informationen über den Bewerber zur Entscheidungsfindung erforderlich sind, ist eine abschließende Aufzählung der Da-

ten, die zulässigerweise mitgeteilt werden dürfen, nicht möglich. So werden bei der Einstellung eines Bauingenieurs andere Daten benötigt als bei der einer Reinigungskraft. Vielfach kann auf die Übermittlung von Detailangaben, die für die Entscheidungsfindung nicht erforderlich sind, verzichtet werden; hierzu einige Beispiele- anstelle des genauen Geburtsdatums genügt das Alter,- Angabe des Wohnorts, nicht jedoch Straße und Hausnummer,- statt genauer Angabe des derzeitigen oder früheren Arbeitgebers nur die Branche, die Art des Unternehmens, des Gewerbe- oder Handwerksbetriebs,- anstelle der einzelnen Zeugnisnoten lediglich die Durchschnittsnote der relevanten Fächer.Zurückhaltung ist außerdem geboten bei Angaben über Lebensumstände, die eine "soziale Auswahl" ermöglichen (z.B. Angaben über Ehegatten, Familienangehörige, Sozialhilfebezug). Gesundheitsdaten dürfen, weil sie einen erheblichen Eingriff in die Intimsphäre darstellen, nicht mitgeteilt werden. Die Feststellung eines Arztes, daß der Bewerber für den Dienstposten geeignet ist, sollte ausreichen.Die Daten sind grundsätzlich allen Mitgliedern des zuständigen Beschlußgremiums zur Verfügung zu stellen. Eine Differenzierung beim Datenumfang nach Fraktionsvorsitzenden und anderen Mitgliedern des Stadtverbandstages dürfte kommunalverfassungsrechtlich allenfalls durch Regelung in der Geschäftsordnung im Sinne einer Selbstbindung in Betracht kommen.Die Mitglieder des Stadtverbandstages sind zur Verschwiegenheit verpflichtet (§§ 26, 206 KSVG). Sie dürfen die Angaben nur für Zwecke der Personalentscheidung verwenden. Um der Gefahr vorzubeugen, daß Unbefug-

te von Daten Kenntnis erlangen oder die Daten für andere Zwecke verwendet werden, ist zu empfehlen, die Sitzungsvorlagen mit der Aufschrift "Personalsache" zu versehen und darauf hinzuweisen, daß die Unterlagen mit Personalangaben nach Abschluß der Beratungen zu vernichten sind. Die Aufnahme einer entsprechenden Regelung in der Geschäftsordnung ist zu empfehlen.14.4 Weitergabe von BewerbungsunterlagenEin Gemeinderatsmitglied hat bei mir angefragt, ob es
rechtens sei, daß der Bürgermeister die Unterlagen mit allen personenbezogenen Daten von sechzehn Bewerbern für ein EDV-Aufgabengebiet ohne deren Kenntnis dem Amtsleiter einer anderen, größeren Kommunalverwaltung übermitteln dürfe, die nach Darstellung der Gemeindeverwaltung über die notwendige Fachkompetenz für die Beurteilung der Bewerberqualifikation verfüge. Die Datenübermittlung der Gemeinde war unzulässig.
Jeder Bewerber muß damit rechnen, daß seine Daten den für die Einstellungsentscheidung zuständigen Stellen der Einstellungsbehörde (Personalabteilung, Gemeinderat, Personalrat) zugehen. Der Bewerber muß sich jedoch auch darauf verlassen können, daß seine persönlichen Unterlagen, z.B. Lebenslauf, Schulzeugnisse und Zeugnisse früherer Arbeitgeber, nicht ohne seine Kenntnis einer am Einstellungsverfahren regelmäßig unbeteiligten Stelle überlassen werden. Soll eine andere Stelle, z.B. ein Gutachter oder Personalberater, beteiligt werden, ist die Einwilligung des Bewerbers einzuholen. Dieser kann sich dann entscheiden, ob er an seiner Bewerbung festhält oder sie zurückzieht, etwa weil er nicht wünscht, daß Dritte Kenntnis von seiner Bewerbung erhalten.

14.5 Freie Datenbankabfragen bei Personalverwaltungssystemen

Das Bildungsministerium beabsichtigt bereits seit Jahren, die Daten der Lehrer - vor allem für Zwecke der Einsatzplanung - automatisiert zu verarbeiten (vgl. 3. TB Tz. 5.1). Nachdem frühere Versionen nicht zum Einsatz kamen, ist nunmehr von einem externen Softwarehaus die Lehrerdatenbank LEDA entwickelt worden. Die Einsatzbedingungen für das Verfahren mit seinen vier Hauptdateien Lehrerstammdaten, Bewerberdatei, Einsatzdaten und Stellenplan werden in einer Dienstanweisung verbindlich festgelegt. In der Anlage zur Dienstanweisung werden auch die für die Aufgabenerfüllung erfahrungsgemäß benötigten "Standardauswertungen" der Datenbank beschrieben. Soweit ein nicht vorhersehbarer, dienstlicher Bedarf entsteht, den Datenbestand nach anderen Kriterien auszuwerten, ist dies unter besonderen, in der Dienstanweisung festzulegenden Sicherungen (z.B. Beteiligung der Personalvertretung) zulässig. Die Verwaltung hat unsere Vorgaben akzeptiert.

In zunehmendem Umfange werden in der Personalverwaltung Datenbanken eingesetzt, bei denen der Anwender nicht auf einen vorgegebenen Programmablauf festgelegt ist, sondern mit Hilfe "freier Abfragesprachen" die gespeicherten Daten selbst in beliebiger Weise nach unterschiedlichen Kriterien miteinander verknüpfen kann. Die Verfahren dienen häufig mehreren, unterschiedlichen Personalverwaltungszwecken; dementsprechend werden eine Vielzahl von Personaldaten benötigt. Es werden Systeme entwickelt, die eine Personalverwaltung ohne Personalakte in Papierform zum Ziel haben, bei denen nahezu alle Personaldaten eines Beschäftigten elektronisch gespeichert und damit für automati-

sierte Auswertungen verfügbar sind. Aus der Sicht des Datenschutzes stellt sich insbesondere die Frage, wie gewährleistet werden kann, daß bei solchen Datenbanksystemen die Personaldaten nur im zulässigen Umfange verarbeitet werden.Grundsätzlich sollte es dabei bleiben, daß die Auswertungsmöglichkeiten vor dem Einsatz eines Personalverwaltungsverfahrens festzulegen und dies durch Menüsteuerung und Bildschirmmasken sicherzustellen sind. Diese Konzeption entspricht den Regeln des Beamtenrechtsrahmengesetzes, nach der die Verarbeitungs- und Nutzungsformen zu dokumentieren und allgemein bekanntzugeben sind (§ 56f). Über den voraussehbaren, regelmäßig anfallenden Auswertungsbedarf hinaus kann eine Datenbankabfrage in eingeschränktem Umfange zugelassen werden, wenn die Verknüpfungsmöglichkeiten für den Betroffenen überschaubar sind und wenn durch technisch--organisatorische Maßnahmen gewährleistet werden kann, daß die Verarbeitung nur im zulässigen Rahmen erfolgt. Neben aufbauorganisatorischen Maßnahmen (z.B. Funktionstrennung und effektive EDV-Revision) sind weitere technische Maßnahmen zu treffen. Dabei kommen u.a. in Betracht:- Beschränkung der Abfrage auf genau definierte, "unkritische" Datenfelder;- aufgaben- und benutzerspezifische Beschränkung auf bestimmte Verknüpfungsmöglichkeiten; gegebenenfalls auf bestimmte Wertebereiche (z.B. nur bestimmte Besoldungsgruppen) oder bestimmte Trefferquoten (z.B. Ausgabe nur einer bestimmten Anzahl von Datensätzen);- ausreichende Protokollierung.

Ergebnisse mit personenbezogenen Daten sind nur zuzulassen, soweit anonymisierte oder aggregierte Angaben zur Erfüllung des jeweiligen Zwecks nicht ausreichen. Der Katalog der Standardauswertungen und die Kriterien für die Abfrage mit einer Datenbanksprache sollten in einer Dienstvereinbarung oder Dienstanweisung festgeschrieben werden. 14.6 Beurteilungen - mehr Transparenz durch Offenlegung der Notenskala?Der Hauptpersonalrat eines Ministeriums hatte vorgeschlagen, bei den regelmäßigen Beurteilungen die Verteilung der Noten innerhalb der jeweiligen Besoldungsgruppe als Statistik bekanntzugeben. Beurteilungen sollen dem einzelnen Beamten Gelegenheit geben, die Einschätzung durch den Dienstherrn kennenzulernen um das eigene Leistungsverhalten besser einordnen zu können. Da ein absoluter Maßstab fehlt, wird so dem Einzelnen transparent, wo er im Gesamtgefüge des Notenspektrums einzuordnen ist. Außerdem wird so nachvollziehbar, ob eine in den Beurteilungsrichtlinien vorgesehene Quotenregelung beachtet wurde. Transparenz der Datenverarbeitung ist ein wichtiges Datenschutzanliegen. Sie darf jedoch nicht so weit gehen, daß Informationen in personenbezogener Form über Kollegen offengelegt werden. Die Angaben in der Notenskala müssen ausreichend anonymisiert sein, d.h. es dürfen keine Rückschlüsse auf einzelne Beamte gezogen werden können. Bei Besoldungsgruppen, denen eine größere Anzahl von Beamten angehört, besteht regelmäßig keine Gefahr, daß der Notenspiegel einer Besoldungsgruppe die Identifizierung eines einzelnen Beamten ermöglicht. Bei Besoldungsgruppen, in der nur wenige Beamte vertreten sind, besteht allerdings die Gefahr der Deanonymisierung. In einem solchen Falle

sind gegebenenfalls mehrere Besoldungsgruppen (z.B. A15-A16) zu einer Rubrik zusammenzufassen, um die Anonymität der Notenangaben sicherzustellen.14.7 MitarbeiterbefragungEin Ministerium beabsichtigte, in Zusammenarbeit mit
dem Personalrat in seinem Geschäftsbereich eine Befragung der Mitarbeiter durchzuführen. So sollten unter anderem Aussagen zum Betriebsklima (Beispiel: wie ist das Zusammengehörigkeitsgefühl in Ihrer Abteilung?), zur Organisation, zur Ausstattung des Arbeitsplatzes, zur Qualität des Chefs (Beispiel: Wird Ihre Leistung vom Vorgesetzten anerkannt?) mit Noten von 1 (sehr gut) bis 5 (sehr schlecht) bewertet werden. Aufgrund des Befragungsergebnisses sollen u.a. auch Fragen der Organisation und des Informationsflusses analysiert werden.Ich habe gebeten, bei der Umfrage folgende Rahmenbedingungen zu beachten:- Die Teilnahme an der Befragung ist freiwillig. Die
Mitarbeiter sind auf die Freiwilligkeit ausdrücklich hinzuweisen.- In dem Fragebogen dürfen keine Angaben verlangt
werden, durch die die Mitarbeiter identifiziert werden können. Aus diesem Grunde ist u.a. die Angabe des Geschlechts weggelassen worden, weil sonst die Antworten in kleineren Organisationseinheiten in Kombination mit Altersangaben leicht bestimmten Personen zugeordnet werden könnten.- Die Durchführung der Befragung und die Auswertung
der Fragebogen erfolgt nicht - wie ursprünglich vorgesehen - durch das Ministerium selbst, sondern

durch eine fachlich geeignete, externe Stelle. Hierin ist eine zusätzliche Maßnahme zu sehen, die Anonymität zu gewährleisten. Der externen Stelle ist aufzuerlegen, dem Ministerium aufbereitete, aggregierte Ergebnisse zu liefern. Die Fragebögen selbst sollten beim Auftragnehmer verbleiben und dort - nach Abschluß der Auswertung - vernichtet werden. Es ist nunmehr beabsichtigt, das Statistische Landesamt mit der Durchführung zu beauftragen.- Die Einwilligung der von der Befragung betroffenen und identifizierbaren Vorgesetzten ist einzuholen, da eine Rechtsgrundlage für die Erhebung und Verarbeitung deren personenbezogener Daten nicht vorhanden ist. Beeinträchtigungen der Persönlichkeitsrechte von Vorgesetzten dürften auch durch die Beauftragung einer externen Stelle nicht auszuschließen sein. Es ist gerade auch ein Ziel der Untersuchung, Führungsschwächen aufzudecken. Die völlige Anonymisierung des Untersuchungsergebnisses ist deshalb weder erreichbar, noch nach Sinn und Zweck der Untersuchung beabsichtigt.

15. Defizite des präventiven, technischen Datenschutzes; Vorsorge geht vor Nachsorge

15.1 Charakterisierung der Situation

Die dezentrale Nutzung der Informationstechnik schreitet weiter fort. Neben der vorwiegend genutzten Textverarbeitung gewinnen auch arbeitsplatzspezifische Verfahren an Bedeutung, bei denen die öffentliche Verwaltung unter Nutzung spezifisch edv-technischer Möglichkeiten (Tabellenkalkulation, Datenbanken und sonstige Standardsoftware) versucht, die Arbeitseffizienz zu steigern und dem Leistungsdruck durch gestiegene Anforderungen und Personalreduzierungen zu begegnen. Beim Bemühen um Funktionsfähigkeit solcher Anwendungen werden teilweise vorhandene Richtlinien ignoriert und erforderliche Maßnahmen des Datenschutzes und der Datensicherung vernachlässigt (z. B. beim Haushaltsvollzugsverfahren des Ministeriums für Wirtschaft und Finanzen; siehe Tz. 15.3.8).

Hinzu kommt die zunehmende Integration von EDV-Arbeitsplätzen durch lokale Netzwerke, Anschlüsse an Telefonanlagen (TK-Anlagen) und Anbindung an übergreifende Netze für die "elektronische Post" (Electronic-Mail); zusätzliche Risiken und Gefährdungen bringen Zugriffe auf externe Datenbanken und Informationssysteme (z. B. Internet) in Verbindung mit neuen, in ständiger Fortentwicklung begriffenen Techniken (z. B. X25 und ISDN). Die Risiken werden schließlich noch größer, etwa durch die Absicht, die Betreuung und Wartung der EDV-Technik an Private zu vergeben (z. B. beim neuen TK-Anlagenverbund der Landesverwaltung; vgl. Tz. 15.3.6).

Diesen Risiken und Gefährdungen zu begegnen, auf die Durchsetzung geeigneter Maßnahmen zu drängen und deren Umsetzung zu begleiten, stellt auch für den Landesbe-

auftragten für Datenschutz eine permanente Herausforderung dar, die unter Berücksichtigung der vorhandenen, sehr beschränkten und der Entwicklung nicht angemessenen Ressourcen an Personal und Sachmitteln kaum zu bewältigen ist.15.2 Grundlegende Mängel15.2.1 Beteiligung des Landesbeauftragten für Datenschutz ein Element des vorbeugenden RechtsschutzesDen erstmaligen Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, sowie deren wesentliche Änderung hat die zuständige oberte Landesbehörde freizugeben. Im Interesse eines vorbeugenden Rechtsschutzes ist nach dem Saarländischen Datenschutzgesetz der Landesbeauftragte für Datenschutz vor der Freigabe von automatisierten Verfahren und demzufolge auch vor der Einrichtung von automatisierten Abrufverfahren zu hören (§ 8 Abs. 2 SDSG). Der Landesbeauftragte ist im übrigen über Planungen des Landes zum Aufbau automatisierter Informationssysteme rechtzeitig zu unterrichten, sofern in den Systemen personenbezogene Daten verarbeitet werden sollen (§ 22 Abs. 2 Satz 2 SDSG).Diese Beteiligungen setzen eine rechtzeitige Information und Einbeziehung in die Verfahrensentwicklung voraus. Es reicht nicht aus, kurzfristig vor dem Abschlußtest umfangreiche Unterlagen zu versenden. Ohne vorlaufende Terminabstimmung einzuladen - welches schon wiederholt vorgekommen ist - kann Sinn und Zweck der Anhörung nicht erfüllen. Unterlagen sollten wenigstens 4 Wochen vor dem Abschlußtest übersandt werden. Größere Projekte bedürfen einer Begleitung durch den Landesbeauftragten für Datenschutz schon zu einem früheren

Zeitpunkt, um noch eine angemessen Einbeziehung seiner Forderungen im Rahmen der Verfahrensentwicklung sicherstellen zu können.Zum Teil erfuhr ich erst aus Presseveröffentlichungen von der Inbetriebnahme von Verfahren, so daß meinen Forderungen, die aus einer datenschutzrechtlichen Prüfung hergeleitetet werden, erst nachträglich Rechnung getragen werden kann. Die aus der Sicht des Datenschutzes zu treffenden Maßnahmen und der daraus hergeleitete Bedarf an Hard- und Software muß schon bei der Beschaffung berücksichtigt werden. Eine ganzheitliche Betrachtungsweise durch rechtzeitige Integration der Anforderungen in ein Gesamtkonzept ist erforderlich, um teure Nachrüstungen und die bis dahin bestehenden Defizite vermeiden zu können. Es ist deshalb außerordentlich nachteilig für die Umsetzung des Datenschutzes im technischen Bereich, wenn ich erst aus Presseveröffentlichungen von der Inbetriebnahme von EDV-Verfahren und auotmatisierten Informationssystemen Kenntnis erhalte (z. B. das im folgenden geschilderte Verfahren "Immun" der Unikliniken des Saarlandes).15.2.2 Funktionstrennung und Kontrolle der Betriebssystem-, Anwendungssystem- und Netzadministration ein Element der VerfahrenssicherheitGerade im Rahmen von dezentralen Verfahren muß immer wieder auf das Risiko der mangelnden Funktionstrennung hingewiesen und die Berücksichtigung geeigneter Maßnahmen gefordert werden. Bei Einzelplatzsystemen, aber auch bei Mehrplatzsystemen unter UNIX ist häufig festzustellen, daß der Verfahrensentwickler gleichzeitig auch Systembetreuer und Anwender ist oder zumindest Betriebssystem- und Anwendungssystembetreuung in einer

Hand liegen (z. B. das später dargestellte Verfahren zum Haushaltsvollzug, Tz. 15.3.8). Die Zusammenfassung von Kenntnissen und Rechten in einer Hand birgt erhebliche Gefahren für die Persönlichkeitsrechte, weil unbefugte Kenntnisnahme und Manipulation erleichtert werden.Erschwerend kommt hinzu, daß die Standard-Betriebssysteme DOS, WINDOWS und UNIX nur unzureichende Kontrollfunktionen bieten, um die umfangreichen Befugnisse des Systemverwalters und der Netzadministration überwachen zu können. Hier habe ich verstärkt die Anwendung zusätzlicher Hard- und Softwareprodukte einschließlich einer geeigneten Protokollierung gefordert, die eine Überprüfung erleichtern. In besonderen Fällen - zum Schutz besonderer Amts- und Berufsgeheimnisse (z.B. Arzt- und Steuerdaten) - kann eine Kontrolle nur durch ein auf zwei Personen gesplittetes Paßwort und damit durch das Vier-Augen-Prinzip sichergestellt werden.In einigen Fällen sind meine Forderungen zur Funktions-
trennung und damit zur Aufteilung von Funktionen auf mehrere Personen auf Ablehnung gestoßen. Insbesondere die Universitätskliniken haben vorgetragen, daß die Personallage eine Verwirklichung nicht zulasse. Seit 1989 fordere ich eine entsprechende personelle Ausstattung. Der Ausschuß für Datenschutz im Landtag hat sich in seiner Sitzung vom 7. Juli 1992 ohne Erfolg für eine Finanzierung zweier zusätzlicher Planstellen für die Universitätskliniken im Landeshaushalt ausgesprochen. Auch neuerdings haben die Universitätskliniken die Funktionstrennung für das neu einzuführende System MediCare abgelehnt (vgl. oben Tz. 12.4). Die AOK hat die Funktionstrennung ebenfalls aus finanziellen Erwägungen - vor allem im Urlaubs- und Krankheitsfall - nicht vollständig verwirklicht. Es kann aber nicht mit Verweis auf einen unzureichenden Personalbestand eine

Erhöhung des Risikos durch mangelnde Funktionstrennung und damit eine Gefährdung des informationellen Selbstbestimmungsrechts betroffener Personen hingenommen werden. Wie ich schon in meinem 10. Tätigkeitsbericht 1989 (Lt-Drucksache 9/2075, Tz. 4.3.1 und Entschließung der DSB-Konferenz vom 10. Oktober 1988, Anlage 3) dargelegt habe, ist eine Informationsverarbeitung unzulässig, die eine notwendige und ausreichende Datensicherung vernachlässigt. Der dafür notwendige Finanz- und Personalbedarf ist von vornherein zu berücksichtigen. Es kann nicht akzeptiert werden, daß das zur Risikominimierung im Großrechnerbereich inzwischen in mühsamen Abstimmungen erreichte Sicherheitsniveau nun bei dezentralen Systemen und Verfahren mit Verweis auf nicht verfügbare personelle und sachliche Ressourcen unterschritten wird.15.2.3 Dienstanweisungen für den PC-Einsatz, eine

notwendige ArbeitshilfeObwohl 1992 ein Leitfaden für die Erstellung von

Dienstanweisungen erarbeitet wurde (GMBl. S. 462) mußte ich bei der Überprüfung einzelner Gemeinden, aber auch anderer öffentlicher Stellen feststellen, daß in vielen Fällen die technisch-organisatorischen Maßnahmen für den PC-Einsatz durch Dienstanweisung nicht oder nicht ausreichend geregelt waren. Im Interesse eines ordnungsgemäßen Ablaufs der Informationsverarbeitung, der Sicherstellung der Anforderungen des Datenschutzes und der ausreichenden Information der Mitarbeiter habe ich auf die Erstellung von Dienstanweisungen gedrungen. Ich werde diesen Gesichtspunkt bei der Prüfung von Dienststellen verstärkt berücksichtigen.

15.2.4 Schulung vor Einsatz der Informationstechnik am Arbeitsplatz; Unterrichtung tut not!Bei Datenschutzprüfungen vor Ort mußte ich gelegentlich feststellen, daß das Personal zwar in der Handhabung der Anwendungssoftware geschult, aber über die aus den Datenschutzanforderungen herrührenden Rahmenbedingungen, z. B. Paßwortnutzung, nicht informiert war. Die gesetzlich vorgeschriebene Unterrichtung hatte nicht oder nur eingeschränkt stattgefunden (§ 7 SDSG), so daß das Risikobewußtsein und die dadurch beeinflußte Bereitschaft zur Befolgung entsprechender Anweisungen noch zu wünschen übrig ließ.15.3 Besondere technische Probleme15.3.1 "elektronische Post" (Electronic Mail)Die Landesverwaltung betreibt ein einfaches Electronic-Mail-System zum Informationsaustausch im Rahmen der Pressearbeit der Landesregierung. Unter Nutzung herkömmlicher Telefonleitungen wird zwischen den Ressorts und mit den landeseigenen Dienststellen in Bonn und Brüssel eine Dateiübertragung vorgenommen, die das Bearbeiten der Texte gegenüber dem früherem Fax-Versand wesentlich erleichtert. Das Projekt soll auch auf die Bundesratsarbeit ausgedehnt und über Kopfstellen der Ressorts auch für andere Bereiche nutzbar gemacht werden. Dabei soll auch eine Ausweitung durch Beteiligung an einem Dokumentenaustausch zwischen Bundesrat und Landesvertretungen erfolgen. In einer dritten Phase ist eine Vernetzung der Leitungsbereiche der Staatskanzlei, des Ministeriums für Wissenschaft und Kultur und der Universität des Saarlandes vorgesehen, wobei auch eine Vernetzung über Internet erprobt werden soll.

Da nicht auszuschließen ist, daß auch Dateien mit personenbezogenen Daten ausgetauscht werden, habe ich darauf hingewiesen, daß bei solchen Übermittlungen über Electronic Mail besondere Schutzvorkehrungen zu treffen sind. Insbesonder könne durch eine Verschlüsselung der Daten mit ausreichend sicheren, kryptografischen Verfahren (mindestens DES-Algorithmus) eine angemessene Sicherheit, auch bei der Nutzung von Kopfstellen, erreicht werden. Dabei sollte eine Ende-zu--Ende-Verschlüsselung und ein sicherer Austausch der Schlüssel zwischen Absender und Empfänger selbstverständlich sein.Wie schon in meinem 14. Tätigkeitsbericht 1992 (Lt--
Drucksache 10/1403, Tz. 11.4) dargestellt, ist der Datenschutzaspekt ein "integrierender Bestandteil der Entwicklung; die Verträglichkeit mit dem Persönlichkeitsrecht ist von Anfang an durch geeignete Maßnahmen zu gewährleisten". Die Landesregierung hat in ihrer Stellungnahme dazu eine Berücksichtigung dieser Forderungen zugesichert und den Organisationserlaß im Oktober 1994 demgemäß geändert.15.3.2 Entsorgung von Adrema-PlattenAufgrund einer Anfrage einer Gemeinde wurde ich mit dem Problem konfrontiert, eine Vorschlag zur datenschutzgerechten Entsorgung alter, für den automatischen Adressendruck genutzer, sogenannter "Adrema-Platten" zu unterbreiten, die durch die inzwischen verbreiteten PC-Anwendungen schon seit längerer Zeit abgelöst wurden. Ich habe vorgeschlagen, diese Platten möglichst einzuschmelzen oder unter Berücksichtigung der Richtlinie des MdI vom 9.1.89 (GMBl vom 30.1.89, S. 2) und der durch die einschlägige DIN 32757 vorgegebenen Partikelgröße bei einer saarländischen Entsorgungsfirma schreddern zu lassen. Da dieses Problem bei anderen

saarländischen Gemeinden in ähnlicher Form auftreten dürfte, habe ich darüber auch den Saarländischen Städte- und Gemeindetag informiert.15.3.3 Optische DatenspeicherungDas Ministerium der Finanzen hat mit einem Projekt zur Speicherung von Daten der Kfz-Besteuerung auf optischen Datenträgern begonnen. Damit soll die aufwendige EDV-Druckausgabe und Verteilung der Kontenblätter auf die Kfz-Steuerstellen der Finanzämter ersetzt und dem Sachbearbeiter ein schneller Teminalzugriff auf die Daten ermöglicht werden. Weitere Anwendungen aus dem Gesundheits- und Sozialbereich zeichnen sich ab. So wurde ich vom Ministerium für Frauen, Arbeit, Gesundheit und Soziales um Stellungnahme zur optischen Datenspeicherung bei den Sozialversicherungsträgern gebeten. In Berlin, Niedersachsen und Sachsen-Anhalt wurden die Landesbeauftragten für den Datenschutz mit Anfragen und Projekten zur Speicherung von Patientenakten auf optischen Datenträgern befaßt. In einer hessischen Klinik wurde die optische Speicherung von Röntgenbildern getestet.Die saarländische Steuerverwaltung benutzt eine Speicherungstechnik mit Datenträgern, die nur einmal beschrieben, aber beliebig oft gelesen werden können (WORM-Technik). Mit Blick auf die gesetzlichen Anforderungen an die Datenlöschung stößt diese Technik auf erhebliche datenschutzrechtliche Bedenken. Das Saarländische Gesetz zum Schutz personenbezogener Daten schreibt vor, daß personenbezogene Daten zu löschen sind, "wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die speichernde Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist". Löschen ist "das Unkenntlichmachen gespeicherter Daten" (§ 3 Abs. 2

Ziff. 6 SDSG). Nach dem eindeutigen Wortsinn der gesetzlichen Vorschrift muß die Kenntnisnahme der Daten für jedermann, zu jederzeit tatsächlich unmöglich sein; d.h. die Daten sind physikalisch zu löschen. Diesen Anforderungen genügt die Löschung lediglich der Verweisdaten nicht.Bei die Worm-Technik werden folgende Verfahren zur
Löschung angeboten:- Löschung der Verweisdaten auf die optisch gespeicher-
ten Informationen mit der Folge, daß letztere phyikalisch erhalten bleiben.- Erstellen einer Kopie des optischen Datenträgers,
der die zu löschenden Daten nicht mehr enthält.Nur die letzte Alternative würde den Anforderungen
einer physikalischen Löschung genügen, wenn der ursprüngliche Datenträger ebenso unverzüglich vernichtet wird (Entfernen der Speicherfläche durch Ätzen, Zerstören des Datenträgers). Beim Zerstören der optischen Datenträger muß beachtet werden, daß die Speicherkapazitäten sehr groß sind; so können pro Quadratzentimeter bis zu 1000 Seiten DIN-A4 gespeichert sein. Es muß die Möglichkeit ins Kalkül gezogen werden, daß - auch unter Verwendung neuer Analysetechniken - eine Rekonstruktion erfolgen kann. Die Grundsätze der DIN 32757 (Vernichtung von Informationsträgern), die für Papier und Mikrofilm gelten, können nicht ohne weiteres übernommen werden.Ich habe das Ministerium für Wirtschaft und Finanzen
um Stellungnahme gebeten.

15.3.4 Elektronische Unterstützung bei der Dateimeldung

Das Saarländische Datenschutzgesetz schreibt vor, dem Landesbeauftragten für Datenschutz die Beschreibung der automatisiert geführten Dateien, in denen personenbezogene Daten gespeichert sind, mit den Angaben der Dateibeschreibung für ein dort zu führendes Dateienregister vorzulegen. Die Form dieser Meldungen wurde vom Ministerium des Innern in Verwaltungsvorschriften festgelegt (GMBl. 1993, S. 254 und 300). Zur Verfahrenserleichterung bei der Erstellung der Dateibeschreibungen habe ich für die verschiedenen, in der Landesverwaltung genutzten Textsysteme ein "elektronisches Formular" erstellt, das die Texte der Dateimeldung als Textbausteine (Formulare) enthält. Diese können die Anwender mit Hilfe ihres PC "abrufen" und je nach Sachlage mit den individuellen Angaben ergänzen. Gleichzeitig habe ich angeregt, den Behörden und sonstigen öffentlichen Stellen des Landes für die Verwaltung dieser Meldungen ein landeseinheitliches, PC-gestütztes Verfahren zur Verfügung zu stellen.

In diesem Zusammenhang ist aufgrund der Erkenntnisse verschiedener Datenschutzprüfungen vor Ort noch darauf hinzuweisen, daß meiner Dienststelle viele Ersteinrichtungen von Dateien zum Dateienregister noch nicht gemeldet oder es versäumt wurde, bei Änderung bestehender Verfahren die Dateimeldung zu aktualisieren. Die Behörden und öffentlichen Stellen sind aufgefordert, ihre Verfahren und Meldungen daraufhin zu überprüfen.

15.3.5 Projekt IMMUN bei den Unikliniken in Homburg

Das neue Kommunikationsnetz "IMMUN", dessen Inbetriebnahme ich im Oktober 1994 aus Pressemeldungen entneh-

men mußte, werde ich kritisch begleiten. Mit Hilfe dieses Netzes wurde eine neue Kommunikationsinfrastruktur aufgebaut, über "die Daten und Informationen, auch Text- und Bildinformationen ... dort zur Verfügung stehen, wo sie benötigt werden". (IMMUN, Antrag zur Erneuerung der Kommunikationsinfrastruktur, Uniklinik-en, Juni 1992). Das ärztliche und pflegerische Personal soll durch unmittelbare Zugriffsmöglichkeiten auf alle vorhandenen Patientendaten ... umfassend unterstützt werden". Wieweit bei diesem Kommunikationsnetz dem Datenschutz
Rechnung getragen wird, kann ich leider erst im Nachhinein prüfen, weil ich nicht rechtzeitig informiert wurde. Die Berücksichtigung meiner Forderungen könnte unter Umständen umfangreiche Änderungen zur Folge haben, die durch eine frühzeitige Einbeziehung meiner Dienststelle hätten vermieden werden können.15.3.6 Telekommunikations-Anlagenverbund der Landesverwaltung

Die Landesregierung hat sich inzwischen entschlossen,
den Telefonverkehr über einen Anlagenverbund abzuwickeln. Damit sollen die verschiedenen Ressorts und einige nachgeordnete Dienststellen unter einer einheitlichen, zentralen Rufnummer erreichbar sein. Gleichzeitig soll die Betreuung der Technik vereinheitlicht und die Vermittlung zentralisiert werden. Die Installationsarbeiten sind Ende des Jahres 1994 weitgehend abgeschlossen. Zu den Problemen der TK-Anlagen und den Gefahren für die Kommunikationsfreiheit und das "nicht öffentlich gesprochene Wort" berichtete ich bereits (mein 10. TB, Lt-Drucksache 10/1403, Tz. 11.3.1; mein 12. TB, Lt-Drucksache 10/1402, Tz. 9.1).

Aufgrund der weitreichenden und grundsätzlichen Konsequenzen aus dieser neuen Konzeption habe ich eine umfangreiche Überprüfung der zentralen Komponenten und Funktionen vorgenommen. Obwohl noch eine abschließende Stellungnahme meinerseits vorbereitet wird, in der weitergehende technisch-organisatorische Maßnahmen zur Sicherstellung des Datenschutzes zu fordern sind, kann jetzt schon auf die Problematik der Verlagerung von Dienstleistungsfunktionen auf Private aufmerksam gemacht werden. Die Landesregierung beabsichtigt, die umfangreichen
Arbeiten zur technischen Betreuung der Anlage (Systembetreuung, Konfiguration, Datensicherung, Wartung, Reparatur) auf Private zu verlagern und verzichtet auf die Bereitstellung eigenen, qualifizierten Personals. Lediglich für den Betrieb der Anlage (Zuteilung von Berechtigungen, Gebührenauswertung, Vermittlung) wird eigenes Personal vorgehalten, das zwar für diese Tätigkeiten eingewiesen und geschult wurde, jedoch über keine Kenntnisse verfügt, um die von Technikern des privaten Auftragnehmers vorgenommenen Handlungen kontrollieren zu können. Dabei ist eine mögliche Reaktivierung unzulässiger Leistungsmerkmale (z. B. Aufschalten ohne den zugehörigen Signalton) und ihre mißbräuchliche Nutzung ebenso riskant, wie eventuelle Zugriffe über die Betriebssystemebene auf die Verbindungs- und Gebührendaten, die derzeit nicht protokolliert werden können. Die unkontrollierte Implementation von Programmen ist ebenso möglich wie das unberechtigte Kopieren von Software- und Datenbeständen. Aus Kostengründen wird überdies erwogen, die Wartung über Fernzugriffe von einer außerhalb des Saarlandes gelegenen Wartungszentrale des Auftragnehmers durchzuführen. Durch entsprechende Vertragsklauseln wird der Auftragnehmer zwar verpflichtet, seine Mitarbeiter zu unterrichten und unzulässige Handlungen zu unterlassen. Dies ist jedoch keine ausreichende Vorsorgemaßnahme.

Der Betrieb einer TK-Anlage und insbesondere eines solch umfangreichen Anlagenverbundes - einbezogen sind mehrere Ressorts und nachgeordnete Behörden - kann nicht nur unter Kostengesichtspunkten gesehen werden. Der Anlagenbetreiber kann sich seiner Verantwortung für einen sicheren, datenschutzgerechten Betrieb nicht durch Delegation auf einen privaten Auftragnehmer entziehen. Der Schutz des Fernmeldegeheimnisses und des nicht-öffentlich gesprochenen Wortes der Bediensteten, aber auch das informationelle Selbstbestimmungsrecht Dritter, die anrufen oder angerufen werden, muß gewahrt werden. Die Verantwortung hierfür hat der Anlagenbetreiber als speichernde Stelle. Dazu muß er ausreichend qualifiziertes Personal in der benötigten Zahl bereitstellen, das auch in der Lage ist, wichtige Funktionen beim Betrieb der Anlagen selbst wahrzunehmen und die Aktivitäten von externen Dienstleistern zu überwachen. Eine rein vertragliche Verhinderung unzulässiger Handlungen ist nicht ausreichend.15.3.7 Unbefugte PC-Nutzung bei einer GemeindeDurch einen Petenten wurde ich darauf aufmerksam gemacht, daß bei einer Gemeinde ein Verwaltungsfremder auf der Ebene des Systemverwalters prinzipiell Zugang zu allen Daten auf einem Personal Computer gehabt hatte, der für die Datenverarbeitung eines Eigenbetriebes eingesetzt wurde. Meine Überprüfungen vor Ort bestätigten diese Vermutungen. Auf dem Computer waren u.a. auch Personaldaten gespeichert. Außerhalb der Dienstzeit sollte aus Geheimhaltungsgründen im Rahmen der Umstrukturierung der Verwaltungsorganisation der Gemeinde ein neues Organigramm erstellt werden.Das Systemverwalterpaßwort eröffnet Möglichkeiten in der Nutzung aller Daten und Programme. Die Einräumung

einer solchen Befugnis ist - gleichgültig, ob diese in vollem Umfang genutzt wurde - mit Datenschutzgrundsätzen nicht vereinbar. Um zukünftig alle Risiken aus einer solchen arbeitsplatzbezogenen Datenverarbeitung weitgehend ausschließen zu können, habe ich die Gemeinde aufgefordert, auf der Basis des "Leitfadens für die Erstellung von Dienstanweisungen für dem PC-Einsatz (siehe Kapitel 15) eine Dienstanweisung zu erstellen und zur Prüfung vorzulegen. Diese Dienstanweisung sollte die gesamte Datenverarbeitung der Gemeindeverwaltung umfassend regeln. Bis zur Umsetzung der dort festgelegten Regelungen habe ich besondere Sicherungsmaßnahmen auf dem Einzelplatz-PC und den Ausschluß einer Nutzung durch Verwaltungsfremde gefordert.15.3.8 Neues Haushaltsvollzugsverfahren auf UNIX-Plattformen Das Ministerium für Wirtschaft und Finanzen beabsichtigt eine selbstentwickelte, landeseinheitliche Verfahrenslösung zum Haushaltsvollzug zu Beginn des Jahres 1995 in Betrieb zu nehmen. Mit Hilfe von Arbeitsplatzrechnern als Terminals wird auf die Verfahrensteile "Mittelverteilung, Mittelbewirtschaftung, Zahlung und Buchführung" auf ressortspezifischen Server-Rechnern zugegriffen. Zahlungsdaten werden ohne zahlungsbegründende Unterlagen über ein Datenaustauschverfahren von der Landeshauptkasse abgerufen und in das dort auf Großrechner betriebene Verfahren für das Haushalts--Kassen-Rechnungswesen integriert. Ein Personenbezug der in diesem Verfahren bearbeiteten Daten kann z.B. durch die Verwendung der Personalnummer der Bediensteten des Landes in Verbindung mit dem Bezügeverfahren zur Erstattung der Reisekosten herge-

stellt werden. Im Zahlungsverkehr werden regelmäßig Adressen der Zahlungsempfänger verwendet. Bei der Bearbeitung von Zuschüssen und Subventionen können Hinweise auf wirtschaftliche Verhältnisse einbezogen sein.Das Verfahren wurde offensichtlich unter hohem Zeitdruck und ohne Beachtung der Projektrichtlinien vom 30.10.87 (GMBl. vom 30.11.87, S. 346) realisiert. Zur Beurteilung lag lediglich eine Anwenderbeschreibung und eine technische Kurzbeschreibung vor; insbesondere fehlte die detaillierte Ausgestaltung der Maßnahmen für Verfahrenssicherheit und den Datenschutz" (Tz. 4.4.1, lit. g der Projektrichtlinie). In Anbetracht der besonderen Bedeutung der Anwendung
für eine Verbesserung des Verwaltungsvollzugs und des Zwanges einer Verfahrenseinführung, die sich an dem Beginn eines Haushaltsjahres zu orientieren hat, habe ich mich bemüht, die notwendigen Details auch in bilateralen Gesprächen mit den verschiedenen Beteiligten in Erfahrung zu bringen und noch rechtzeitig in die Umsetzung einzubringen. Ausreichende technisch-organisatorische Maßnahmen zur Sicherstellung des Datenschutzes und ihre verbindliche Regelung in einer Dienstanweisung stehen noch aus; das Ministerium der Finanzen sieht die Veranwortung hierfür bei den Ressorts, von denen mir bisher noch keine konkreten Vorlagen zur Verfügung gestellt werden konnten. Eine Stellungnahme auf meine inzwischen vorgelegten
Forderungen, die vor der Inbetriebnahme des Verfahrens umzusetzen sind, stand ebenfalls bei Redaktionsschluß noch aus.

15.3.9 Anforderungen an den Einsatz tragbarer ComputerAufgrund der Miniaturisierung und der leistungsfähigen
Hard- und Software nimmt der Einsatz tragbarer Computer (Laptop, Notebook, Palmtop, Pentop, PDA) immer mehr zu. Konkrete Einsatzfälle habe ich beim Beratungsdienst der Landesversicherungsanstalt (s.o. Tz. 11.2), beim Projekt "Medicare" der Unikliniken und bei der Automation der steuerlichen Betriebsprüfung kontrolliert. Da diese Geräte auch außerhalb dienstlicher Räume eingesetzt werden, wachsen die aus einem eventuellen Diebstahl oder Verlust herrührenden Gefahren für die Sicherheit personenbezogener Daten. Der Einsatz tragbarer Computer für die Verarbeitung
personenbezogener Daten ist deshalb nur unter folgenden Rahmenbedingungen zulässig:Technische Maßnahmen:- Permanente Verschlüsselung der Daten und Paßwörter
mit zertifizierter Software auf internen und externen Datenträgern; ("online-Verschlüsselung", d.h.: Entschlüsseln beim Lesen, Verschlüsseln beim Schreiben, so daß auf Datenträgern Phasen ohne Verschlüsselung nicht entstehen);- Zugriff auf den PC nur nach Eingabe einer Benutzer-
kennung und eines Paßwortes; ausreichend sichere Paßwortregelungen (Länge der Paßworte mindestens 6 Zeichen, keine Trivialpaßworte, regelmäßige Änderung, Festlegung nur durch den Benutzer); Begrenzung der Zahl unzulässiger Zugriffsversuche;

- Zugriff auf Software und Daten nur über ein nach den jeweiligen Berechtigungen (z. B. Benutzer, lokaler Verwalter, Systembetreuung) abgestuften System;- Schutz des Diskettenlaufwerks und aller Schnittstellen gegen unzulässige Nutzung (Laden eines Betriebssystems, Kopieren von Software und Daten);- möglichst hardwareunterstützte Sicherungssysteme für Zugriff und Verschlüsselung zur Erhöhung der Sicherheit;- nicht-manipulierbare Protokollierung wichtiger Aktivitäten einschließlich gescheiterter Zugriffsversuche und Auswertung der Protokolle durch besonders dafür Beauftragte; ausreichend kurze Kontrollzeiträume und angemessene Löschungsfristen für die Protokolldaten;- Ausschluß des Zugriffs auf die Betriebssystemebene durch den Benutzer;- Sicherung eines eventuell mit den PC durchzuführenden, externen Zugriffs auf Daten durch eindeutige Identifizierung der Kommunikationspartner, Verschlüsselung des Datenverkehrs bei besonders sensiblen, personenbezogenen Daten und automatische Abschaltung der Verbindung und des Verfahrens bei ausbleibender Nutzung.Organisatorische Maßnahmen:- Beschaffung von Hard- und Software nach einheitlichen Gesichtspunkten;- zentral organisierte Geräte- und Datenträgerverwaltung;

- ausschließliche Nutzung dienstlicher Geräte, Programme, Daten und Datenträger (keine dienstliche Nutzung privater PC);- Befugte Zugriffe und Datenverarbeitung nur innerhalb festgelegter Zuständigkeiten;- Regelung der Datensicherung und der Aufbewahrung der zugehörigen Datenträger;- sichere Aufbewahrung, Löschung und Vernichtung von Datenträgern allgemein;- möglichst eindeutige Zuordnung von Geräten zu Benutzern;- Überprüfung zurückgegebener Geräte auf einwandfreien Zustand, dabei auch Virenprüfung und Löschen aller benutzerspezifischen Daten;- Wegschließen der Geräte bei Nichtbenutzung;- Einsatz von Software nur nach Freigabe;- Funktionstrennung zwischen Systembetreuung, Programmierung, Anwendungsbetreuung und Betrieb und klare Beschreibung der jeweiligen Funktionen;- unverzügliche Löschung personenbezogener Daten, wenn ihre Speicherung unzulässig oder ihre Kenntnis für die speichernde Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist;- Auftragsdatenverarbeitung (z.B. Entwicklung, Betreuung, Wartung, Reparatur, Entsorgung), soweit im Gesetz zugelassen;

- Regelung der PC-Nutzung durch eine Dienstanweisung vor Inbetriebnahme des Verfahrens.

16. Sonstige Bereiche16.1 Einholung eines Gutachtens für die Erteilung der
Fahrerlaubnis zur FahrgastbeförderungVoraussetzung für die Erteilung einer Fahrerlaubnis
zur Fahrgastbeförderung ist unter anderem der Nachweis der geistigen und körperlichen Eignung des Führerscheinbewerbers (§ 15 e Abs. 3 StVZO). Dieser Nachweis kann regelmäßig erbracht werden- durch das Zeugnis eines Amtsarztes oder eines anderen in der Verordnung genannten Arztes (§ 15 e Abs. 3 a StVZO) oder- auf Verlangen der Führerscheinstelle durch ein fachärztliches Gutachten oder das Gutachten einer amtlich anerkannten medizinisch-psychologischen Untersuchungsstelle (§ 15 e Abs. 3 c StVZO).Das Ministerium für Umwelt, Energie und Verkehr hat
durch Erlaß geregelt, daß vor Erteilung der Fahrerlaubnis zur Fahrgastbeförderung stets das Gutachten einer amtlich anerkannten medizinisch-psychologischen Untersuchungsstelle (MPU) zu verlangen ist. Diese Weisung findet keine Gründe im Gesetz und steht nicht im Einklang mit der neueren Rechtsprechung des Bundesverfassungsgerichts.Die Behörde kann den Nachweis der geistigen und körperlichen Eignung durch Vorlage eines amtsärztlichen Zeugnisses, eines fachärztlichen Gutachtens oder durch die Vorlage eines Gutachtens einer amtlich anerkannten medizinisch-psychologischen Untersuchungsstelle (MPU--Gutachten) verlangen. Die Entscheidung, ob überhaupt ein Gutachten und gegebenenfalls welches Gutachten (MPU-Gutachten oder fachärztliches Gutachten) verlangt wird, ist in das Ermessen der Behörde gestellt. Eine

Vermutung für die Nichteignung zur Fahrgastbeförderung, die nur durch Vorlage eines MPU-Gutachtens widerlegt werden kann, besteht nicht. Da der Erlaß die Durchführung einer Einzelfallprüfung ausschließt, führt dies zum Nichtgebrauch des gesetzlich eingeräumten Ermessens und damit zu einem Ermessensfehlgebrauch der ausführenden Führerscheinbehörde. Nach der Rechtsprechung des Bundesverfassungsgerichtes (BVerfG, Beschluß vom 24.06.1993, NJW 1993, Seite 2365) ist indessen vor Anforderung eines MPU-Gutachtens stets zu prüfen, ob tatsächliche Feststellungen einen Eignungsmangel als naheliegend erscheinen lassen (Einzelfallprüfung) und gegebenenfalls ob Eignungszweifel nicht durch einen "schonenderen" Eingriff in das Persönlichkeitsrecht des einzelnen (also z.B. durch Vorlage eines fachärztlichen Gutachtens) behoben werden können (Grundsatz der Verhältnismäßigkeit). Dabei muß berücksichtigt werden, daß das von der Führerscheinstelle geforderte MPU-Gutachten die Erhebung höchstpersönlicher Befunde voraussetzt, die unter den Schutz des allgemeinen Persönlichkeitsrechts fallen. Das gilt nicht nur für den medizinischen, sondern im gesteigerten Maße auch für den psychologischen Teil der Untersuchung. So erforscht der Psychologe zunächst den Lebenslauf: Elternhaus, Ausbildung, Beruf, Familienstand, Kinder, besondere Krankheiten, Operationen, Alkohol, Rauchen, finanzielle Verhältnisse, Freizeitgestaltung. Sodann werden Ablauf und Ursachen etwaiger Gesetzesverstöße und die vom Betroffenen daraus gezogenen Lehren erörtert. Leistungsfähigkeit, Verhalten unter Leistungsdruck, Schnelligkeit und Genauigkeit der optischen Wahrnehmung, Reaktionsvermögen bei schnell wechselnden optischen und akustischen Signalen und Konzentration werden getestet. Diese Befunde stehen dem unantastbaren Bereich privater Lebensgestaltung noch näher als die rein medizinischen Feststellungen, die bei der geforderten Untersuchung zu erheben

sind. Die beim psychologischen Teil der Untersuchung ermittelten Befunde zum Charakter des Betroffenen berühren seine Selbstachtung ebenso wie sein gesellschaftliches Ansehen. Hinzu kommt, daß er die Einzelheiten in einer verhörähnlichen Situation offenlegen muß.Eingriffe in diesen hoch sensiblen Bereich dürfen nur vorgenommen werden, wenn alle sonstigen Mittel, die der Führerscheinstelle durch Gesetz zur Verfügung stehen, die Eignungsbedenken nicht auszuräumen vermögen.Das zuständige Ministerium hat es abgelehnt, seinen Erlaß entsprechend den Vorgaben des Bundesverfassungsgerichts abzuändern. 16.2 Bargeldloser Zahlungsverkehr - elektronische

Autobahngebühr

Moderne bargeldlose Zahlungsverfahren haben Vorteile, weil sich der Einkauf von Waren und Dienstleistungen reibungslos und leicht abwickeln läßt. Dieser Aspekt ist besonders wichtig für den Einzug von Autobahngebühren, die angesichts des wachsenden, europaweiten Verkehrs streckenbezogen erhoben werden sollen, um insbesondere die Lasten des Durchgangsverkehrs in stärkerem Maße auf die Benutzer und Verbraucher abwälzen zu können. Würden herkömmliche Mautstellen eingerichtet, würden sich - wie man dies in anderen europäischen Ballungszentren erleben kann - nachteilige Folgen für den Verkehrsfluß ergeben, die vermieden werden können, wenn die Gebühren ohne Fahrtunterbrechung erhoben werden.Bargeldlose Zahlungsverfahren bergen aber auch die Gefahr in sich, daß Reisewege, -ziele und -zeiten der

Reisenden aufgezeichnet werden und dadurch detaillierte Bewegungsbilder des Einzelnen entstehen, die nicht nur für Strafverfolgungsbehörden sondern auch für Finanzämter und die werbende Wirtschaft von Interesse sein können. Ein solches Ergebnis wäre mit der verfassungsrechtlich verbürgten Freizügigkeit nicht vereinbar. Eine solche Verfahrensweise ist um so mehr abzulehnen, als technische Alternativen bestehen, die weitaus bürgerfreundlicher sind. Es können - wie dies in skandinavischen Ländern bereits der Fall ist - Wertkartensysteme eingesetzt werden, bei denen im voraus bezahlt wird (Prepaid-Verfahren) und deshalb die Speicherung personenbezogener Daten regelmäßig nicht erforderlich ist. Die Datenschutzbeauftragten des Bundes und der Länder haben in ihrer Entschließung vom 26./27.10.1993 gefordert, daß grundsätzlich die "datenfreie Fahrt" gewährleistet sein muß (Anlage 11). Bei den zur Zeit in der Erprobung befindlichen Systemen sollen deshalb bei regelgerechter Straßenbenutzung grundsätzlich keine personenbezogenen Daten entstehen (Grundsatz der Anonymität).16.3 Anhörbogen für (Verkehrs-)OrdnungswidrigkeitenÜber den aus datenschutzrechtlicher Sicht zulässigen Datenumfang auf dem Anhörbogen für (Verkehrs-)Ordnungswidrigkeiten habe ich bereits ausführlich in meinem 6. Tätigkeitsbericht, Lt-Drucksache 8/1647, Tz. 5.3 berichtet. Bereits damals wurde Einigkeit mit dem Ministerium des Innern dahingehend erzielt, daß im Anhörbogen Daten zum Beruf, Arbeitgeber und Führerschein nicht mehr erhoben werden. Angaben zu den wirtschaftlichen Verhältnissen werden ebenfalls regelmäßig nicht

erhoben. Dem Betroffenen kann jedoch im Einzelfall freigestellt werden, wirtschaftliche Verhältnisse vorzutragen, die eine Verringerung des Bußgeldbetrages zur Folge haben können. Durch eine entsprechende Gestaltung muß jedoch für den Betroffenen eindeutig ersichtlich sein, bei welchen Fragen eine Auskunftspflicht besteht und welche auf freiwilliger Basis erhoben werden.Durch eine Eingabe mußte ich feststellen, daß immer
noch Anhörbogen verwendet werden, die diesen Erfordernissen nicht Rechnung tragen. So erhielt der Petent einen Anhörbogen, der die Erhebung von Beruf und Arbeitgeber zwingend vorsah. Ich habe daraufhin bei allen Ressorts eine datenschutzgerechte Gestaltung - auch für den nachgeordneten Bereich - gefordert. Dabei stellte sich heraus, daß noch mehrere Behörden Anhörbögen benutzen, die nicht erforderliche Datenerhebungen vorsehen. Nachdem eine Änderung - entsprechend den Vorgaben - zugesagt wurde, ist hoffentlich für die Zukunft eine datenschutzgerechte Erhebung gewährleistet, die die schutzwürdigen Belange der Betroffenen beachtet.16.4 Gesetz zur Änderung des Saarländischen Abfallgesetzes
In meinem 12. Tätigkeitsbericht (Lt-Drucksache 10/451, Tz. 9.2) und in meinem 14. Tätigkeitsbericht (Lt--Drucksache 10/1403, Tz. 4.3) habe ich über die Erstellung von Verzeichnissen kontaminationsverdächtiger Flächen in verschiedenen Landkreisen des Saarlandes berichtet. Ich hatte darauf hingewiesen, daß der Betrieb solcher Kataster eine normenklare, bereichspezifische gesetzliche Grundlage voraussetzt. Datenschutzrelevant sind derartige Verzeichnisse und Kataster deshalb, weil sie grundstücksbezogen sind und deshalb

regelmäßig mit nicht unverhältnismäßig hohem Aufwand den Eigentümern zugeordnet werden können. Bei den erfaßten Flächen besteht ein mehr oder weniger begründeter Kontaminationsverdacht, worin eine nicht unerhebliche Beeinträchtigung der betroffenen Eigentümer liegt, weil der Verkehrswert des Grundstücks erheblich gemindert werden kann. Der betroffene Eigentümer hat diese Belastung nur hinzunehmen, wenn Erhebung und Bewertungsverfahren sowie die Verwertung, insbesondere die Erteilung von Auskünften im einzelnen gesetzlich geregelt sind.Im Berichtszeitraum ist das Saarländische Abfallgesetz
um Vorschriften über die Führung eines Katasters über Altablagerungen und Altstandorte beim Landesamt für Umweltschutz ergänzt worden (Gesetz vom 1. Juni 1994, ABl S. 982).Ich habe hinsichtlich der Grundkonzeption des Gesetzes aus datenschutzrechtlicher Sicht keine Bedenken angemeldet, jedoch die Ausräumung einiger Regelungsdefizite gefordert:- Art und Umfang der im Kataster zu speichernden Daten
  waren nicht hinreichend konkret und normenklar festgelegt. Ich habe daher vorgeschlagen, in das Gesetz eine Ermächtigung für den zuständigen Minister aufzunehmen, den Datensatz des Katasters durch Rechtsverordnung festzulegen. Eine eindeutige Normierung des Datensatzes ist unabdingbare Voraussetzung für die Rechtmäßigkeit des Katasters. Meiner Forderung wurde Rechnung getragen. - Wenn sich herausstellt, daß ein in das Kataster
  eingetragener Altstandort oder eine Altablagerung nicht mehr altlastenverdächtig ist, ist die gespeicherte Fläche zu löschen. Eine entsprechende Lö-

schungsverpflichtung wurde auf meine Anregung hin in das Gesetz aufgenommen.- Ein zentraler regelungsbedürftiger Punkt bei der Führung der Kataster sind die Auskunfts- und Einsichtsrechte Dritter. Es bedarf einer Abwägung zwischen den berechtigten Interessen der dritten Personen und den Belangen des Betroffenen. Nach der auf meine Anregung hin zustande gekommenen Formulierung wird Dritten Einsicht in das Kataster und Auskunft gewährt, soweit ein berechtigtes Interesse glaubhaft gemacht wird und keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Belange des Betroffenen beeinträchtigt werden. - Auf meinen Vorschlag hin wurde in das Gesetz die Verpflichtung der katasterführenden Behörde aufgenommen, den Eigentümer oder Nutzungsberechtigten über die Eintragung seines Grundstückes zu unterrichten. Die Unterrichtung der Betroffenen dient nicht nur der Transparenz der Informationsverarbeitung, sondern leistet auch einen wichtigen Beitrag für eine im Interesse des Umweltschutzes liegende faire Kooperation mit den Betroffenen. In das Saarländische Abfallgesetz wurde darüber hinaus eine Vorschrift aufgenommen, die es dem Kommunalen Abfallbeseitigungsverband erlaubt, bei Gewerbebetrieben, Eigenbetrieben der öffentlichen Hand und den öffentlichen Krankenhäusern Angaben über das Abfallaufkommen zu statistischen Zwecken zu erheben (Gewerbeabfallkataster).Ich habe Bedenken erhoben, daß die auch vom Bundesverfassungsgericht postulierte Abschottung der Statistik und die Wahrung des Statistikgeheimnisses nicht gewährleistet ist, wenn das Gewerbeabfallkataster bei dem Kommunalen Abfallbeseitigungsverband geführt wird. Ich

habe deshalb dringend empfohlen, die Durchführung der Statistik bei dem in diesen Fragen erfahrenen Landesamt für Statistik zu belassen. Diese Institution ist bisher kraft Gesetzes für die Durchführung von Landesstatistiken zuständig (§ 3 LStatG). Nicht nur die Wahrung des Statistikgeheimnisses, sondern auch die Akzeptanz der Erhebung durch die Betriebe würde dadurch besser gewährleistet. Nicht zuletzt dürfte durch die Erstellung von Statistiken durch das Landesamt für Statistik ein nicht unerheblicher Synergieeffekt erreicht werden. Meine Bedenken wurden nicht berücksichtigt.16.5 Einkommensabhängige WohnungsbauförderungUm die Fehlbelegung von Sozialwohnungen zu verhindern, ist vorgesehen, die Wohnungsbauförderung umzustellen. Der Bauherr/Vermieter soll eine in ihrer Höhe feste Grundförderung erhalten, um Mieten am unteren Ende der ortsüblichen Vergleichsmiete zu ermöglichen. Daneben soll eine Zusatzförderung an den Vermieter gezahlt werden, deren Höhe vom Einkommen des Mieters abhängt. Die Zusatzförderung soll alle drei Jahre überprüft werden.Abgesehen davon, daß bei der Bewilligungsbehörde neue Datensammlungen über die regelmäßig zu überprüfenden Verhältnisse der Mieter entstehen, ist ein solches Förderungsmodell aus der Sicht des Datenschutzes vor allem deshalb problematisch, weil der Vermieter aus der Höhe der Zusatzförderung Rückschlüsse auf das jeweilige Einkommen des Mieters ziehen kann. Verringert z. B. die Bewilligungsbehörde die Zusatzförderung, so kann der Vermieter daraus schließen, in welchem Umfange sich das Einkommen seines Mieters erhöht hat.

Der Gesetzgeber hat sich über die datenschutzrechtlichen Bedenken hinweggesetzt und inzwischen im Wohnungsbauförderungsgesetz vom 6. Juni 1994 (BGBl I S. 1184) diese Informationsweitergabe der Bewilligungsstelle an den Vermieter legitimiert. Es wird darauf zu achten sein, daß bei der Umsetzung in die Praxis die schutzwürdigen Belange des betroffenen Mieters weitgehend berücksichtigt werden.16.6 Parlamentarische Anfrage und PersonaldatenschutzIn einer parlamentarischen Anfrage wurde die Landesregierung aufgefordert, über die Höhe der Gehälter und sonstigen geldwerten Leistungen der Geschäftsführer einer landeseigenen Gesellschaft des privaten Rechts Auskunft zu geben. Die Betroffenen hatten sich an mich gewandt, weil sie davon ausgehen mußten, daß diese vertraulichen Angaben bei einer Auskunftserteilung an den Landtag nicht geheim bleiben, sondern einem größeren Personenkreis bekannt würden.Das Informationsrecht des Parlaments gegenüber der Exekutive und auch das Fragerecht des einzelnen Abgeordneten ist verfassungsrechtlich begründet (so zum Beispiel hinsichtlich der Rechte der Untersuchungsausschüsse Art. 44 GG, Art. 79 SVerf). Das Fragerecht des Abgeordneten wird zwar im Grundgesetz nicht einmal erwähnt und in der Saarländischen Verfassung nur andeutungsweise angesprochen (Art. 76 Abs. 1 SVerf). Das Fragerecht des Abgeordneten hat indessen sein verfassungsrechtliches Fundament in den Aufgaben und Befugnissen, die die Verfassungen den Parlamenten zuweisen (Kontrolle der vollziehenden Gewalt Art. 65 Abs. 3 SVerf).In der Literatur wird eine Antwortverweigerung der Exekutive bereits dann für zulässig gehalten, wenn

dafür wichtige Gründe vorliegen (Maunz/Dürig, GG, Art. 43 Randnr. 8). Auskunftsverweigerungen mit dem lapidaren Hinweis auf den Datenschutz sind jedoch nicht gerechtfertigt. Das Recht auf informationelle Selbstbestimmung hat nicht schlechthin Vorrang gegenüber den Auskunftsbedürfnissen des Parlaments. Der Auffassung, daß das Individualrecht auf Datenschutz gegen dem "einfachen" Auskunftsrecht des Parlaments stets Vorrang habe und deshalb eine Beantwortung unter Preisgabe personenbezogener Daten nicht in Betracht komme, kann ebenfalls nicht gefolgt werden (Burkholz Verwaltungsarchiv 1993, 203, 225). Zu Unrecht wird dem Fragerecht im Vergleich mit der Einrichtung des Untersuchungsausschusses eine geringere verfassungsrechtliche Bedeutung zugewiesen. Beide Institutionen fußen auf dem Kontrollrecht des Parlaments gegenüber der Exekutive. An die Ablehnungsbegründung des Auskunftsverlangens eines Abgeordneten sind deshalb gegebenenfalls qualifizierte Anforderungen zu stellen.Nähere Regelungen, wie die parlamentarische Anfrage
ausgeübt werden soll, insbesondere wie Konflikte zu lösen sind, wenn Individualrechte Betroffener entgegenstehen, enthält allerdings weder das Grundgesetz noch die Saarländische Verfassung. Bis zum Erlaß möglichst bestimmter Vorschriften - wie dies im Hamburgischen Datenschutzgesetz und in neueren Landesverfassungen bereits geschehen ist - muß ein Ausgleich zwischen der parlamentarischen Kontrollfunktion durch Ausübung des Fragerechts einerseits und dem Schutz des Persönlichkeitsrechts andererseits gefunden werden, der beide Verfassungspositionen soweit wie möglich zur Geltung kommen läßt. Die Güterabwägung hat die Sensibilität der mitzuteilenden, personenbezogenen Angaben und die Bedeutung gerade dieser Daten für die Klärung politischer Fragen ebenso zu berücksichtigen wie die Form der Erörterung und Offenbarung im Parlament.

Zwar ist im Interesse des Personaldatenschutzes immer eine Anonymisierung der Angaben anzustreben. Wenn jedoch die persönlichen und sachlichen Verhältnisse untrennbar mit dem Gegenstand der Untersuchung verknüpft sind, kann die generelle Eignung der Bekanntgabe dieser Daten zur wirksamen Wahrnehmung der parlamentarischen Kontrollfunktion nicht in Frage gestellt werden. Eine unübersteigbare Schranke besteht allenfalls für Informationen mit streng persönlichem Charakter und für unzumutbare intime Angaben und Selbstbezichtigungen, zu denen Gehaltsdaten allerdings nicht zählen. Andererseits kann ein allgemeines, politisches Interesse die Offenbarung von Personaldaten nicht ohne weiteres rechtfertigen. Ein parlamentarisches und öffentliches Untersuchungs- und Kontrollinteresse, demgegenüber die Sensitivität der Gehälter als schutzbedürftige Angaben über die privaten Verhältnisse der Geschäftsführer an Gewicht verlieren, kann insbesondere dann entstehen, wenn tatsächliche Anhaltspunkte den Verdacht von Mißbrauch und "Unregelmäßigkeiten" in der Abwicklung der Geschäfte begründen. Tatsächliche Anhaltspunkte in dieser Hinsicht waren mir nicht ersichtlich. Meine Überlegungen bewegten sich auf rein rechtlich-theoretischer Ebene.Die organisatorisch-technischen Maßnahmen der Datensicherung sind ein wesentliches Moment des Datenschutzes. Das Bundesverfassungsgericht hat für die parlamentarischen Untersuchungsausschüsse die Notwendigkeit von hinreichenden Geheimschutzmaßnahmen ausdrücklich betont (BVerfGE 67, 100, 144; BVerfGE 71, 1, 47). Das Gericht hat im Zusammenhang mit der Entscheidung über das Volkszählungsgesetz auch herausgestellt, daß der Gesetzgeber mehr als früher auch organisatorische und verfahrensrechtliche Vorkehrungen zu treffen hat, welche der Gefahr der Verletzung der Persönlichkeitsrechte entgegenwirken (BVerfGE 65, 1, 44). Um einer unverhältnismäßigen Beeinträchtigung der Betroffenen

vorzubeugen, sollte die parlamentarische Anfrage - jedenfalls, wenn personenbezogene Angaben nach Abwägung der Interessen mitgeteilt werden müssen - nicht in einer Landtagsdrucksache veröffentlicht werden. Konfliktlösungsmechanismen sind bei der Behandlung der parlamentarischen Anfrage in Betracht zu ziehen, die eine schonende Verfahrensweise erlauben, um eine Abwägung der Interessenlage im Vorfeld öffentlicher Erörterungen zu gewährleisten. So wäre etwa an die Einrichtung eines Einigungsausschusses - wie bereits in Schleswig-Holstein praktiziert - zu denken.Die Bestimmung der Geschäftsordnung des Landtages des Saarlandes zum Fragerecht des Abgeordneten (§ 58) hat keine Außenwirkung (Art. 70 Abs. 1 SVerf) und kann deshalb keine Eingriffsermächtigung gegenüber den Betroffenen darstellen; sie regelt ausschließlich innere Angelegenheiten des Parlaments. Ein Regelungsbedarf hinsichtlich der Behandlung der parlamentarischen Anfrage ist seitens der Präsidentinnen und Präsidenten der Landtage anerkannt (70. Konferenz, Zeitschrift für Parlamentsfragen 1992, 573 ff.).16.7 Vereinbarungen zwischen Kommunen und PostZur Sicherung der Präsenz der Deutschen Bundespost (DBP) im ländlichen Raum hat die DBP Verhandlungen mit den Kommunen über die Verlegung von Hilfstätigkeiten zu kommunalen Aufgaben auf die Postämter aufgenommen. In größeren Gemeinden hätte dies für den Bürger den Vorteil, daß er statt des längeren Weges zur Gemeindeverwaltung nur das nahegelegene Postamt aufsuchen muß.Aus zwei Gemeinden wurden mir entsprechende Pläne bekannt. Gegen diese Vorhaben bestanden aus datenschutzrechtlicher Sicht keine grundsätzlichen Beden-

ken, sofern nur Hilfstätigkeiten übertragen werden. Bereichsspezifische Datenschutzbestimmungen dürfen nicht unterlaufen werden. Es kommen nur Tätigkeiten in Betracht, bei denen personenbezogene Daten geringerer Sensibilität anfallen. Im wesentlichen sollten Annahme-- und Ausgabetätigkeiten übernommen werden: Insbesondere sollten die Postämter Vordrucke (z. B. zur Ausstellung von Geburts-, Heirats- und Sterbeurkunden) und Anträge (z. B. zur Ausstellung eines Führerscheins) bereithalten und ausgefertigte Dokumente (z. B. Reisepaß) aushändigen. Dem Bürger muß jedoch durch entsprechende Hinweise bewußt gemacht werden, daß er den Service der Post nicht gezwungen ist, in Anspruch zu nehmen. Nur dann kann es hingenommen werden, daß Informationen über seine Person von einer an sich unzuständigen Stelle zur Kenntnis genommen werden. Der Bürger darf nicht gehindert sein, sich unmittelbar an die Gemeindeverwaltung zu wenden.Personenbezogene Daten, die der Post im Zusammenhang
mit Dienstleistungen für die Gemeinde bekannt werden, dürfen nicht für vom Erhebungszweck abweichende Zwecke - auch nicht die der Post - genutzt werden.Für die Bundespost als Bundesbehörde gilt das Bundes-
datenschutzgesetz, soweit sie jedoch Hilfsaufgaben für eine saarländische Gemeinde erledigt, ist das Saarländische Datenschutzgesetz maßgeblich. Insoweit hat sich die Poststelle der Kontrolle des Landesbeauftragten für Datenschutz zu unterwerfen, da es sich hier um eine Auftragsdatenverarbeitung nach dem Saarländischen Datenschutzgesetz handelt (§ 5).Die mir vorgelegten Vertragsentwürfe zwischen den
Kommunen und der Deutschen Bundespost waren in den angeführten Punkten ergänzungsbedürftig.

16.8 Datenschutzdefizite infolge der Privatisierung der Deutschen Bundespost POSTDIENSTDie Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung vom 26./27.10.1993 (Anlage 12) auf die Gefahren hingewiesen, die dem Datenschutz aus der sogenannten Postreform II erwachsen können. Nach der dazu erforderlichen Grundgesetzänderung (BGBl. I 1994, 2245) wurde durch das Postneuordnungsgesetz (BGBl. I 1994, 2325) die Deutsche Bundespost POSTDIENST in die Deutsche Post AG und die Deutsche Bundespost TELEKOM in die Deutsche Telekom AG umgewandelt. In einer weiteren Entschließung der Datenschutzbeauftragten vom 09./10.03.1994 (Anlage 13) wurde darauf aufmerksam gemacht, daß damit zwei staatliche Einrichtungen aufhören zu existieren, gegenüber denen sich der Bürger bisher unmittelbar auf das Post- und Fernmeldegeheimnis berufen konnte. Der Einzelne darf jedoch durch die Postreform keine Schlechterstellung seiner datenschutzrechtlichen Position erfahren. Im Postneuordnungsgesetz ist zwar durch eine Ergänzung des Bundesdatenschutzgesetzes (§ 2 Abs. 1) geregelt, daß die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen - jedenfalls solange sie ihre Monopolstellung behalten - als öffentliche Stellen des Bundes gelten und damit weiterhin der Kontrolle des Bundesbeauftragten für den Datenschutz unterliegen. Ab dem Jahre 1998 werden die öffentlichen Sprachtelefondienste der Mitgliedstaaten der Europäischen Union ihre Monopolstellung verlieren. Ab diesem Zeitpunkt dürfte die datenschutzrechtliche Behandlung der durch diese Stellen verarbeiteten personenbezogenen Informationen nach den weniger strengen Vorschriften für den privaten Bereich zu behandeln

sein. Durch die Privatisierung droht, der grundrechtliche Schutz des Post- und Fernmeldegeheimnisses in Verlust zu geraten.Zum Schutz von Individualrechten und des Post- und Fernmeldegeheimnisses muß auch in Zukunft das Post- und Telekommunikationswesen einer effektiven, unabhängigen Datenschutzkontrolle unterworfen bleiben. Es müssen bundesweit einheitliche Kriterien und Maßstäbe beachtet werden. Jeder Anschlußinhaber sollte selbst entscheiden dürfen, ob und gegebenenfalls wie seine Rufnummer auf Einzelentgeltnachweisen erscheint.In meinem 14. Tätigkeitsbericht (Lt-Drucksache 10/1403, Tz. 11.1) habe ich bereits dargelegt, daß es mit dem Verhältnismäßigkeitsgrundsatz nicht vereinbar ist, in jeder beliebigen strafgerichtlichen Ermittlung auf gespeicherte Verbindungsdaten zurückgreifen zu können. Insofern bedarf das Fernmeldeanlagengesetz (§ 12) einer grundlegenden, längst überfälligen, Überarbeitung, die der Gesetzgeber im Rahmen des Postneuordnungsgesetzes nicht in Angriff genommen hat.16.9 Europäische Richtlinie zum Datenschutz in ISDN

und in MobilfunknetzenUnionsweit sollen bereichsspezifische Regelungen für den Datenschutz in Telekommunikationsnetzen auf Grund eines geänderten Vorschlags für eine Richtlinie zum Datenschutz in digitalen Telekommunikationsnetzen (ISDN-Richtlinie) getroffen werden. Ich berichtete hiervon bereits in meinem 12. Tätigkeitsbericht (Lt-Drucksache 10/451, Tz. 1.2.1 und Anlage 7).Die Datenschutzbeauftragten des Bundes und der Länder haben in ihrer Entschließung vom 26./27.9.94 (Anlage 14) die Bundesregierung dazu aufgefordert, die deut-

sche Ratspräsidentschaft für eine zügige Verabschiedung der ISDN-Richtlinie zu nutzen. Da die Europäische Union die rechtlichen und technischen Voraussetzungen für die Liberalisierung der Telekommunikationsmärkte in weiten Bereichen bereits geschaffen hat, passen mehrere Mitgliedstaaten, darunter auch Deutschland, ihr nationales Telekommunikationsrecht den Vorgaben der EU an.Auch auf der Ebene des Gemeinschaftsrechts der EU ist dem Prinzip Geltung zu verschaffen, wonach für öffentliche und private Stellen gleiche Datenschutzregelungen zu gelten haben und die Verarbeitung personenbezogener Daten durch (private) Diensteanbieter nicht privilegiert werden darf.Das Datenschutzniveau wurde durch den geänderten Vorschlag zur ISDN-Richtlinie in einigen Punkten gegenüber dem ursprünglichen Entwurf deutlich gesenkt:- die Zweckentfremdung soll schon bei "berechtigten Interessen" der Verarbeiter zulässig sein; die Datenverarbeitung ist nicht mehr auf die Zwecke der Telekommunikation beschränkt;- das ausdrückliche Verbot, personenbezogene Daten nicht zur Erstellung elektronischer Profile der Teilnehmer zu nutzen, ist entfallen;- es ist nicht mehr untersagt, Inhaltsdaten nach Beendigung der Übertragung zu speichern;- die Regelung über die Garantie der Vertraulichkeit der Kommunikationsbeziehungen und -inhalte (Fernmeldegeheimnis) wurde gestrichen;

- zum Einzelgebührennachweis und zur Anrufweiterschaltung sind konkrete Vorgaben im Richtlinienentwurf nicht mehr enthalten.Die stärkere wirtschafts- und industriepolitische
Ausrichtung des geänderten Vorschlags zur ISDN-Richtlinie ist zu bedauern, die mit dem Hinweis auf das Subsidiaritätsprinzip begründet wird. Der rechtliche und technische Ausgestaltungsspielraum des nationalen Gesetzgebers wird betont. Das Ziel, datenschutzrechtliche Standards europaweit zu harmonisieren, wird dadurch zumindest erschwert, wenn nicht gar vereitelt.16.10 Integriertes Verwaltungs- und Kontrollsystem im Agrarsektor (InVeKoS)In meinem 14. Tätigkeitsbericht (Tz. 11.3.3) habe ich
mich bereits kritisch mit dem von der Europäischen Union (EU) eingeführten integrierten Verwaltungs- und Kontrollsystem "InVeKoS" auseinandergesetzt. Landwirte, die Beihilfen der EU in Anspruch nehmen wollen, müssen sämtliche von ihnen bewirtschafteten Flächen mit Angaben zur Nutzung, Größe und geographischen Lage angeben. Bestandteil des Konzepts ist die Kontrolle der angegebenen Nutzungsarten durch Fernerkundung (Satelliten- oder Luftbildaufnahmen). Zur Vermeidung unverhältnismäßiger Einschränkungen des informationellen Selbstbestimmungsrechts der betroffenen Landwirte hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 26./27.10.1993 (Anlage 15) die Beachtung von Mindestbedingungen gefordert.

Anlage 1

Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1994 - bei Stimmenthaltung Bayerns und in Abwesenheit Baden-Württembergs -

Situation des Datenschutzes "10 Jahre nach dem Volkszählungsurteil"Die Konferenz hat folgende Bestandsaufnahme zustimmend zur Kenntnis genommen.Nach Ablauf von über 10 Jahren seit der Verkündung des Urteils des Bundesverfassungsgerichtes zum Volkszählungsgesetz am 15. Dezember 1983 sieht sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder veranlaßt, eine Bestandsaufnahme der Situation vorzulegen, in der sich der Datenschutz derzeit befindet. Entwicklung nach dem Volkszählungsurteil:Bereits unmittelbar nach Inkrafttreten der Datenschutzgesetze in Bund und Ländern war die Frage heftig diskutiert worden, welchen Rang der Datenschutz gegenüber anderen Rechtsgütern habe. Befürwortern der Auffassung, dem Datenschutz komme Grundrechtsqualität zu, standen zurückhaltendere Stimmen gegenüber, die die Subsidiarität des Datenschutzes betonten.Das Volkszählungsurteil hat den Datenschutz zu einer elementaren Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten

freiheitlichen demokratischen Gemeinwesens erklärt und den Grundrechtscharakter der informationellen Selbstbestimmung festgeschrieben. Dieses Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Damit wurde klargestellt, daß der Datenschutz unter den Bedingungen der modernen Datenverarbeitung das zentrale Mittel zur Gestaltung der Informationsbeziehungen zwischen den Einzelnen und den Institutionen in Staat und Gesellschaft ist. Das Bundesverfassungsgericht hat seine Grundposition in der Zwischenzeit in einer Reihe weiterer Urteile eindrucksvoll bestätigt.Danach ist von dem verfassungsrechtlichen Grundsatz
auszugehen, daß die Entscheidung über die Preisgabe und Verwendung personenbezogener Daten zuallererst beim Betroffenen selbst liegt. Einschränkungen der individuellen Dispositionsfreiheit sind für die Rechts-- und Gesellschaftsordnung von so wesentlicher Bedeutung, daß sie nur auf einer gesetzlichen Grundlage zulässig sind. Wie mit personenbezogenen Daten umzugehen ist, darf weder administrativer Zeckmäßigkeit noch dem Markt überlassen bleiben, sondern ist im Gesetzgebungsverfahren, d.h. vor den Augen der Öffentlichkeit zu entscheiden.Bei der Regelung des Informationsumgangs ist von den
individuellen Freiheitsrechten auszugehen; doch darf und muß der Gesetzgeber selbstverständlich berücksichtigen, daß der Einzelne in vielfältiger Weise auf den Schutz und die Hilfe des Staates angewiesen ist und daß die Tätigkeit des Staates kontrollierbar sein muß. In gesetzlich klar vorgegebenen Fällen ist daher die Verwendung personenbezogener Daten auch ohne selbstbestimmte Mitwirkung des Betroffenen erforderlich.

Das Grundrechtsverständnis mit der Selbstbestimmung des Bürgers als Regelfall und ihre Einschränkung als Ausnahme ist allerdings keineswegs von allen Seiten als Selbstverständlichkeit akzeptiert worden: Nach 10 Jahren ist eine positive, aber auch eine kritische Bilanz zu ziehen.Nach der Entscheidung des Bundesverfassungsgerichts sind, wenn auch in vielen Fällen in langwierigen Verfahren, viele gesetzgeberische Aktivitäten entfaltet worden. Dabei mußte mancher datenschutzrechtlicher Fortschritt hart umkämpft werden.Neben einer grundlegenden Novellierung der Datenschutzgesetze in Bund und Ländern wurden Spezialbestimmungen in zahlreichen Sondermaterien geschaffen. Auf der Ebene des Bundes zählen dazu:- einzelne Bücher des Sozialgesetzbuches,- das Personalaktenrecht für Beamte,- das Straßenverkehrsrecht,- die Gesetze über die Nachrichtendienste des Bundes,- das Telekommunikationsrecht.Besonderer Handlungsbedarf für die Verwirklichung der informationellen Selbstbestimmung entstand durch die deutsche Einigung. Dabei stellt die Aufarbeitung der Hinterlassenschaft des Staatssicherheitsdienstes der ehemaligen DDR auch für den Datenschutz eine besondere Herausforderung dar.Noch weitergehend ist der Umfang der datenschutzrechtlichen Neuregelungen in den Ländern, in denen die Vorgaben des Bundesverfassungsgerichtes teilweise konsequenter umgesetzt wurden als im Bund.Diese Verrechtlichungswelle hat auch Kritik hervorgerufen:

In Dutzenden von Gesetzen ist nunmehr das "Kleingedruckte" des Rechts auf informationelle Selbstbestimmung bereichsspezifisch geregelt. Das so entstandene Normengeflecht ist engmaschig und kompliziert. Dies steht der Intention des Verfassungsgerichtes, der Bürger solle bereits aus normenklaren Gründen erkennen können, mit welcher Verarbeitung seiner Daten er zu rechnen hat, gelegentlich bereits entgegen. Eine weitergehende Kritik stellt in Frage, ob diese Normenflut mit ihren perfektionistischen und detaillistischen Regelungen der Verwirklichung des Grundsatzes der Verhältnismäßigkeit dient und notwendig war. Geäußert wurde auch die Annahme, daß die Effizienz der staatlichen Verwaltung bei der Bewältigung ihrer Aufgaben unter der Last perfektionistischer detaillistischer Regelungen gelitten habe und daß die Kreativität der Gesellschaft und ihre Fähigkeit zur Anpassung und Bewältigung der gegenwärtigen Herausforderungen durch enge, starre Gesetze behindert würden.Dem muß allerdings entgegen gehalten werden, daß die
Fülle und Kompliziertheit der Datenverarbeitung in den verschiedensten Verwaltungsbereichen für die Regelungsdichte verantwortlich ist. Sie ist eine Konsequenz des Umstands, daß in allen Verwaltungsbereichen der - zunehmend automatisierten - Informationsverarbeitung immer mehr Bedeutung zukommt: Eine notwendige Folge der Entwicklung hin zu "Informationsgesellschaft".Ein weiterer Grund für die Komplexität der Gesetzgebung liegt darin, daß die Gesetze häufig nicht darauf abzielen, die Rechtsposition des Bürgers zu stärken, sondern vielmehr Verarbeitung personenbezogener Daten zu ermöglichen, oft über das Maß hinaus, das bislang zulässig war. Viele Vorschriften sind so derart allgemein und umfassend zugunsten der Eingriffsseite formuliert, daß es schwerfällt, sie als "Datenschutzgeset-

ze" im eigentlichen Sinn zu verstehen. Wann immer Verwaltungen sich durch den Datenschutz behindert glaubten, ertönte der Ruf nach dem Gesetzgeber, der - zugunsten der Verwaltung - korrigierend eingreifen soll.Trotz alledem blieb der Datenschutz in wesentlichen
Bereichen ungeregelt. Auf Bundesebene gibt es z.B. bis heute keine hinreichenden datenschutzrechtlichen Vorschriften auf den Gebieten des Arbeitnehmerdatenschutzes, der Justizmitteilungen und der Zwangsvollstreckung, des Abgabenrechts, des Mieterschutzes, der Arbeit von Auskunfteien, Detekteien und privaten Sicherheitsdiensten, der Bundespolizeibehörden, des Ausländerzentralregisters oder - am gravierendsten - des gesamten Strafverfahrens.Die Konferenz der Datenschutzbeauftragten des Bundes
und der Länder appelliert an den Bundesgesetzgeber, diese Lücken umgehend und im Sinne der informationellen Selbstbestimmung zu schließen.Zur aktuellen Situation:Die derzeitige Situation des Datenschutzes wird von
den beiden großen Themenbereichen geprägt, die die Innenpolitik beherrschen: Die innere Sicherheit und der Zustand unserer Wirtschafts- und Sozialordnung. Diese Felder ängstigen die Menschen und stärken die Kontrollbedürfnisse des Staates. Auf beiden Gebieten wird die vermeintliche Lösung darin gesucht, daß die gesetzlichen Möglichkeiten zur Verarbeitung personenbezogener Daten erheblich ausgeweitet und auf der anderen Seite die Rechte der Bürger entsprechend eingeschränkt werden.Auf dem Gebiet der Strafverfolgung haben sich bisher
die Ermittlungen auf den Beschuldigten konzentriert

und die prozessuale Aufklärung geschah im wesentlichen offen.Jetzt setzt man auf Heimlichkeit und interessiert sich für Unbeteiligte. Ermittlungsverfahren ist nicht mehr Aufklärung eines konkreten Tatverdachts, sondern flächendeckende Sammlung personenbezogener Daten. Der Staat hält sich nicht mehr an die Grenzen der Ausforschung, die selbstverständlich waren, und er trifft dabei auf breite öffentliche Zustimmung.Im Bereich der Wirtschafts- und Sozialordnung wird auf
besonders drastische Weise versucht, durch die Einführung neuer Übewachungsverfahren eine Kostenminderung zu erreichen. Die Daten werden einerseits genutzt, durch Plafondierungen und Wirtschaftlichkeitsuntersuchungen eine Kostendämpfung zu erreichen (so etwa bei der Intensivierung der Kontrolle der Ärzte im Gesundheitsstrukturgesetz) oder eine angeblich mißbräuchliche Inanspruchnahme von Sozialleistungen aufzudecken (insbesondere durch regelmäßige Datenabgleiche bei Sozialhilfe und Arbeitsförderung).Auf den Datenschutz wirkt sich dabei die Tendenz aus,
weg von einer angeblichen egozentrischen Selbstbestimmung hin zu einer stärker betonten Gemeinschaftsverantwortung zu kommen. Individualrechte werden vielfach ohne zwingende Gründe zugunsten staatlicher Eingriffsrechte zurückgedrängt. Mehr und mehr begegnet der Staat dem einzelnen Bürger mit Mißtrauen und schafft ein immer dichteres Kontrollnetz. Es ist fraglich, ob dieses Menschenbild dem des Grundgesetzes entspricht.Hinzu kommt, daß das reine Verwaltungsinteresse, das
Bestreben nach größtmöglicher Perfektion und Einzelfallgerechtigkeit ein immer größeres Gewicht erhält. Je mehr Perfektion die Verwaltung angestrebt, desto mehr Daten muß sie erheben, nutzen, abgleichen oder

sonst verarbeiten. Das Gespür für den "Mut zur Lücke" geht verloren. Kennzeichend für den demokratischen Rechtsstaat ist aber nicht seine Allwissenheit, sondern die bewußte Beschränkung seiner Informationsherrschaft.Besonders gern wird zur Intensivierung der Kontrolle die Wunderwaffe des Datenabgleichs genutzt. Perfektion und Korrektheit lassen sich dadurch auf bequeme Weise erreichen: Auf Knopfdruck lassen sich die verschiedensten Kontrollmechanismen in Gang bringen, ohne daß sich die Behörde unmittelbar mit dem einzelnen Bürger auseinandersetzen muß. Mühelos ist die Prüfung von Zehntausenden in kürzester Frist möglich.Wird der Weg zu intensiverer Kontrolle und Überwachung, insbesondere zum Abgleich der verschiedensten Datenbestände, ungebremst fortgesetzt, könnte sich aus einer Unsumme von automatisierten Dateien und aus einem Netz von Datenabgleichen, das schließlich alle Bürger und fast alle ihre Lebensbereich erfaßt, der "gläserne Bürger" ergeben. Selbst wenn jeder einzelne Abgleich und Kontrollvorgang für sich eine gewisse Berechtigung haben sollte, trägt er bei zu einem umfassenden Netz von Überwachungs- und Überprüfungsmöglichkeiten. Jeder Bürger wird dabei potentiell zum Verdächtigen, dessen korrektes Verhalten ist zu überprüfen gilt. Damit ändert sich das Verhältnis des Bürgers zum Staat auf grundlegende Weise.Wie dem begegnen?Zwar ist die verfassungsrechtliche Dimension des Datenschutzes unbestritten. Gleichwohl fehlt der informationellen Selbstbestimmung das Fundament im Grundgesetz. Eine grundlegende Verbesserung könnte erreicht werden, wenn 10 Jahre nach der Anerkennung des Grundrechts auf

Datenschutz durch das Bundesverfassungsgericht dieses Grundrecht auch ausdrücklich in das Grundgesetz aufgenommen würde. Daß die erforderliche Mehrheit in Bundesrat und Bundestag hierfür bisher nicht erreicht werden konnte, bedauert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ausdrücklich.Die verfassungsrechtliche Verbesserung bei einer derartigen Grundgesetzänderung bestünde auch darin, daß bei jedem Gesetzentwurf von Anfang an die Berücksichtigung des Grundrechts auf Datenschutz zu prüfen wäre. Eine Einschränkung des Grundrechts müßte künftig durch ausdrückliche Erwähnung im Gesetz unter Angabe des neuen Grundgesetzartikels kenntlich gemacht werden (sog. Zitiergebot nach Art. 19 GG); anderenfalls wäre das Gesetz nichtig. Dies wäre ein erheblicher "Mehrwert" zu Gunsten der Bürger.Für die weitere Ausgestaltung des einfachen Datenschutzrechts sollten folgende Erwägungen zugrunde gelegt werden:In der Informationsgesellschaft ist der effektive Schutz der personenbezogenen Daten die Voraussetzung für eine breite Teilnahme der Bürger an der Gesellschaft. Nur wenn der Bürger sicher sein kann, daß seine dem Staat und der Wirtschaft überlassenen Daten soweit wie möglich geschützt werden, nimmt er aktiv am Gemeinschaftsleben teil. Der Bürger kann seine Freiheit zur Kommunikation (und umgekehrt ebenso seine Entscheidung zur Freiheit von Kommunikation) nur verwirklichen, wenn der Staat seine Schutzpflichten für die Daten der Bürger ernst nimmt.Die wichtigste Folge dieser Einsicht ist, daß Datenschutzvorschriften nicht nur Rechtssicherheit, sondern auch materielle Freiheitsräume garantieren müssen. Dies bedeutet, daß bei der Frage, ob der Einzelne

einer Auskunftspflicht unterworfen werden soll, ob seine Daten außer für den Erhebungszweck auch für andere Zwecke freigegeben werden sollen, wie lange belastende Daten aufbewahrt werden dürfen und welche Datenverarbeitungsvorgänge dem Betroffenen verborgen bleiben dürfen, jeweils strenge Maßstäbe angelegt werden müssen. Hierfür ist eine neue Grenzziehung für Eingriffe in das Recht auf informationelle Selbstbestimmung erforderlich: Der Begriff des "überwiegenden Allgemeininteresses", der alleine einen Eingriff in die informationelle Selbstbestimmung rechtfertigt, ist inhaltlich mehr aufzufüllen und mehr als bisher im Lichte der informationellen Selbstbestimmung zu interpretieren. In konkreten Konfliktfällen darf die Freiheitsicherung der Bürger gegenüber effektiver Staatstätigkeit nicht ins Hintertreffen geraten.Für das Bundesverfassungsgericht ist die Beteiligung unabhängiger Datenschutzbeauftragter wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten im Interesse eines vorgezogenen Rechtsschutzes von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung. Dies gilt insbesondere in den Bereichen, in denen eine Auskunfts- oder Einsichtsanspruch des Bürgers nicht oder nur unvollständig besteht. Daraus folgt, daß Rolle und Kompetenzen der Datenschutzbeauftragten auch im Hinblick auf effektivere Eingriffsmöglichkeiten gestärkt werden müssen. Versuche, die Kontrollmöglichkeiten der Datenschutzbeauftragten zu beschränken, muß schärfstens widersprochen werden.Datenschutzrechtliche Verstöße gehen meist auf Unkenntnis und mangelndes Problembewußtsein seitens der öffentlichen Stellen zurück. Aus- und Fortbildung in Fragen des Datenschutzes muß daher erheblich mehr Gewicht beigemessen werden als bisher. Insbesondere

sind Bemühungen zu fördern, den Datenschutz in den einschlägigen Ausbildungsplänen (Informatikunterricht in der Schule, Rechts- und Informatikstudium in den Hochschulen) sowie den Fortbildungsveranstaltungen an der öffentlichen Verwaltung als obligatorisches Fach zu verankern.Die Datenverarbeitungstechniken haben sich gegenüber der Zeit des Volkszählungsurteils geradezu revolutionär verändert. Der Umsetzung des Volkszählungsurteils durch die Schaffung der eigenen Rechtsgrundlagen muß daher verstärkt die Entwicklung geeigneter technisch organisatorischer Maßnahmen zur Seite gestellt werden. Der Blick des Datenschutzes muß sich stärker auf die Technik des Verarbeitunsprozesses selbst richten. Dies bedeutet nicht nur die Entwicklung spezifischer Datenschutzvorkehrungen für neue informationstechnische Entwicklungen (Miniaturisierung der Rechner, Chipkarten, neue Vernetzungstechniken), sondern auch neuer komplexer Anwendungsformen (z.B. im Bereich des Zahlungsverkehrs, der Straßenbenutzung oder der Textverarbeitung).Die Europäische Union wird zunehmend zur Informations-
und Datengemeinschaft. Dies macht einen europäischen Datenschutz erforderlich. Die Konferenz teilt mit den europäischen Nachbarn nicht nur die Überzeugung, daß der Datenschutz in Europa harmonisiert werden muß, sondern auch daß die Rechte der Gemeinschaftsbürger auf einem hohen Niveau gesichert werden müssen, damit die Öffnung der Grenzen für Güter, Kapital und Dienstleistungen - und damit auch für persönliche Daten - nicht zu Nachteilen für den einzelnen führt.Innerhalb von Deutschland, wirft die Integration der
neuen und der alten Bundesländer nach wie vor Probleme auf. Nach wie vor besteht die Neigung, über Bürger aus den neuen Bundesländern erheblich mehr Daten zu erhe-

ben und unter erleichterten Bedingungen Daten zu verarbeiten als dies in den alten Ländern der Fall wäre.Die Notwendigkeit für Übergangsregelungen in den neuen Bundesländern wird nicht bestritten; die Eingriffe in Persönlichkeitsrechte müssen aber dennoch verhältnismäßig, erforderlich und darüber hinaus zeitbefristet sein. Aus dem Einigungsprozeß herrührende Sonderregelungen und Verwaltungsvorschriften sind nicht festzuschreiben, sondern auch im Sinne der informationellen Selbstbestimmung schrittweise abzubauen.

Anlage 2

Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994

Datenschutzrechtliche Anforderungen an ein Übereinkommen der Mitgliedstaaten der Europäischen Union über die Errichtung eines europäischen Polizeiamtes (Europol)Die Datenschutzbeauftragten der Länder gehen gemeinsam mit dem Bundesdatenschutzbeauftragten davon aus, daß bei den Verhandlungen mindestens folgende Punkte berücksichtigt werden:- Das Übereinkommen muß der verfassungsrechtlichen

Kompetenzverteilung in Bund und Ländern für die Polizei entsprechen. Die materielle Verantwortung für die Datenverarbeitung muß, soweit die Daten von Landesbehörden erhoben worden sind, weiterhin bei den Ländern liegen. Davon bleiben die Zuständigkeiten und die dazugehörigen Befugnisse des BKA als nationale Stelle für den Informationsverkehr mit EUROPOL unberührt.- Die Regelungen zur Verarbeitung personenbezogener Daten müssen präzise sein und dem Grundsatz der Verhältnismäßigkeit entsprechen. Beispielsweise erfüllen die in den bisherigen Entwürfen vorgesehenen Befugnisse zur europaweiten Speicherung von Daten unbeteiligter Personen diese Voraussetzungen nicht.

Die Datenschutzbeauftragten erwarten, daß die deutsche Seite eine Klarstellung über die Verantwortung der Länder, zum Beispiel durch eine Protokollerklärung zum EUROPOL-Übereinkommen, trifft.

Anlage 3

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

Ausländerzentralregistergesetz - gegen die Stimme Bayerns -

Das Ausländerzentralregister beim Bundesverwaltungsamt in Köln existiert seit 40 Jahren ohne gesetzliche Grundlage. Derzeit stehen den verschiedenen Benutzern des Registers Daten zu mindestens 8 Millionen Ausländern, die sich in der Bundesrepublik aufhalten oder aufgehalten haben, zur Verfügung. Gespeichert sind neben Daten zur Identifizierung und weiteren Beschreibung der Person insbesondere Angaben zum Meldestatus, Aufenthaltsrecht und Asylverfahren.

Die Datenschutzbeauftragten des Bundes und der Länder haben immer wieder darauf hingewiesen, daß die Führung eines derartigen Registers ohne gesetzliche Regelung mit dem vom Grundgesetz Deutschen wie Ausländern gleichermaßen garantierten Recht auf informationelle Selbstbestimmung unvereinbar ist. Sie begrüßen daher, daß mit dem am 02. März 1994 vom Bundeskabinett beschlossenen Entwurf für ein Ausländerzentralregistergesetz eine gesetzliche Grundlage geschaffen werden soll.

Zwar enthält dieser Gesetzentwurf gegenüber früheren Entwürfen eine Reihe datenschutzrechtlicher Verbesserungen, Bedenken bestehen jedoch weiterhin: Die Datenschutzbeauftragten wenden sich insbesondere dagegen, daß das Ausländerzentralregister nicht nur als Informations- und Kommunikationssystem für die mit der Durch-

führung ausländer- und asylrechtlicher Vorschriften betrauten Behörden dienen, sondern darüber hinaus als Informationsverbund für Aufgaben der Polizei, Strafverfolgungsorgane und Nachrichtendienste zur Verfügung stehen soll.Die Funktionserweiterung wird deutlich durch die Speicherung von Erkenntnissen der Sicherheitsbehörden zu Ausländern in das Register. So soll der INPOL-Fahndungsbestand des BKA, soweit er Ausschreibungen zur Festnahme und zur Aufenthaltsermittlung von Ausländern enthält, in das Ausländerzentralregister übernommen werden. Gleiches gilt für die vorgesehene Speicherung von Angaben zu Personen, bei denen Anhaltspunkte für den Verdacht bestehten, daß sie im einzelnen bezeichnete Straftaten planen, begehen oder begangen haben. Diese Informationen dienen nicht einem Informationsbedarf zur Erfüllung ausländerbehördlicher Aufgaben, sondern - worauf die Entwurfsbegründung hinweist - der Kriminalitätsbekämpfung. Für diese Zwecke stehen den Sicherheitsbehörden aber eigene Informationssysteme zur Verfügung. Nach Auffassung der Datenschutzbeauftragten dürfen deshalb derartige Erkenntnisse nicht in das Register aufgenommen werden.Die im Entwurf vorgesehenen Voraussetzungen unter
denen u.a. für Polizeibehörden, Staatsanwaltschaften und Nachrichtendienste automatisierte Abrufverfahren eingerichtet werden können, stellen keine wirksamen Vorkehrungen für eine Begrenzung der Abrufe dar. Besonders problematisch ist der geplante automatisierte Zugriff durch die Nachrichtendienste auf einen - wenn auch reduzierten - Datensatz. Für die Dienste ist in den jeweiligen bereichsspezifischen Gesetzen der automatisierte Abruf aus anderen Datenbeständen ausgeschlossen. Die Erforderlichkeit derartiger Abrufe ist in keiner Weise belegt. Die Datenschutzbeauftragten

sprechen sich deshalb dafür aus, zumindest auf den automatisierten Abruf durch Nachrichtendienste zu verzichten.

Anlage 4

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

Informationsverarbeitung im Strafverfahren - bei Stimmenthaltung Bayerns -

Die Datenschutzbeauftragten des Bundes und der Länder erinnern an ihre Vorschläge zu gesetzlichen Regelungen der Informationsverarbeitung im Strafverfahren, die sie seit 1981 unterbreitet haben. Während die Befugnisse von Polizei und Staatsanwaltschaft zur Datenerhebung bei Ermittlungen mittlerweile in weitreichender Form gesetzlich abgesichert wurden, fehlen weiterhin Regelungen in der Strafprozeßordnung, wie die erhobenen Daten in Akten und Dateien weiter verarbeitet werden dürfen. Die Datenschutzbeauftragten des Bundes und der Länder halten die Beachtung folgender Grundsätze für notwendig, die in den Entwürfen des Bundes (Art. 4§474 ff. StPO des Entwurfs für ein Verbrechensbekämpfungsgesetz - BT-Drucksache 12/6853) und der Länder (Entwurf eines Strafverfahrensänderungsgesetzes 1994 des Strafrechtsausschusses der Justizministerkonferenz) nicht ausreichend berücksichtigt sind:

1. Strafrechtliche Ermittungsakten enthalten eine Vielzahl höchstsensibler Daten insbesondere auch über Opfer von Straftaten und Zeugen, die deshalb eines wirksamen Schutzes bedürfen. Es würde den Besonderheiten der im Strafverfahren - auch mit Zwangsmitteln - erhobenen Daten nicht ent-

sprechen, wenn Strafakten als Informationsquelle für jegliche Zwecke anderer Behörden oder von nicht am Strafverfahren Beteiligten dienten. Die einzelnen Zwecke und die zugriffsberechtigten Stellen sind daher abschließend normenklar festzulegen.1.1 Ingesamt ist sicherzustellen, daß der in anderen Zweigen der öffentlichen Verwaltung verbindlich geltende Standard des Datenschutzes für Übermittlungen keinesfalls unterschritten wird.1.2 Soweit ein unabweisbarer Bedarf anderer Stellen an Informationen aus Strafverfahren besteht, ist er in erster Linie durch Erteilung von Auskünften zu befriedigen. Akteneinsichtnahmen oder Aktenübersendungen können erst dann zugelassen werden, wenn eine Auskunftserteilung nicht ausreicht. Nicht erforderliche Aktenteile müssen ausgesondert werden. An Privatpersonen dürfen Informationen aus strafrechtlichen Ermittlungen nur weitergegeben werden, wenn deren rechtliche Interessen davon abhängen. 2. Bei Regelungen zur dateimäßigen Speicherung ist zu unterscheiden zwischen Systemen zur Vorgangsverwaltung (wie z. B. zentrale Namensdateien) und Dateien, die der Unterstützung strafprozessualer Ermittlungen dienen (z. B. Spurendokumentations- und Recherchesysteme).2.1 Der Datensatz zur Vorgangsverwaltung ist auf die Angaben zu beschränken, die zum Auffinden der Akten und zur Information über den Verfahrensstand erforderlich sind. Daten über Personen, die keine Beschuldigten sind, dürfen nur dann erfaßt werden, wenn dies zur Vorgangsverwaltung

zwingend erforderlich ist. In diesen Fällen bedarf es besonderer Zugriffs- und Verwendungsbeschränkungen. In jedem Fall sind die Daten entsprechend dem Verfahrensstand zu aktualisieren. Vom Gesetzgeber sind konkrete Löschungsfristen vorzusehen. Die Speicherung ist längstens auf den Zeitpunkt zu begrenzen, für den die Akte aufbewahrt wird. Vorgangsverwaltungssysteme können so auch für eine wirksame Kontrolle der Aufbewahrungsfristen genutzt werden.2.2 Die Staatsanwaltschaft kann sich zur Verwaltung ihres konventionell gespeicherten Datenmaterials grundsätzlich eines behördeninternen, automatisierten Nachweissystems bedienen. Länderübergreifende automatisierte Informationssysteme dürfen in Beachtung des Erforderlichkeitsprinzips demgegenüber allenfalls für solche Vorgänge errichtet werden, bei denen bestimmte Tatsachen die Prognose begründen, daß auf die erfaßten Daten zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben (erneut) zugegegriffen werden muß. Eine solche Prognose wird in der Regel dann nicht gerechtfertigt sein, wenn das zugrundeliegende Verfahren mit einer Einstellung nach §170 Abs. 2 StPO oder einem rechtskräftigen Freispruch abgeschlossen worden ist, sofern nicht auch nach Abschluß des Verfahrens noch tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte eine strafbare Handlung begangen hat. Eine Bereitstellung von Daten jedenfalls zu Zwecken der Strafverfolgung wird ferner grundsätzlich dann nicht in Betracht kommen, wenn die Ermittlungen konkrete Anhaltspunkte dafür bieten, daß der Beschuldigte nicht erneut strafbare Handlungen begehen wird. Dies kann z. B. bei Fahrlässigkeitstaten der Fall sein. Bei laufen-

den Verfahren kann die Zulässigkeit der Aufnahme von Daten im Hinblick auf die Möglichkeiten einer Verbindung von Verfahren, die Einstellung nach §154 StPO oder die Gesamtstrafenbildung gegeben sein.2.3 Für einen Informationsverbund zwischen verschiedenen speichernden Staatsanwaltschaften mit der Möglichkeit eines Direktzugriffs auf die Daten der jeweils anderen Behörden ergibt sich als Voraussetzung, daß die Weitergabe aller dem Zugriff unterliegenden Daten zumindest bei abstrakter Betrachtung zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben der übermittelnden oder der zugriffsberechtigten Stellen geeignet und angemessen sein muß. Für den Bereich der Strafverfolgung gilt ein umfassendes Aufklärungsgebot (§152 Abs. 2, §160 StPO). Die Staatsanwaltschaft kann im Rahmen ihrer Ermittlungen grundsätzlich ohne Rücksicht auf das Gewicht des Tatvorwurfs von allen öffentlichen Behörden - also auch von anderen Staatsanwaltschaften - Auskunft verlangen (§161 Satz 1 StPO). Diese Auskunftspflicht besteht über das Ermittlungsverfahren hinaus bis zum Abschluß des Strafverfahrens. Daten, die im Falle einer entsprechenden Anfrage zu mit einem Strafverfahren zusammenhängenden Zwecken offenbart werden müßten, können damit - ungeachtet der besonderen Voraussetzungen für die Errichtung eines Direktabrufverfahrens - von jeder Staatsanwaltschaft für andere Staatsanwaltschaften grundsätzlich auch in einem Informationssystem mit Direktabrufmöglichkeit bereitgestellt werden, sofern nur bestimmte Tatsachen die Annahme rechtfertigen, daß die Daten in einem Verfahren einer anderen

Behörde verwertet werden müssen. Eine solche Annahme wird regelmäßig wiederum in den unter 2.2 dargestellten Fällen nicht zu begründen sein. Eine Bereitstellung von Daten wird darüber hinaus auch dann nicht erfolgen können, wenn diese einem besonderen Amtsgeheimnis unterliegen und deshalb auch auf Anforderung nicht ohne weiteres übermittelt werden dürften. Auf §78 SGB X ist in diesem Zusammenhang hinzuweisen. Ein Direktabruf durch andere Stellen als Staatsanwaltschaften ist schon nach der Zweckbestimmung des Systems ausgeschlossen.2.4 In der Praxis dienen derzeit die bestehenden polizeilichen Informationssysteme auch den Zwecken der Strafverfolgung. Eine Abstimmung der polizeilichen und der staatsanwaltschaftlichen Informationssysteme ist geboten. Eine weitere Abstimmung wird im Hinblick auf das Bundeszentralregister zu erfolgen haben, das ebenfalls Daten zu Zwecken der Strafverfolgung, aber auch der Strafvollstreckung speichert. Die Datenschutzbeauftragten halten daher eine grundlegende Überarbeitung dieser Entwürfe für notwendig und bieten hierfür ihre Unterstützung an (vgl. Beschlüsse der Datenschutzkonferenzen vom 28./29. September 1981 zu "Mindestanforderungen für den Datenschutz bei den Zentralen Namenskarteien der Staatsanwaltschaften", vom 24./25. November 1986 "Überlegungen zu Regelungen der Informationsverarbeitung im Strafverfahren" und vom 05./06. April 1989 zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts vom 03. November 1988).

Anlage 5

Entschließung der 48. Konferenz der Datenschutzbeauftragtendes Bundes und der Länder vom 26./27. September 1994 Fehlende bereichsspezifische gesetzliche Regelungen bei der JustizObwohl seit dem Volkszählungsurteil des Bundesverfassungsgerichts mehr als 10 Jahre vergangen sind, werden im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet. Stattdessen sind in den letzten Jahren in zunehmendem Maße automatisierte Verfahren neu eingesetzt worden. Die Eingriffe in das Recht auf informationelle Selbstbestimmung stützen die Justizverwaltungen auf die Rechtsprechung des Bundesverfassungsgerichts zum sog. Übergangsbonus.Die Datenschutzbeauftragten des Bundes und der Länder weisen im Hinblick auf die kommende Legislaturperiode den Bundesgesetzgeber erneut darauf hin, daß gesetzliche Regelungen im Bereich der Justiz überfällig sind. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Der zur Zeit dem Bundesrat vorliegende Entwurf eines Strafverfahrensänderungsgesetzes beispielsweise wird datenschutzrechtlichen Anforderungen in keiner Weise gerecht. Im Bereich der Justiz fehlen ausreichende gesetzliche
Regelungen für die

- Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien,- Datenerhebung, -verarbeitung und -nutzung im Strafvollzug,- Übermittlung von Daten aus den bei Gerichten geführten Registern (z.B. Grundbuch) und deren Nutzung durch die Empfänger,- Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen (Justizmitteilungsgesetz),- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien.Eine Berufung auf den sog. Übergangsbonus auf unbegrenzte Zeit steht nicht in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts. Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe in der neuen Legislaturperiode unverzüglich bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes des Bürgers entgegenwirken.

Anlage 6

Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 Art. 12 Verbrechensbekämpfungsgesetz zur Trennung von Polizei und NachrichtendienstenGeheimdienstliche Informationsmacht und polizeiliche

Exekutivbefugnisse müssen strikt getrennt bleiben. Die Datenschutzbeauftragten des Bundes und der Länder stellen mit Besorgnis Entwicklungen fest, die die klare Trennungslinie zwischen Nachrichtendiensten und Polizeibehörden weiter zu verwischen drohen. Dies betrifft vor allem den Einsatz des Bundesnachrichtendienstes nach dem Verbrechensbekämpfungsgesetz:- Der BND erhält danach bei der Fernmeldeaufklärung

auch Befugnisse, die auf eine gezielte Erhebung von Daten für polizeiliche Zwecke hinauslaufen können. Deshalb ist bei dem Vollzug des Gesetzes darauf zu achten, daß nicht gezielt Informationen gesammelt werden, die vom Auftrag des BND nicht umfaßt werden.- Zwischen nachrichtendienstlichen Vorfelderkenntnissen und polizeilichen Zwangsmaßnahmen ist ein Filter erforderlich, der vor allem Unbeteiligte vor überzogenen Belastungen schützt.Die Datenschutzbeauftragten fordern, für die Zusammenarbeit von Nachrichtendiensten und Polizei in der Durchführung und Gesetzgebung das Trennungsgebot strikt zu beachten. Dies gilt auch bei der Fernmeldeaufklärung des BND. Eine wirksame Kontrolle durch den

Datenschutzbeauftragten in diesem sensiblen Bereich ist auch nach der Rechtsprechung des Bundesverfassungsgerichts sicherzustellen.

Anlage 7

Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 - gegen die Stimme Bayerns und bei Stimmenthaltung Sachsens -

Regelmäßige Datenübermittlungen an die öffentlich-rechtlichen Rundfunkanstalten und die Gebühreneinzugszentrale (GEZ)Die öffentlich-rechtlichen Rundfunkanstalten drängen seit langem auf die Schaffung einer Rechtsgrundlage für die regelmäßige übermittlung von Meldedaten aller Einwohner an die gemeinsame Gebühreneinzugszentrale (GEZ). Sie verweisen dazu auf bereits bestehende Regelungen in den Ländern Hessen und Nordrhein-Westfalen. Auf Bitten der Konferenz der Regierungschefs der Länder hat deshalb nunmehr der zuständige Arbeitskreis der Innenministerkonferenz einen Musterentwurf für eine bundesweite Lösung im Melderecht erarbeitet. Der Entwurf sieht vor, daß künftig alle Meldebehörden in der Bundesrepublik im Fall der Anmeldung, Abmeldung oder des Todes eines volljährigen Einwohners bis zu acht Kerndaten an die GEZ übermitteln dürfen.Die Datenschutzbeauftragten des Bundes und der Länder lehnen eine derartige Regelung insbesondere aus folgenden Gründen ab:Die Regelung könnte im Ergebnis zu einem bundesweiten Melderegister bei Volljährigen führen. Sie könnte außerdem gegen das verfassungsrechtlich garantierte Verhältnismäßigkeitsprinzip verstoßen. Den Rundfunkanstalten stünde möglicherweise der unkontrollierte

Zugriff auf Millionen personenbezogener Daten volljähriger Einwohner der Bundesrepublik zu, obwohl es für die Rundfunkanstalten nur von Interesse ist, welcher Einwohner bei ihnen gebührenpflichtig ist und bislang seine Gebührenpflicht nicht angemeldet hat. Das vorgesehene generelle übermittlungsverfahren kennt keine Unterscheidung zwischen erforderlichen und nicht erforderlichen Daten, sondern überläßt diese Unterscheidung der GEZ. Über die Frage, ob ein Volljähriger überhaupt gebührenpflichtig ist, geben die Meldedaten keine Auskunft. Das muß nach wie vor im herkömmlichen Verfahren durch Befragung ermittelt werden.Die Datenschutzbeauftragten des Bundes und der Länder
sind bereit, an geeigneten und verfassungskonformen Lösungen der Landesregierungen zur Sicherung des Gebührenaufkommens der Rundfunkanstalten mitzuwirken.

Anlage 8

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. August 1994Vorschlag der Kommission der Europäischen Union für
eine Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik - EG-Statistikverordnung -(KOM(94) 78 endg.; Ratsdok. 5615/94 = BR-Drs. 283/94)Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, daß die Europäische Union eine allgemeine Regelung für die Gemeinschaftsstatistik trifft, weisen allerdings daraufhin, daß die datenschutzrechtliche Entwicklung bei der Europäischen Union mit dem Aufbau der europäischen Statistik keineswegs Schritt gehalten hat.Sie stellen mit Besorgnis fest, daß der vorliegende Vorschlag einer EG-Statistikverordnung die nationalen datenschutzrechtlichen Grundsätze und wesentliche Standards des Statistikrechts weitgehend nicht berücksichtigt. Sie fordern daher zur Wahrung des Rechts der Betroffenen auf informationelle Selbstbestimmung mit Nachdruck, daß die Bundesregierung ihre Bedenken gegen diesen Vorschlag geltend macht und diese bei den Beratungen auf europäischer Ebene zum Tragen bringt.Die Datenschutzbeauftragten des Bundes und der Länder unterstützen ausdrücklich den Beschluß des Deutschen Bundesrates vom 8. Juli 1994 (BR-Drs. 283/94 - Beschluß -).

Gegen den vorgelegten Vorschlag einer Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik (EG-Statistikverordnung) erheben sie insbesondere die folgenden datenschutzrechtlichen Bedenken:1. In Art. 1 sollte als die zuständige Gemeinschaftsdienststelle unmißverständlich das Statistische Amt der Europäischen Gemeinschaften (EUROSTAT) bestimmt werden, weil die erforderlichen rechtlichen, administrativen, technischen und organisatorischen Maßnahmen - insbesondere zur Sicherung der Zweckbindung der zu statistischen Zwecken erhobenen Daten sowie zur Wahrung der statistischen Geheimhaltung - bei dieser Stelle bereits aufgrund der EG-Übermittlungsverordnung 1588/90 vom 11. Juni 1990 getroffen werden können. Eine jederzeit revidierbare Organisationsentscheidung der Kommission darüber, welche Dienststelle der Europäischen Union für statistische Aufgaben zuständig ist, birgt dagegen die Gefahr, daß Daten an unterschiedliche Stellen der Kommission zu unterschiedlichen Zwecken übermittelt werden. Zugleich sollte EUROSTAT zumindestens einen der Selbständigkeit der Statistischen Ämter in der Bundesrepublik Deutschland vergleichbaren organisationsrechtlichen Status erhalten, der die unter dem Gesichtspunkt der Objektivität und Neutralität gebotenen Eigenständigkeit bei der Aufgabenerfüllung garantiert. Dies könnte anläßlich der für 1996 vorgesehenen Revision des Vertrages über die Europäische Union geschehen.2. Das mehrjährige statistische Programm sollte nicht wie in Art. 3 vorgesehen von der Kommission beschlossen werden. Die grundlegenden Entscheidungen

über die Bürger belastende Datenerhebungen sollten dem Rat mit Zustimmung des Europäischen Parlaments vorbehalten bleiben. Dabei sollte der Planungscharakter des Programms in den Vordergrund gestellt werden.3. Art. 5 sollte festlegen, daß statistische Einzelmaßnahmen durch einen Rechtsakt gemäß dem Verfahren nach Art. 189 b EG-Vertrag angeordnet werden. Dies gilt auch für die statistische Auswertung von Daten, die bei den administrativen Stellen bereits vorliegen (sog. Sekundärstatistik). Die im Vorschlag vorgesehene generelle Befugnis der Kommission, statistische Einzelmaßnahmen zu regeln, ist viel zu weitgehend.4. Die in Art. 12 vorgesehene Übertragung der Befugnis zur Organisation der Verbreitung der statistischen Daten auf die Kommission widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag, aus dem folgt, daß grundsätzlich die Mitgliedstaaten nach ihrem nationalen Recht zur Verbreitung der statistischen Daten zuständig sind. Ferner sollte in Art. 12 festgelegt werden, daß an Stellen außerhalb der statistischen Gemeinschaftsdienststelle nur nicht-vertrauliche statistische Daten übermittelt werden dürfen.5. Der in Art. 13 gegenüber der Definition in der EG-Übermittlungsverordnung 1588/90 neu definierte Begriff "statistische Geheimhaltung" muß präzisiert werden. Dazu gehört insbesondere, daß festgelegt wird, unter welchen Voraussetzungen statistische Daten vertraulich sind und nicht nur als vertraulich gelten. Dies gilt um so mehr, als im Verordnungsvorschlag dieser Begriff nicht nur in Art. 13, sondern auch in Art. 9 Abs. 2 - allerdings mit einem anderen Begriffsinhalt - definiert

wird. Der Begriff "statistische Geheimhaltung" sollte an einer Stelle in der Verordnung und so definiert werden, daß er Art. 2 Nr. 1 der EG-Übermittlungsverordnung 1588/90 und damit den derzeit geltenden nationalen Begriffsbestimmungen entspricht. Dies stände auch im Einklang mit dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag.6. Gemäß dem Grundsatz der Subsidiarität sollte - ebenso wie die Befugnis zur Verbreitung statistischer Ergebnisse (Art. 11 Abs. 1) - auch die Festlegung der Zuständigkeit für die Durchführung der statistischen Einzelmaßnahmen (Art. 7) den Mitgliedstaaten überlassen bleiben.7. Auch die in Art. 16 vorgesehene generelle Zugangsregelung einzelstaatlicher Stellen und der Gemeinschaftsdienststelle zu Registern der Verwaltung widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag. Dieser gebietet hier, daß - jedenfalls grundsätzlich - die Mitgliedstaaten zu bestimmen haben, in welcher Weise sich die für die Erstellung der Gemeinschaftsstatistiken zuständigen nationalen Stellen Daten beschaffen. Damit ist aber nicht zu vereinbaren, daß auch Stellen der Kommission unmittelbar Zugang zu nationalen Verwaltungsregistern haben sollen. Ferner bleibt unklar, ob die nach Art. 16 erhobenen Daten Erhebungs- oder Hilfsmerkmale sein sollen. Im übrigen darf über Art. 16 ein Zugang zu solchen personenbezogenen Daten, die nach nationalem Recht einer besonderen Geheimhaltung, z. B. dem Steuer- oder auch dem Sozialgeheimnis unterliegen, nicht eröffnet werden.

8. Die Regelung des Art. 17 ist mißglückt. Allem Anschein nach soll hier eine weitgehende Ausnahmeregelung von der statistischen Geheimhaltung zugunsten von Forschungsinstituten, einzelner Forscher und von für die Erstellung von Nicht-Gemeinschaftsstatistiken zuständigen Stellen vorgesehen werden, die die Möglichkeit eröffnet, die in diesem Bereich geltenden strengeren nationalen Regelungen zu umgehen. Außerdem würde von der für EUROSTAT geltenden EG-Übermittlungsverordnung 1588/90 abgewichen werden. Art. 17 sollte deshalb so gefaßt werden, daß die nationalen Zugangsregelungen für Einrichtungen mit der Aufgabe der unabhängigen wissenschaftlichen Forschung nicht umgangen werden können.9. Der Vorschlag der Kommission sieht weder eine alsbaldige Trennung und Aufbewahrung von Erhebungs- und Hilfsmerkmalen noch eine alsbaldige Löschung personenbezogener Hilfsmerkmale vor. In der Bundesrepublik Deutschland dagegen gehören entsprechende Regelungen (vgl. §12 BStatG) zum Kernbereich des Statistikrechts. Im Volkszählungsurteil hat das Bundesverfassungsgericht ihnen grundrechtssichernde Bedeutung beigemessen.10. Schließlich fehlt es für die Organe der Europäischen Union noch immer an einer unabhängigen und effektiven Datenschutzkontrollinstanz, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der Europäischen Union in seinen Rechten verletzt zu sein.

Anlage 9

Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1994 Abbau des Sozialdatenschutzes - gegen die Stimme Bayerns -Der Gesetzgeber hat in den vergangenen Monaten die Möglichkeit der Überprüfung von Sozialleistungsempfängern ohne deren vorherige Befragung oder Kenntnis in drastischem Umfang vermehrt. Insbesondere durch das seit dem 1. Juli 1993 geltende Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms ist das Kontrollinstrumentarium von Sozial- und Arbeitsämtern noch einmal erheblich erweitert worden. Ohne Rücksicht auf konkrete Anhaltspunkte für einen unberechtigten Leistungsbezug im Einzelfall sind künftig automatisierte Datenabgleiche zwischen Sozialhilfeträgern sowie zwischen diesen und der Arbeitsverwaltung bzw. der Kranken-, Unfall- und Rentenversicherung gestattet.Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist sehr besorgt über diese Entwicklung, die zu einem immer dichteren Datenverbundsystem im Sozialleistungsbereich und zu immer nachhaltigeren Eingriffen in das Recht auf informationelle Selbstbestimmung aller Betroffenen, d. h. auch und gerade der großen Mehrheit rechtstreuer Antragsteller und Leistungsbezieher, führt.Mit Nachdruck wenden sich die Datenschutzbeauftragten gegen Versuche von Sozialverwaltungen, bei der Umsetzung der neuen Kontrollregelungen durch extensive Interpretation über den gesetzlich vorgegebenen Rahmen

hinauszugehen. So erlaubt beispielsweise der neu gefaßte §117 Abs. 3 des Bundessozialhilfegesetzes entgegen der Handhabung einzelner Kommunen keinen automatisierten Datenabgleich zwischen Sozialhilfedatei und Kraftfahrzeug-Register, sondern nur den Vergleich von Angaben in Verdachtsfällen.Die dargestellte Entwicklung macht es erneut notwendig, auf die verfassungsrechtliche Qualität des Grundsatzes der Datenerhebung beim Betroffenen hinzuweisen. An dem Prinzip, daß bei der Überprüfung der Leistungsberechtigung und der Nachweise Auskünfte zunächst beim Antragsteller anzufordern sind und nur aufgrund konkreter Verdachtsmomente Nachfragen bei dritten Stellen oder Datenabgleiche erfolgen dürfen, muß für den Regelfall festgehalten werden, soll der Einzelne mündiger Bürger bleiben und nicht zum bloßen Objekt staatlicher Verhaltenskontrolle werden.Sorge äußert die Konferenz auch über die hartnäckigen Bestrebungen, Datenbestände der Sozialverwaltung für immer neue Zwecke und Adressaten zu öffnen. Beispiele dafür sind die im Gesetzgebungsverfahren zum 2. SGB-Änderungsgesetz im letzten Augenblick gescheiterten Anträge, Polizei und Staatsschutz in unvertretbarem Umfang Zugriff auf Daten Arbeitsloser und sonstiger Sozialleistungsempfänger zu geben. Das Sozialgeheimnis muß ein wirksamer Sonderschutz für die besonders sensiblen Daten in der Sozialverwaltung bleiben. Nur dies entspricht der Abhängigkeit des Einzelnen von staatlichen Leistungen und der sich daraus ergebenden speziellen Verletzlichkeit seines Rechts auf informationelle Selbstbestimmung.

Anlage 10

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

Chipkarten im Gesundheitswesen Die Datenschutzbeauftragten von Bund und Länder verfolgen die zunehmende Verwendung von Chipkarten im Gesundheits- und Sozialwesen mit kritischer Aufmerksamkeit.Chipkarte als gesetzliche KrankenversicherungskarteDie Krankenversicherungskarte, die bis Ende des Jahres in allen Bundesländern eingeführt sein wird, darf nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten. Die Datenschutzbeauftragten überprüfen, ob- die Krankenkassen nur die gesetzlich zulässigen

Daten auf den Chipkarten speichern und - die Kassenärztlichen Vereinigungen dafür sorgen, daß

nur vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte Lesegeräte und vom Bundesverband der Kassenärztlichen Vereinigungen geprüfte Programme eingesetzt werden.Chipkarte als freiwillige GesundheitskarteSogenannte "Gesundheitskarten", etwa "Service-Karten" von Krankenversicherungen und privaten Anbietern, "Notfall-Karten", "Apo(theken)-Cards" und "Röntgen-Karten" werden neben der Krankenversicherungskarte als freiwillige Patienten-Chipkarte angeboten und empfohlen. Während die Krankenversicherungskarte nach dem So-

zialgesetzbuch nur wenige Identifikationsdaten enthalten darf, kann mit diesen "Gesundheitskarten" über viele medizinische und andere persönliche Daten schnell und umfassend verfügt werden. Gegenüber der konventionellen Ausweiskarte oder einer Karte mit einem Magnetstreifen ist die Chipkarten-Technik ungleich komplexer und vielfältig nutzbar. Damit steigen auch die Mißbrauchsgefahren bei Verlust, Diebstahl oder unbemerktem Ablesen der Daten durch Dritte. Anders als bei Ausweiskarten mit Klartext können Chipkarten nur mit technischen Hilfsmitteln gelesen werden, die der Betroffene in der Regel nicht besitzt. So kann er kaum kontrollieren, sondern muß weitgehend darauf vertrauen, daß der Aussteller der Karte und sein Arzt nur die mit ihm vereinbarten Daten im Chip speichern, das Lesegerät auch wirklich alle gespeicherten Daten anzeigt und der Chip keine oder nur eindeutig vereinbarte Verarbeitungsprogramme enthält.Die Freiwilligkeit der Entscheidung für oder gegen die Gesundheitskarte mit Chipkarten-Technik ist in der Praxis bisweilen nicht gewährleistet. So wird ein faktischer Zwang auf die Entscheidungsfreiheit des Betroffenen ausgeübt, wenn der Aussteller - etwa ein Krankenversicherungsunternehmen oder eine Krankenkasse - mit der Einführung der Chipkarte das bisherige konventionelle Verfahren erheblich ändert, z. B. den Schriftwechsel erschwert oder den Zugang zu Leistungen Karten-Inhabern vorbehält bzw. erleichert.So stellt beispielsweise eine Kasse ihren Mitgliedern Bonuspunkte in Aussicht, wenn sie auf sog. Aktionstagen der Kasse Werte wie Blutzucker, Sauerstoffdynamik, Cholesterol sowie weitere spezielle medizinische Daten ohne ärztliche Konsultation messen und auf der Karte speichern und aktualisieren lassen. In Abhängigkeit von der Veränderung dieser Werte wird von der Kasse ge-

gebenenfalls ein Arztbesuch empfohlen. Die Vergabe solcher Bonuspunkte widerspricht dem Prinzip der Freiwilligkeit bei der Erhebung der Daten für die Patienten-Chipkarte. Der Effekt wird noch verstärkt, indem die Kasse die "Möglichkeit einer Beitragsrückerstattung" in Aussicht stellt. Die Datenschutzbeauftragten des Bundes und der Länder sehen in dieser Art der Anwendung der Chipkarten-Technik das Risiko eines Mißbrauchs, solange der Inhalt und die Nutzung der Daten nicht mit den zuständigen Fachleuten - wie den Medizinern - und den Krankenkassen abgestimmt ist.Die Konferenz der Datenschutzbeauftragten des Bundes
und der Länder hält für den Einsatz und die Nutzung freiwilliger Patienten-Chipkarten zumindest - vorbehaltlich weiterer Punkte - die Gewährleistung folgender Voraussetzungen für erforderlich:- Die Zuteilung einer Gesundheitskarte und die damit
verbundene Speicherung von Gesundheitsdaten bedarf der schriftlichen Einwilligung des Betroffenen. Er ist vor der Erteilung der Einwilligung umfassend über Zweck, Inhalt und Verwendung der angebotenen Gesundheitskarte zu informieren.- Die freiwillige Gesundheitskarte darf nicht - etwa
durch Integration auf einem Chip - die Krankenversichertenkarte nach dem Sozialgesetzbuch verdrängen oder ersetzen.- Die Karte ist technisch so zu gestalten, daß für
die einzelnen Nutzungsarten nur die jeweils erforderlichen Daten zur Verfügung gestellt werden.- Der Betroffene muß von Fall zu Fall frei und ohne
Benachteiligung - z. B. gegenüber dem Arzt, der Krankenkasse oder der Versicherung - entscheiden können, die Gesundheitskarte zum Lesen der Gesund-

heitsdaten vorzulegen und ggf. den Zugriff auf bestimmte Daten zu beschränken. Er muß ferner frei entscheiden können, wer welche Daten in seinen Datenbestand übernehmen darf. Der Umfang der Daten, die gelesen oder übernommen werden dürfen, ist außerdem durch die gesetzliche Aufgabenstellung bzw. den Vertragszweck der Nutzer beschränkt.- Der Kartenaussteller muß sicherstellen, daß der Betroffene jederzeit vom Inhalt der Gesundheitskarte unentgeltlich Kenntnis nehmen kann.- Der Betroffene muß jederzeit Änderungen und Löschungen der gespeicherten Daten veranlassen können.Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dafür aus, daß der Gesetzgeber dies durch bereichsspezifische Rechtsgrundlagen sicherstellt.

Anlage 11

Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993

Kartengestützte Zahlungssysteme im öffentlichen NahverkehrMit der Weiterentwicklung von Chipkarten werden kartengestützte Zahlungssysteme zunehmend auch im Verkehrsbereich eingesetzt. Damit besteht die Gefahr, daß sehr detaillierte Bewegungsprofile entstehen, die den persönlichen Bereich jedes Einzelnen einschränken und z.B. auch für Strafverfolgungsbehörden, Finanzämter und für die Werbewirtschaft von Interesse sein könnten. Da sämtliche Fahrten für einen gewissen Zeitraum aufgelistet werden können, hat jeder Kontoinhaber die Möglichkeit, Fahrten sämtlicher Familienmitglieder jederzeit nachzuvollziehen.So sind im öffentlichen Nahverkehr zahlreiche sogenannte Postpaid-Verfahren in Erprobung, bei denen dem Fahrgast am Monatsende die aufsummierten Fahrpreise vom Konto abgebucht werden. Diese Zahlungsweise erfordert die Speicherung umfangreicher personenbezogener Daten: Neben der Konto-Nr. und Bankleitzahl des Fahrgastes werden sowohl Datum und Uhrzeit des Fahrscheinkaufs bzw. des Fahrantritts als auch Automatennummer und Preisstufe der jeweiligen Fahrt erhoben.Eine solche Vorgehensweise ist umso problematischer, als technische Alternativen existieren, die weitaus datenschutzfreundlicher sind. Im öffentlichen Nahverkehr können - wie skandinavische und auch deutsche Projekte aufzeigen - Wertkartensysteme eingesetzt

werden, bei denen im voraus bezahlt wird und die daher gänzlich ohne personenbezogene Daten auskommen.Die Datenschutzbeauftragten halten es daher für dringend erforderlich, daß mehr als bisher bei der Einführung kartengestützter Zahlungssysteme darauf geachtet wird, die "datenfreie Fahrt" zu ermöglichen. Im öffentlichen Nahverkehr sollte weiterhin auch die datenschutzfreundlichste Lösung angeboten werden: Der Kauf einer Fahrkarte am Automaten mit Bargeld.Die Konferenz fordert weiter, daß noch vor der Pilotierung der dargestellten Technikvorhaben im Verkehrsbereich eine Untersuchung möglicher Alternativen, eine Analyse der von ihnen ausgehenden Gefahren für das informationelle Selbstbestimmungsrecht und eine Darstellung der technischen und organisatorischen Möglichkeiten zur Gewährleistung des Persönlichkeitsschutzes zu erstellen ist (Technikfolgen-Abschätzung). Nur Verfahren mit dem geringsten Eingriff in das allgemeine Persönlichkeitsrecht sollten eine Chance zur Erprobung erhalten.

Anlage 12

Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 Datenschutz bei der Privatisierung der Deutschen Bundespost Telekom und bei der europaweiten Liberalisierung des Telefonnetzes und anderer TelekommunikationsdiensteIm Zuge der sog. Postreform II soll die Deutsche Bundespost Telekom - nach der dafür notwendigen Änderung des Grundgesetzes - in Form einer Aktiengesellschaft privatisiert werden. Zugleich hat der Ministerrat der Europäischen Gemeinschaften in seiner Entschließung vom 22. Juli 1993 (Amtsblatt der EG Nr. C 213 vom 6. 8. 1993) seine Entschlossenheit bekräftigt, die Monopole im öffentlichen Sprachtelefondienst (Festnetz) der Mitgliedstaaten bis zum 1. Januar 1998 zu beseitigen.In absehbarer Zeit werden daher in Deutschland neben der "Telekom AG" auch im Telefondienst andere private Unternehmen Telekommunikationsdienstleistungen anbieten. Diese Privatisierung hat Konsequenzen für den Datenschutz, der bisher für die Deutsche Bundespost Telekom auf einem vergleichsweise hohen Niveau geregelt ist. Insbesondere das grundgesetzlich garantierte Fernmeldegeheimnis würde für private Netzbetreiber und Diensteanbieter jedenfalls nicht mehr unmittelbar gelten.Die Datenschutzbeauftragten des Bundes und der Länder halten es für unabdingbar, daß durch die Privatisierung und Liberalisierung der Schutz der Bürger insbesondere in solchen Bereichen nicht verringert wird,

die - wie der Telefondienst - der Daseinsvorsorge zuzurechnen sind. So wie bisher die konkurrierenden privaten Betreiber der Mobilfunknetze einen gleichmäßig hohen Datenschutzstandard gewährleisten müssen, hat dies auch zu gelten, wenn in Zukunft private Unternehmen im Wettbewerb miteinander stationäre Telefonnetze betreiben und entsprechende Dienste anbieten. Die Einhaltung von datenschutzrechtlichen Bestimmungen bei Telekommunikationsnetzen und -diensten muß zukünftig von einer unabhängigen Stelle nach bundesweit einheitlichen Kriterien und von Amts wegen kontrolliert werden können.Da der Wettbewerb zwischen privaten Netzbetreibern und Diensteanbietern nicht nur national begrenzt, sondern im europäischen Binnenmarkt stattfinden wird, sind auch Rechtsvorschriften der Europäischen Gemeinschaften erforderlich, die einen möglichst hohen, einheitlichen Datenschutzstandard in der Telekommunikation gewährleisten.

Anlage 13

Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. März 1994 Gesetzentwurf der Bundesregierung zur Neuordnung des Postwesens und der Telekommunikation (Postneuordnungsgesetz - PTNeuOG, BR-Drs. 115/94 = BT-Drs. 12/6718) und zu der dafür erforderlichen Änderung des Grundgesetzes (BR-Drs. 114/94 = BT-Drs.12/6717)I.Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, daß mit der Umwandlung der Deutschen Bundespost POSTDIENST in die Deutsche Post AG und der Deutschen Bundespost TELEKOM in die Deutsche Telekom AG zwei staatliche Einrichtungen aufhören zu existieren, gegenüber denen sich der Bürger bisher unmittelbar auf das Post- und Fernmeldegeheimnis berufen kann. Sie treten deshalb dafür ein, in der Verfassung sicherzustellen, daß jeder, der Post- und Fernmeldedienstleistungen erbringt, das Post- und Fernmeldegeheimnis zu wahren hat.II.Im Gesetz zur Neuordnung des Postwesens und der Telekommunikation ist ein den Vorgaben des Bundesverfassungsgerichts in seinem Volkszählungsurteil vom 15. Dezember 1983 und in seinem Fangschaltungsbeschluß vom

25. März 1992 entsprechender Schutz von Individualrechten zu gewährleisten. Die Datenschutzbeauftragten halten inbesondere folgende Änderungen des Gesetzentwurfs für erforderlich:a) Der Umfang der zulässigen Verarbeitung personenbezogener Daten im Post- und Telekommunikationswesen ist im Gesetz selbst festzulegen; lediglich deren konkrete Ausgestaltung kann der Regelung durch Rechtsverordnungen überlassen bleiben.b) Die Gewährleistung des Datenschutzes und des Post- und Fernmeldegeheimnisses muß in den Katalog der Ziele der Regulierung aufgenommen werden.c) Das Post- und Telekommunikationswesen muß auf Dauer - auch nach dem Wegfall der Monopole - einer effektiven, unabhängigen datenschutzrechtlichen Kontrolle von Amts wegen nach bundesweit einheitlichen Kriterien unterworfen bleiben, auch soweit personenbezogene Daten nicht in Dateien verarbeitet werden.d) Die Frist für die Speicherung von Verbindungsdaten zur Ermittlung und zum Nachweis der Entgelte ist präzise festzulegen.e) Die vorgesehene Vorschrift zum Einzelentgeltnachweis schränkt den Kreis der Einrichtungen, die Telefonberatung durchführen und die nicht auf Einzelentgeltnachweisen erscheinen sollen, in unakzeptabler Weise ein. Dem Schutz des informationellen Selbstbestimmungsrechtes und des Fernmeldegeheimnisses der Angerufenen würde es dagegen am ehesten entsprechen, wenn jeder inländische Anschlußinhaber selbst entscheiden kann, ob und gegebenenfalls wie seine Rufnummer auf Einzelent-

geltnachweisen erscheinen soll. Damit wäre auch die Anonymität von Anrufen bei Beratungseinrichtungen unbürokratisch sicherzustellen. Ein entsprechendes Verfahren wird in den Niederlanden bereits praktiziert.f) Es wäre völlig unangemessen, wenn in Zukunft erlaubt würde, daß die Telekommunikationsunternehmen Nachrichteninhalte über die Befugnisse des §14 a Fernmeldeanlagengesetz hinaus auch für die Unterbindung von Leistungserschleichungen und sonstiger rechtswidriger Inanspruchnahme des Telekommunikationsnetzes und seiner Einrichtungen sowie von Telekommunikations- und Informationsdienstleistungen erheben, verarbeiten und nutzen dürften.III.Die Datenschutzbeauftragten betonen, daß angesichts der neuen technischen Möglichkeiten digitaler Kommunikations- und Informationsdienste und der mit ihrer Nutzung zwangsläufig verbundenen Datenverarbeitung eine grundlegende Überarbeitung des §12 Fernmeldeanlagengesetz, der die Weitergabe vorhandener Telekommunikationsdaten in Strafverfahren erlaubt, überfällig ist. Sie erinnern an die Umsetzung der entsprechenden Entschließung des Bundesrates vom 27. August 1991 (BR-Drs. 416/91).

Anlage 14

Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 Geänderter Vorschlag für eine Europäische Richtlinie zum Datenschutz im ISDN und in Mobilfunknetzen vom 13.Juni 1994 (KOM (94) 128 endg. - COD 288)Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, daß die Europäische Kommission mit der Vorlage des geänderten Vorschlags für eine Richtlinie zum Datenschutz im ISDN ihre Absicht bekräftigt hat, unionsweit bereichsspezifische Regelungen für den Datenschutz in Telekommunikationsnetzen zu schaffen. Es kann kein Zweifel daran bestehen, daß die digitalen Telekommunikationsnetze in der Europäischen Union zunehmend zur wichtigsten Infrastruktur für die Verarbeitung personenbezogener Daten werden. Der Regelungsdruck wird erhöht durch die Tatsache, daß die Europäische Union die rechtlichen und technischen Voraussetzungen für die Liberalisierung der Telekommunikationsmärkte in weiten Bereichen bereits geschaffen hat und mehrere Mitgliedsstaaten, darunter Deutschland, derzeit ihr nationales Telekommunikationsrecht auf die Vorgaben der EU umstellen.Aus diesem Grund sollte der geänderte Vorschlag für eine ISDN-Richtlinie so bald wie möglich vom Ministerrat und vom Europäischen Parlament abschließend beraten werden. Die Bundesregierung sollte die deutsche Ratspräsidentschaft dazu nutzen, den geänderten Vorschlag für eine ISDN-Richtlinie im Rat behandeln zu lassen.

Dabei sollte sich die Bundesregierung insbesondere für folgende Verbesserungen des Richtlinienvorschlags aus datenschutzrechtlicher Sicht einsetzen:1. Für Telekommunikationsorganisationen und Diensteanbieter müssen die gleichen gemeinschaftsrechtlichen Regelungen zum Datenschutz gelten. Die Verarbeitung personenbezogener Daten durch Diensteanbieter darf nicht privilegiert werden.2. Die Beschränkung der Datenverarbeitung auf Zwecke der Telekommunikation sollte wieder in die Richtlinie aufgenommen werden. Der allgemeine Zweckbindungsgrundsatz der Datenschutzrichtlinie läßt die Zweckentfremdung schon bei "berechtigten Interessen" der Verarbeiter zu. Das ist angesichts zunehmender Diversifizierung der Aktivitäten von Netzbetreibern und Diensteanbietern eine zu weitgehende Lockerung der Zweckbindung im Telekommunikationsbereich.3. Das ursprünglich vorgesehene Verbot, personenbezogene Daten zur Erstellung von elektronischen Profilen der Teilnehmer zu nutzen, sollte wieder in die Richtlinie aufgenommen werden.4. Die Speicherung von Inhaltsdaten nach Beendigung der Übertragung sollte - wie im ursprünglichen Richtlinienentwurf vorgesehen - untersagt werden.5. Die Vertraulichkeit der Kommunikationsbeziehungen und -inhalte (Fernmeldegeheimnis) sollte - wie es der ursprüngliche Richtlinienvorschlag ebenfalls vorsah - auf Unionsebene garantiert werden.6. Um eine Harmonisierung des Gemeinschaftsrechts beim Einzelgebührennachweis zu erreichen, sollten konkre-

te Vorgaben in die Richtlinie aufgenommen werden, z.B. indem den angerufenen Teilnehmern die Aufnahme ihrer Rufnummer in Einzelgebührennachweise freigestellt wird.7. Im Fall der Anrufweiterschaltung sollte die automatische Information des anrufenden Teilnehmers darüber, daß sein Anruf (z.B. bei einem Arzt) an einen Dritten weitergeschaltet wird, gewährleistet sein.Die Konferenz begrüßt die im geänderten Vorschlag vorgesehene Kostenfreiheit für die verschiedenen Optionen der Anzeige der Rufnummer des Anrufers und für die Nichtaufnahme von Daten in das Teilnehmerverzeichnis (Telefonbuch).Diese Vorschläge berücksichtigen das Subsidiaritätsprinzip und beschränken sich auf Änderungen, die zur Gewährleistung der Vertraulichkeit der Kommunikation in der Europäischen Union realisiert werden müssen. Zudem wird die Europäische Union insoweit im Rahmen ihrer ausschließlichen Zuständigkeit tätig. Die Konferenz bittet auch die Entscheidungsträger auf Unionsebene sowie die Datenschutzbehörden der anderen Mitgliedsstaaten, diese Anregungen zu unterstützen.

Anlage 15

Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993Integriertes Verwaltungs- und Kontrollsystem (InVeKoS) (Verordnungen der EWG Nrn. 3508/92 und 3887/92)Die vom Ministerrat der EG 1992 beschlossene Reform der gemeinsamen Agrarpolitik sieht die Angleichung der gemeinschaftlichen Preise für bestimmte Kulturpflanzen an den Weltmarkt vor und gewährt auf Antrag als Ausgleich für die dadurch bedingten Einkommenseinbußen flächen- und tierbezogene Zuwendungen an die Erzeuger. Zur Verhinderung einer mißbräuchlichen Verwendung von Fördermitteln hat die EG die Mitgliedsstaaten dabei zur Einführung eines "Integrierten Verwaltungs- und Kontrollsystem (InVeKoS)" verpflichtet. Diese haben danach integrierte Datenbanken mit Angaben über Flurstücke, deren kulturartige Nutzung sowie den Tierbestand einzurichten und in einem Mindestumfang entsprechende Kontrollen durchzuführen.Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder hat die EG mit dem "Integrierten Verwaltungs- und Kontrollsystem" den Landwirtschaftsverwaltungen der Länder ein Überwachungssystem verordnet, das dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot, widersprechen kann. Insbesondere legt das EG-Recht für die Kontrolldichte nur ein Mindestmaß an Kontrollen, jedoch keine Obergrenze fest.Zur Vermeidung unverhältnismäßiger Einschränkungen des informationellen Selbstbestimmungsrechts der betroffe-

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