FREIE HANSESTADT BREMEN

Landesbeauftragter für den Datenschutz

Vorgelegt zum 31. März 1998

BREMISCHE BÜRGERSCHAFT **Drucksache 14/1005**
Landtag 21.04.98
14. Wahlperiode

20. Jahresbericht des Landesbeauftragten für den Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats meinen 20. Bericht über das Ergebnis meiner Tätigkeit im Jahre 1997 zum 31. März 1998 (§ 33 Abs. 1 Bremisches Datenschutzgesetz - BrDSG).

Dr. Stefan Walz, Landesbeauftragter für den Datenschutz

Inhaltsübersicht

1. Neue Herausforderungen an den Datenschutz durch technologische und europäische Entwicklungen

1.1 Umsetzung der EG-Datenschutzrichtlinie

1.1.1 Noch immer kein Kabinettsentwurf

Die Frist für die Anpassung des deutschen Datenschutzrechts an die EG-Richtlinie 95/46/EG („Datenschutzrichtlinie") läuft im Oktober 1998 ab (vgl. zuletzt 19. JB, Ziff. 5.1). Zwar wurde im Dezember 1997 ein Referentenentwurf zur Novellierung des Bundesdatenschutzgesetzes (BDSG) zur Stellungnahme an die Landesregierungen und Fachverbände geschickt, doch lag ein Kabinettsentwurf, der das Gesetzgebungsverfahren erst eröffnet, bis zum Redaktionsschluß dieses Berichts noch nicht vor. Die Prognose für die fristgemäße Umsetzung der EG-Vorgaben ist daher angesichts der zu Ende gehenden Legislaturperiode im Bund sehr ungünstig.

1.1.2 Reichweite der Reform: Minimalismus versus Modernisierung

Dabei herrscht bereits über das erforderliche Ausmaß der Reform des deutschen Datenschutzrechts keine Einigkeit. Die Debatte spielt sich ab zwischen den Polen eines defensiven Minimalismus einerseits und einer an den Entwicklungen der IuK-Technologie orientierten Modernisierung andererseits. Die Datenschutzbeauftragten gehören zur zweiten „Fraktion": Sie verlangen, daß die Gelegenheit der BDSG-Novellierung genutzt wird für eine Reaktion auf neue Technikrisiken wie z. B. Videoüberwachung, Chipkartentechnologie und Vernetzung. Die 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat diese Forderungen im Oktober 1997 noch einmal bekräftigt (vgl. den Text des Beschlusses u. Ziff. 22.6.).

Doch laufen alle Teilnehmer an der Novellierungsdebatte die gleiche Gefahr, die Diskussion über die Zukunft des Datenschutzes auf die Ebene der rechtlichen Regulierung zu verengen. Es gilt zu vermeiden, daß juristische Sandkastenspiele stattfinden, die ohne nennenswerten Einfluß auf die Entwicklung der Informationsgesellschaft bleiben.

Die Debatte über die Richtlinie in Deutschland wurde während ihrer Ausarbeitung, also seit 1990, von der Ministerialbürokratie, aber auch von den Wirtschaftsverbänden, vorrangig „strukturkonservativ" unter der Fragestellung geführt, wie unser — angeblich — bewährtes deutsches System vor der Aufnahme von ausländischen Rechtsordnungen stammenden Regelungselementen möglichst weitgehend geschützt werden kann. Betrachtet man die bis jetzt bekanntgewordenen Entwürfe aus dem Bundesinnenministerium und die zugehörigen Reaktionen, hat sich daran bis heute wenig geändert.

1.1.3 Anstöße für Alternativen zum deutschen System

Ohne Zweifel stellt die Richtlinie keinen konzeptionellen Neuentwurf „aus einem Guß" dar, sondern ein „patchwork" aus unterschiedlichen einzelstaatlichen Datenschutzsystemen: Der Sonderschutz für die sensitiven Daten (Art. 8) stammt u. a. aus Frankreich, das Registrierungssystem (Art. 18 ff.) kennen fast alle unsere Nachbarländer, die Anerkennung der von Verbänden ausgehandelten Verhaltensregeln (Art. 27) kommt aus den Niederlanden usw.. Die Grundstruktur der Richtlinie ist allerdings sehr „deutsch" ausgefallen. Belege für diese These sind u. a. die Begriffsbestimmungen, das Prinzip des „Verbots mit Erlaubnisvorbehalts", sowie die Enumerierung von Zulässigkeitstatbeständen, die denen des BDSG sehr ähnlich sind. Andere Länder wie Großbritannien oder Frankreich haben also erheblich größeren Umstellungsaufwand als Deutschland.

Für alle Mitgliedstaaten allerdings gilt der gleiche strukturelle Nachteil: Die Datenschutzgesetze der Mitgliedstaaten, aus denen das „patchwork" der Richtlinie zusammengesetzt ist, sind selbst wiederum auf dem Hintergrund eines inzwischen veralteten Technikszenarios entstanden. Bestes Beispiel dafür ist die in der Richtlinie vorgesehene generelle Registrierpflicht für Datenverarbeitungen (Art. 18 Abs. 1), die geprägt ist von der Vorstellung weniger, klar abgrenzbarer DV-Verfahren in einer Großrechnerlandschaft, eine von der Entwicklung der IuK-Technologie inzwischen überholte Konzeption (vgl. allerdings u. Ziff. 1.3.). Daher sind auch die neuen Gesetze Italiens und Griechenlands, die sich unmittelbar an der bereits verabschiedeten Richtlinie orientiert haben, ohne wirklich innovative Elemente.

Die immer wieder zu hörenden Klagen über die „Systemwidrigkeit" einiger Elemente der Richtlinie — bezogen auf das deutsche Regelungssystem — sind also nicht nur überzogen, vielmehr verkennen sie auch die Chance, die darin liegt, daß wir wegen des Drucks der Umsetzung der Richtlinie über Alternativen zu unserem deutschen Modell nachdenken (müssen). Dazu zwei Beispiele: Verhaltensregeln (Art. 27) bieten einen Rahmen, in dem sich Verbände oder sonstige Repräsentanten von Datennutzern und Betroffenen über ihre jeweiligen Interessen verständigen und faire Verarbeitungsbedingungen aushandeln können, etwa im Bereich des Direktmarketing oder der Versicherungen. Unseren gewohnten hoheitlich-normativen Rechtsvorstellungen sind sie zwar fremd. Aber: Verhaltensregeln delegieren Regelungsverantwortung; sie sind Elemente der Selbstregulierung bzw. „prozeduralen Rechts", das Rechtstheoretiker gerade für sich rasch verändernde gesellschaftliche Sachverhalte und Interessenlagen empfehlen. Daß „codes of conduct" auch ihre Schwächen im Hinblick auf Repräsentativität und Umsetzung in den jeweiligen Branchen haben, zeigt die niederländische Erfahrung.

Zweites Beispiel ist die Datenschutzkontrolle (Art. 28): Die anderen EG-Länder hatten und haben wenig Verständnis für die besonderen Befindlichkeiten des deutschen „dualen" Kontrollsystems mit unterschiedlichen Zuständigkeiten und Befugnissen von Datenschutzbeauftragten und Aufsichtsbehörden. Die Richtlinie geht konsequenterweise von einem einheitlichen Überwachungsstandard in Verwaltung und Wirtschaft aus. Für unsere EG-Partnerstaaten sind wirksame Eingriffsbefugnisse auch in der Privatwirtschaft ebenso selbstverständlich wie die einheitliche Wahrnehmung der Aufsichtsfunktion für den öffentlichen wie für den nicht-öffentlichen Bereich. Bei der anstehenden Novellierung muß daher § 38 BDSG erheblich nachgebessert werden.

1.1.4 Stärkung der individuellen Rechtsposition

Es gibt weitere Gründe, die Anforderungen der Richtlinie nicht defensiv abzuwehren, sondern offensiv zu akzeptieren. So stärkt die Richtlinie — gegenüber dem deutschen Niveau — die Rechtspositionen des Einzelnen gegenüber den Daten über ihn verarbeitenden Stellen. Das novellierte BDSG muß daher u. a.

- die Benachrichtigung des Betroffenen und die Information über seine Individualrechte verbessern,
- die Widerspruchsrechte stärken, auch gegenüber rechtmäßigem Datenumgang, sowie
- das Verbot automatisierter Persönlichkeitsprofile einführen, das für beamtenrechtliche Entscheidungen bereits verankert ist in § 56 f Abs. 4 BRRG.

So wichtig aber die Harmonisierung der einzelstaatlichen Datenschutzrechte „nach oben" ist, aus integrationspolitischer Sicht wichtiger ist der folgende Zusammenhang: Die Richtlinie ist Ausdruck der neuen grundrechtlichen Fundierung, die sich die Europäische Union im Maastricht-Vertrag gegeben hat und die in den Amsterdamer Vertrag ohne Änderung übernommen worden ist. Art. F Abs. 2 des EU-Vertrages stellt ausdrücklich fest, daß sich die Gemeinschaft nicht nur an die vom Europäischen Gerichtshof in langjähriger Rechtsprechung herausgearbeiteten gemeinsamen Verfassungsgrundsätze der Mitgliedstaaten gebunden fühlt, sondern an geschriebenes materielles europäisches „Verfassungsrecht", nämlich an die Europäische Menschenrechtskonvention von 1950. Die EMRK gewährleistet in Art. 8 den Schutz des Privatlebens explizit.

1.1.5 Selbstkritische Evaluation des deutschen Modells

Inwieweit die Harmonisierung der einzelstaatlichen Datenschutz-Rechtsordnungen aufgrund der Richtlinie gelingen wird, kann nicht nur durch grenzüberschreitenden Normenvergleich ermittelt werden. Entscheidend ist die Frage nach dem tatsächlich von den staatlichen und gesellschaftlichen Institutionen praktizierten Datenschutz. Selbstkritische Evaluation des eigenen nationalen Datenschutzsystems ist für eine Antwort auf diese Frage notwendige Bedingung. Sie stößt aber auf ein fundamentales empirisches Defizit.

Wir wissen wenig oder nichts Gesichertes

- über die Risikoeinschätzung der Bevölkerung (z. B.: Welche Datenschutzrisiken ängstigen am meisten, welche Datenschutzverstöße werden als gravierend empfunden?),

— über die tatsächliche soziale Verteilung von Datenschutzrisiken (z. B.: Sind Angehörige der Unterschichten oder Mittelschichten mehr von Adreßhandel und Direktmarketing betroffen?),

— über die Inanspruchnahme von Gegenrechten, Widerspruchsmöglichkeiten oder sonstigen datenschutzsichernden Verhaltensweisen (z. B.: Wie häufig wird der Nutzung zu Werbezwecken widersprochen? Wie oft werden erfragte Angaben verweigert?),

— über Implementationsdefizite des allgemeinen wie des bereichsspezifischen Datenschutzrechts (z. B.: Wer von den Millionen von Datennutzern kennt und/oder wendet wissentlich und/oder unwissentlich Datenschutzgesetze korrekt oder unkorrekt an?), oder

— über die tatsächliche Effizienz der Datenschutzbeauftragten und Aufsichtsbehörden (z. B.: Sind zahlreiche Eingaben Ausweis funktionierender Öffentlichkeitsarbeit oder unzulänglicher Kontrolltätigkeit?).

Natürlich gibt es Gründe für dieses Wissensdefizit. Zunächst und vor allem fehlt es an einem klaren Kriterienraster für die systematische Evaluierung von Datenschutzgesetzen und Datenschutzinstanzen. Das „Produkt Datenschutz" ist nicht an seinem Markterfolg meßbar, es kommt als Ergebnis eines komplexen Prozesses zahlreicher Akteure zustande. Die Definition des angestrebten Zustands optimaler „privacy protection", die Abwägung zwischen „berechtigten Interessen" der Datennutzer und „schutzwürdigen Belangen" der Betroffenen erfolgt jeweils subjektiv und hängt ab von Lebenswelten, Interessenlagen, Bildungsstand usw. Zwar können die regelmäßigen Jahres- und Tätigkeitsberichte der Datenschutzinstanzen deren Aktivitäten statistisch und damit ggf. auch empirisch evaluierbar ausweisen. Gemessen wird damit aber nur die „efficiency", also das Verhältnis von Aufwand und Ertrag, nicht aber die „effectiveness", also das Verhältnis von Output und wie auch immer definierter realer Verbesserung des Datenschutzes.

Kurz: Es fehlt eine ganzheitliche Perspektive des Datenschutzsystems, eine Perspektive, die das Datenschutzrecht, die Datennutzer, die Datenkontrolleure und die Betroffenen sowie deren Interaktionen umfaßt. Diese Zustandsbeschreibung müßte Ansporn sein für verstärkte Interaktion zwischen Datenschutzbeauftragten und Bürgern, vor allem aber für ein verstärktes Engagement von Sozialwissenschaftlern. Anders ausgedrückt: Datenschutz muß viel mehr als bisher Gegenstand empirischer Sozialforschung werden. Ohne eine gesamtheitliche Perspektive bleibt es bei der Fehlallokation knapper Datenschutzressourcen und dem Fehler, die Diskussion über Verbesserungen auf die Regulierungsebene zu beschränken.

1.2 Die Einwilligung als „Grundrechtsfalle"? — Datenschutz als Vertragsgegenstand?

Im Idealfall soll die Einwilligung Ausdruck und Konsequenz des Grundrechts auf informationelle Selbstbestimmung sein. Die Realität zeigt jedoch, daß sie zunehmend als Instrument der Grundrechtseinschränkung, als Hebel für die Umgehung des gesetzlichen Schutzsystems genutzt wird. Dies gilt insbesondere in ihrer Form als standardisierte Vertragsklausel etwa bei Banken und Versicherungen. Wegen der grundrechtlichen Verankerung des Datenschutzes und aufgrund der Volkszählungsrechtsprechung des Bundesverfassungsgerichts mit der von ihr statuierten „Drittwirkung" betrachtet die deutsche Doktrin allerdings die Individualrechte auch über die Aufzählung in § 6 BDSG hinaus als unabdingbar.

US-Ökonomen und -Sozialwissenschaftler dagegen akzeptieren vor dem ganz anderen Verfassungs- und Sozialmodell ihres Landes gesetzliche Einschränkungen der Dispositionsbefugnis des Individuums in seinem Interesse nicht. Vielmehr fragen sie ganz unbefangen: Warum sollte Datenschutz einschließlich der Betroffenenrechte nicht Teil von Markt- oder Vertragsbeziehungen sein, wenn funktionierender Wettbewerb mit gleichstarken Vertragspartnern besteht, der Verbraucher bei verschiedenen angebotenen Verarbeitungsvarianten frei über die Verwendung seiner Daten entscheiden und ggf. für die Nutzung sogar ein Entgelt oder einen Preisnachlaß verlangen kann? Wenn z. B. eine Telefongesellschaft niedrigere Gebühren als die Konkurrenz anbietet, dafür aber verlangt, daß ihr der Kunde die Auswertung der Verbindungsdaten zu Nutzungsprofilen oder zu Marketingzwecken erlaubt, warum sollte der Betroffene nicht in diese Zweckänderung zugunsten eines Rabatts einwilligen oder auf sein Widerspruchsrecht verzichten dürfen?

Dies heißt: Wenn einerseits die Einwilligung, Widerspruchsrechte oder sonstige Wahlmöglichkeiten des Betroffenen unverzichtbare Elemente eines wirksamen „Selbstdatenschutzes" sind und als Instrumente gesellschaftlich gewünscht zunehmender Entscheidungsspielräume an Bedeutung gewinnen, andererseits die Schutzgarantien der gesetzlichen Regelungen nicht unterlaufen werden sollen, muß man sich intensiver als bisher mit den Grenzen der Individualautonomie, d. h. ihrer Abgrenzung gegenüber unabdingbarem zwingendem Recht, beschäftigen. Wo die freie Ausübung des Rechts auf informationelle Selbstbestimmung aufhört und die staatliche Interventionspflicht zugunsten der Schwächeren beginnt, muß in der Informationsgesellschaft mit ihren zahlreichen interaktiven elektronischen Verkehrsformen neu definiert werden. Kernelement solcher Überlegungen wird die Definition der Voraussetzungen für die „Freiwilligkeit" sein, die die EG-Richtlinie explizit als Bedingung für eine wirksame Einwilligung nennt (Art. 2 lit. h).

1.3 Globale Technik versus nationales Recht

Mit dem Erlaß der EG-Richtlinie stellt sich die Frage nach der sinnvollen Regelungsebene für die Bewältigung gesellschaftlicher Technikfolgen mit neuer Aktualität. Ohne Zweifel: Globalisierung der Technikentwicklung und Nationalstaatlichkeit des Technikrechts passen auf Dauer nicht zusammen. Dies belegt die Entwicklung des INTERNET. Doch wer annimmt, wegen der globalen Vernetzung sei nationales Telekommunikations- oder Datenschutzrecht bereits jetzt weitgehend obsolet, schießt über das Ziel hinaus. Die große Mehrzahl der von BDSG oder vom Telekommunikationsgesetz (TKG) erfaßten Verarbeitungs-, DatenabrufundTelekommunikationsvorgänge spielt sich noch immer innerhalb der deutschen Grenzen ab. Auch die These, die Großrechnerlandschaft der siebziger Jahre existiere wegen der allgegenwärtigen Dezentralisierung und umfassenden Vernetzung der Datenverarbeitung überhaupt nicht mehr, verkennt die Realität. Nach wie vor gibt es in Deutschland riesige zentrale Datenbanken mit Millionen von Datensätzen (z. B. beim Verband Deutscher Rentenversicherungsträger, bei der Gebühreneinzugszentrale der Rundfunkanstalten, bei der Bundesanstalt für Arbeit usw.).

Gleichwohl werden Steuerungsdefizite des Rechts auch und gerade bei Datenschutz und Datensicherung unvermeidlich, wenn bestimmte Grundstandards sowohl für die technische Normung als auch für die Zulässigkeit der Nutzung grenzüberschreitender Netze nicht international vereinbart werden, was nicht zwingend durch verbindliches Völkerrecht, wie z. B. eine von der französischen Regierung vorgeschlagene „Internet-Konvention", geschehen muß. Die EG versucht dies auf der europäischen Ebene mit zahlreichen Richtlinien, Verordnungen und Empfehlungen. Zu nennen ist in diesem Kontext insbesondere die im Dezember 1997 endlich verabschiedete „ISDN-Richtlinie", die Teilelemente des Datenschutzes in der Telekommunikation harmonisieren soll (vgl. dazu 18. JB, Ziff. 20.13.).

Zu erwarten ist allerdings, daß selbst die EG als Regelungsebene nicht (mehr) ausreicht. Eine differenzierte Einschätzung kommt mithin zu dem Ergebnis, daß die IuK-Entwicklung sich in einer Phase rascher Internationalisierung befindet, in der sowohl grenzüberschreitende als auch nationale Regulierung ihren jeweiligen Stellenwert haben, der sich allerdings zunehmend zugunsten überstaatlicher Normsetzung verschiebt.

1.4 Multimedia: Konvergenz der Technologien — Konvergenz von Rechtsgebieten

Die Konvergenz der Technologien wird in wichtigen Kernelementen zu inhaltlicher Konvergenz der die unterschiedlichen Technologien regelnden Gesetze führen. Genauer ausgedrückt: Soweit Digitalisierung und Vernetzung Datenschutzrisiken erzeugen, müssen die Schutzanforderungen konsequenterweise quer durch herkömmliche Rechtsgebiete harmonisiert werden. Die Multimedia-Entwicklung wird m. a. W. die klassische Aufteilung von Presserecht, Rundfunkrecht, Datenschutzrecht und Telekommunikationsrecht zumindest teilweise aufheben. Damit wird auch die traditionelle Abgrenzung zwischen öffentlichem und Privatrecht porös.

Illustratives Beispiel: Programme für den Zugriff durch Netznutzer sollen — zumindest optional — Anonymität gewährleisten und Nutzungsprofile verhindern, um soziale Kontrolle zu vermeiden. Dies gilt völlig gleich, ob man eine

elektronische Zeitung liest (Presserecht), einzelne Rundfunksendungen interaktiv anfordert (pay-per-view = Rundfunkrecht), telefoniert (Telekommunikationsrecht) oder einen Tele- bzw. Mediendienst (Teledienste- bzw. Teledienstedatenschutzgesetz-TDG/TDDSG, Mediendienstestaatsvertrag-MDStV) abruft. Die deutsche Rechtsentwicklung mit in wichtigen Punkten übereinstimmenden Datenschutzregelungen in TKG, TDG bzw. TDDSG, Mediendienstestaatsvertrag und hoffentlich in Zukunft auch im derzeit vorbereiteten Staatsvertrag über den digitalen Rundfunk geht daher in die richtige Richtung.

1.5 Datenschutzfreundliche Technik — Widerstände und Perspektiven

Datenschutzfördernde Techniken (Privacy Enhancing Technologies, PETs) wie Verschlüsselung, anonymisierte Zugriffsverfahren etc. werden derzeit von vielen als „Königsweg" eines modernen Datenschutzes angesehen. Zweifellos sind sie wichtige Instrumente informationeller Selbstbestimmung in der Informationsgesellschaft. So verhindert z. B. eine anonyme Zugangssoftware zu Datenbanken und Telediensten den „gläsernen" Netzbürger. Die gesetzliche Verpflichtung, solche Techniken einzuführen, stößt allerdings auf erhebliche ökonomische Gegeninteressen. So sind z. B. Telenutzungsdaten von großem Nutzen für die Ermittlung der Kundenakzeptanz von Angeboten oder für Werbezwecke. § 4 Abs. 1 TDDSG läßt den Diensteanbietern die Hintertür offen, daß anonyme Zugangsmöglichkeiten nur insoweit angeboten werden müssen, als dies „technisch möglich und zumutbar ist". Daher besteht jetzt ein Wettlauf mit der Zeit: Nur wenn datenschutzfreundliche Verfahrenselemente so früh wie möglich in die Systemgestaltung einbezogen werden, läßt sich eine spätere Berufung auf technische Unmöglichkeit oder Unzumutbarkeit von vornherein verhindern. Diese Situation droht beispielsweise bei der für den Empfang digitalen Fernsehens vorgesehenen Set-Top-Box.

Gegen die Ablehnung von PETs hilft vor allem das Risiko der Bestrafung durch den Markt. Technologien, die risikobehaftet sind oder erscheinen, droht Akzeptanzverlust bei den (Tele-)Kunden. Wird Vertrauen in eine Technik — etwa in die Sicherheitsfeatures beim Tele-Banking — auch nur ein einziges Mal nachhaltig und durch Medien verstärkt erschüttert, läßt es sich nur langfristig und kostspielig wieder herstellen. Zur Durchsetzung von datenschutzfördernder Technik genügen allerdings negative Risikoszenarien nicht. Vielmehr braucht „der Datenschutz" dazu vor allem Interessenallianzen, etwa mit dem Verbraucherschutz bei den Telediensten oder mit der an elektronischem Geschäftsverkehr interessierten Wirtschaft bei der Verschlüsselung.

Die datenschutzfreundliche Gestaltung von Systemen und Verfahren allein genügt aber nicht. Sie wird nur dann effektiv, wenn Anwender bzw. Verbraucher über ausreichende Mediennutzungs- bzw. Technikkompetenz verfügen, d. h. genügend über die Risiken der Netznutzung und ihre gesetzlichen oder vertraglichen Rechte informiert sind. Ohne hohe Benutzerfreundlichkeit und viel know-how-Vermittlung bleibt der technische Selbstdatenschutz auf „Computerfreaks" begrenzt.

Schließlich muß der Stellenwert technischer Vorkehrungen im Gesamtsystem des Datenschutzes realistisch bewertet werden: Technischer Datenschutz kann wertorientierten Grundrechtsschutz durchsetzen helfen, nicht aber ihn ersetzen. Auch wenn sich Grundrechtsschutz und Verbraucherschutz des Netzbürgers teilweise überlappen, auch wenn die „Drittwirkung" des Rechts auf informationelle Selbstbestimmung in vertragliche Beziehungen eingreift: Der Bürger als Grundrechtsträger wird deswegen nicht reduziert auf den Verbraucher als Vertragspartner.

2. Die Rechtsentwicklung auf Bundesebene — Gewinn- und Verlustrechnung

2.1. Kritik

2.1.1 Kontrollintensität steigt

Auch 1997 war wieder ein Jahr, in dem zahlreiche neue Bundesgesetze verabschiedet worden sind, die Eingriffe in das Persönlichkeitsrecht der Bürgerinnen und Bürger vorsehen oder erfordern. Der politische Wille der letzten Jahre (vgl. dazu zuletzt 19. JB, Ziff. 1.2) zu verstärkter Kontrolle des Einzelnen im Sozialleistungsbereich besteht mindestens in gleicher Intensität fort wie die Absicht des Gesetzgebers, die Eingriffsbefugnisse der Sicherheitsbehörden kontinuierlich auszuweiten. Anregungen und Kritik der Datenschutzbeauftragten fanden nur

teilweise Gehör, zahlreiche ihrer auf ihre spezifische professionelle Erfahrung gestützten Einwände haben Regierung und Parlamentsmehrheit dagegen verworfen.

Eine komplette Übersicht über die einzelnen datenschutzrelevanten Neuregelungen eines Berichtsjahres, wie ich sie in früheren Berichten gegeben hatte (vgl. zuletzt 17. JB, Ziff. 1.2.), ist angesichts der Produktivität und Geschwindigkeit der Gesetzgebungsmaschinerie und der vielfach an versteckter Stelle erfolgten Änderungen und Ergänzungen mit vertretbarem Aufwand nicht mehr möglich. Daher werden in diesem 20. Bericht lediglich einige für die Datenschutzentwicklung zentrale Gesetzesnovellierungen thematisiert.

2.1.2 „Großer Lauschangriff"

Das für die rechtsstaatliche Situation in diesem Land bedeutsamste Ereignis war sicherlich die Verfassungsänderung zur Einführung des sog. Großen Lauschangriffs. Um das akustische Abhören von Wohnungen zu Zwecken der Strafverfolgung zu ermöglichen, beschloß der Bundestag am 16. Januar 1998, das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 Grundgesetz) weiter einzuschränken und die Strafprozeßordnung (StPO) entsprechend zu erweitern. Der Bundesrat stimmte am 6. Februar zwar der Grundgesetzänderung zu, rief aber für die Ausführungsgesetze den Vermittlungsausschuß an. Im Vermittlungsausschuß wurde dann eine Fassung angenommen, die alle in § 53 Abs. 1 StPO aufgezählten Berufsgeheimnisträger von der Überwachung ausnimmt. Das Vermittlungsergebnis wurde vom Bundestag am 6. März 1998 unverändert beschlossen (vgl. BR-Drs. 214/98 u. 214/98-Beschluß).

Vorausgegangen war der Intervention des Bundesrates eine breite gesellschaftliche Protestbewegung, die sich auf die Gefährdung der Zeugnisverweigerungsrechte konzentrierte und daher in erster Linie getragen war von den betroffenen Berufsgruppen der Journalisten, Ärzte und Anwälte. Ich habe ebenso wie eine Reihe meiner Länderkollegen Zielsetzung und Argumente dieser aus gegenüber der Strafverfolgung übergeordneten gesellschaftlichen Werten privilegierten Berufsgruppen unterstützt, auf Bundesebene wie in Bremen.

Gleichwohl standen für mich die grundsätzlichen verfassungsrechtlichen und datenschutzpolitischen Bedenken dieses schweren Grundrechtseingriffs im Vordergrund.

Zunächst: Mit dem legalen Abhören von Privatwohnungen wird eine Tabugrenze für staatliche Grundrechtseingriffe überschritten. Seit 1992 sind zahlreiche neue Fahndungsmethoden gesetzlich ermöglicht worden. Dazu gehören Rasterfahndung, beobachtende Fahndung und Aufzeichnung von Auslandsgesprächen nach dem „Staubsaugerprinzip". Bis heute gibt es keine solide Evaluation von Umfang und Qualität der dadurch erzielten Ermittlungserfolge oder -mißerfolge. Gleichwohl ist ohne empirische Basis zusätzlich die besonders schutzwürdige Unverletzlichkeit der Wohnung (Art. 13 Grundgesetz) eingeschränkt worden.

Sodann: Betroffen von Abhörmaßnahmen sind keineswegs nur überführte Straftäter, wie der Begriff „Gangsterwohnungen" suggeriert. Zum einen soll der Lauschangriff ja erst bestätigen, daß es sich bei Verdächtigen tatsächlich um Schwerkriminelle handelt. Zum anderen werden auch die vielen Unbeteiligten, die sich in möglicherweise über mehrere Wochen „verwanzten" Privaträumen aufhalten, belauscht. Es soll ja genügen, daß sich Beschuldigte in den Räumen dritter Personen „vermutlich aufhalten".

Und schließlich sind die vorgesehenen sog. grundrechtssichernden Maßnahmen, die den Eingriff in die Intimsphäre abfedern sollen, von zweifelhafter Schutzwirkung.

- Der Vorbehalt der richterlichen Anordnung hat im Parallelbereich der Telefonüberwachung den drastischen Anstieg der Fallzahlen nicht verhindert.

- Daß ohne die Abhörmaßnahme die Erforschung der Straftat aussichtslos oder wesentlich erschwert sein muß, ist eine bereits mehrfach vorhandene Einschränkung: Das sog. ultima-ratio-Prinzip gilt schon nach geltendem Recht für die Rasterfahndung und Tonband- und Videoaufzeichnungen außerhalb von Wohnungen. Wollte der Richter diese Voraussetzung kontrollieren, müßte er bei einem Antrag auf akustische Überwachung im einzelnen die Mißerfolge der jeweils schwächeren Aufklärungsbefugnisse prüfen, eine unter dem üblichen

Zeitdruck der gerichtlichen Praxis voraussichtlich wenig gründliche Handhabung.

— Die Zweckbindung der erlauschten Informationen für die Verfolgung schwerer Straftaten ist nicht gewährleistet. Gesprächsinhalte, die mit dem verfolgten Verbrechen nichts zu tun haben, können auch für Bagatelldelikte verwendet werden, zwar nicht als Beweismittel, aber als sog. „Ermittlungsansatz" für weitere Nachforschungen.

2.1.3 Weitere Sicherheits- und Justizgesetze

Auch die EUROPOL-Konvention wurde angenommen, obwohl die nicht nur von Datenschützern, sondern auch im Bundestag selbst geäußerte Kritik sowohl an dem unklaren Speicherumfang der sog. Analysedateien (vgl. die Entschließung der Datenschutzkonferenz u. Ziff. 22.4.) als auch an dem Immunitätsstatus der Europol-Beamten bei Datenmißbrauch nicht ausgeräumt worden ist. Auch beim Gesetz über das Bundeskriminalamt (BKA-Gesetz), dem Begleitgesetz zum Telekommunikationsgesetz (TK-Begleitgesetz), das Einzelheiten der staatlichen Kontrolle in diesem Bereich regelt, und dem Justizmitteilungsgesetz (vgl. dazu 18. JB, Ziff. 6.1 und u. Ziff. 13.6.) haben sich die Datenschutzbeauftragten in vielen Punkten vergeblich für Verbesserungen zugunsten rechtsstaatlicher Liberalität eingesetzt.

2.1.4 Sozialleistungsbereich — neue Datenabgleiche

Im Sozialleistungsbereich ist das Netz für Datenaustausch und Datenabgleich mit zahlreichen, kaum noch überschaubaren Änderungen des Sozialgesetzbuchs und dem Erlaß einschlägiger Rechtsverordnungen noch engmaschiger geknüpft worden (vgl. dazu ausführl. Ziff. 14.9.). Bei allem Verständnis für die Notwendigkeit, Sozialleistungsmißbrauch verstärkt zu bekämpfen: Mit der jetzt erreichten Kontrolldichte und den — etwa in einem Arbeitskreis der Sozialministerkonferenz — angestellten Überlegungen, die Überwachung noch weiter auszubauen, wird der prinzipielle Ansatz immer deutlicher, daß potentiell alle Leistungsbezieher in allen Zweigen des sozialen Sicherungssystems tendenziell unter Betrugsverdacht stehen. Das Fazit: Die Inanspruchnahme sozialer Leistungen, gutes Recht im Sozialstaat, löst ohne vorherige Rücksprache mit den Antragstellern eine für die Betroffenen undurchschaubare Kette von Kontrollmaßnahmen aus.

2.1.5 BDSG-Novellierung stagniert

Zu der notwendigen Novellierung des Bundesdatenschutzgesetzes, die die Rechte der Betroffenen und der Datenschutzkontrollbehörden an den höheren Standard der europäischen Richtlinie anpaßt, ist es nicht gekommen. Das Gesetzgebungsverfahren ist derzeit im Stadium ministerieller Textentwürfe stecken geblieben, so daß jetzt kaum noch zu verhindern ist, daß Deutschland die europarechtlich verbindliche Umsetzungsfrist bis zum Oktober 1998 nicht einhalten wird (vgl. dazu oben Ziff. 1.1.1.). Auch die rechtzeitige Anpassung des gleichfalls änderungsbedürftigen Landesdatenschutzgesetzes wird damit behindert.

In der Bilanz ergibt sich auf Bundesebene im Berichtsjahr ein klares Mißverhältnis zwischen den Datenschutz einschränkenden und den Datenschutz verbessernden Neuregelungen. Anders ausgedrückt: Viel Eingriffs- steht wenig Schutzgesetzgebung gegenüber.

2.2 Fortschritte

2.2.1 Zukunftsorientierte Multimedia-Gesetzgebung

Gleichwohl bleibt die Haben-Seite nicht ganz leer, im Gegenteil: Mit dem am 1. August 1997 in Kraft getretenen neuen Multimedia-Recht (Teledienstegesetz, Teledienstedatenschutzgesetz, Gesetz über die digitale Signatur, Mediendienstestaatsvertrag der Länder) ist Deutschland das erste europäische Land, das wichtige rechtliche Weichen für die sozialverträgliche Gestaltung einer durch globale Vernetzung und interaktive Telekommunikation geprägten Informationsgesellschaft gestellt hat. Das Prinzip der Datenvermeidung und das Gebot anonymer Nutzungsmöglichkeit bei Telediensten (z. B. Telebanking, Teleshopping) sollen dafür sorgen, daß der Netzbürger nicht zum „gläsernen Fahrer auf der Datenautobahn" wird, sondern frei von der Befürchtung staatlicher oder sozialer Kontrolle am häuslichen Bildschirm sich informieren, bestellen oder elektronische Briefe austauschen kann. Jetzt kommt es entscheidend darauf an, daß die Telediensteanbieter, aber auch die Hersteller und Entwickler der für den online-Betrieb vorge-

sehenen Geräte und Programme die Vorgaben des neuen Multimedia-Rechts zügig umsetzen. Ansonsten bleiben die erreichten Rechtsfortschritte auf dem Papier.

2.2.2 Verschlüsselungsfreiheit (vorerst) gewahrt

Kontraproduktiv für eine liberal-rechtsstaatlich verfaßte Informationsgesellschaft ebenso wie für die Zukunftsbranche des elektronischen Geschäftsverkehrs wäre auch jede Einschränkung der technischen Möglichkeit oder rechtlichen Befugnis, über Netz gesandte Nachrichten zu verschlüsseln. Anläufe des Bundesinnenministeriums, mit einem Kryptogesetz oder mittels technischer Vorgaben wie vorgeschriebener Chips den Sicherheitsbehörden „elektronische Nachschlüssel" zu verschaffen, hatten im Berichtsjahr keinen Erfolg, vor allem wegen des Widerstands aus der Wirtschaft und wegen rechtlicher Bedenken des Bundesjustizministeriums. Nach jüngsten Presseberichten im Februar 1998 ist aber damit zu rechnen, daß diese Pläne in Bonn weiterverfolgt werden. „Hände weg vom Netz" muß da — plakativ gesprochen — die Devise lauten.

2.2.3 Fortschritte in Brüssel

Positives ist auch für die EG-Ebene zu vermelden. Der Amsterdamer Vertrag vom Juni 1997, der den Vertrag über die Europäische Union (Maastricht I) ändert und ergänzt und am 1. Januar 1999 in Kraft treten soll, legt mit dem neu eingefügten Art. 250 zum ersten Mal ausdrücklich fest, daß auch die Institutionen der Europäischen Gemeinschaft sich bei der Verarbeitung personenbezogener Angaben an das von ihr den Mitgliedstaaten vorgegebene Datenschutzrecht zu halten haben. Über die Einhaltung dieser Verpflichtung wird eine EG-eigene Kontrollinstanz wachen (Art. 286). Damit wird die von den Datenschutzbeauftragten der Mitgliedstaaten zu wiederholten Malen kritisierte Datenschutzlücke in Brüssel geschlossen (vgl. auch u. Ziff. 8.1.).

3. Zur Entwicklung in Bremen

3.1 Plus ...

3.1.1 Grundrecht auf Datenschutz

Seit dem 15. Oktober 1997 haben die Bremer Bürgerinnen und Bürger ein ausdrücklich verbrieftes Grundrecht auf Datenschutz. Die neuen Absätze 3 bis 5 des Artikels 12 der Landesverfassung (vgl. Brem.GBl. Nr. 49 v. 27. Oktober 1997, S. 353; zur Vorgeschichte vgl. 19. JB, Ziff. 7.2.) markieren zweifelsohne den gesetzgeberischen Höhepunkt des Berichtsjahrs. Bemerkenswert ist auch die neue verfassungsrechtliche Verpflichtung staatlicher Stellen, bei der Aufgabenwahrnehmung durch private Dritte („Outsourcing") für die Einhaltung des in der Verwaltung geltenden Datenschutzstandards zu sorgen (Art. 12 Abs. 5 LV). Zugrunde liegt das Prinzip, daß Privatisierung öffentlicher Aufgaben nicht zu verringertem Datenschutz für die Bürger führen darf.

Die Verfassungsänderung ist in diesem Punkt durch den Datenschutzausschuß intensiv vorbereitet und auch im nichtständigen Ausschuß zur Reform der Landesverfassung eingehend beraten worden. Bremen ist das bisher einzige „alte" Bundesland, das nach der Wende dem Datenschutz Grundrechtsgeltung verschafft und damit ein wichtiges Signal für eine die Persönlichkeitsrechte der Bürger wahrende Entwicklung der Informationsgesellschaft gesetzt hat.

3.1.2 Datenschutzordnung der Bürgerschaft

Ganz oben auf die „Positiv-Liste" gehört auch die Datenschutzordnung (DS-O) der Bremischen Bürgerschaft, die seit September 1997 gilt und der ebenfalls intensive Ausschußberatungen vorausgegangen sind (vgl. 19. JB, Ziff. 7.3.). Damit verpflichtet sich die Legislative, für die das Bremische Datenschutzgesetz direkt nicht gilt, beim Umgang mit personenbezogenen Daten zu parlamentarischen Zwecken zur Wahrung von Vertraulichkeit, Zweckbindung etc. und gewährt den Betroffenen die üblichen Individualrechte, z. B. auf Auskunft. Damit hat die Bürgerschaft generell die Voraussetzung dafür geschaffen, daß schutzwürdige Belange der Bürger nicht tangiert werden, wenn die senatorischen Behörden persönliche Angaben übermitteln, um den Informationsrechten des Parlaments zu entsprechen.

Allerdings reicht die bloße Existenz der Datenschutzordnung als Anlage zur Geschäftsordnung nicht aus. Vielmehr verlangt sie von den Abgeordneten und/oder der Bürgerschaftsverwaltung im Einzelfall je nach Sensibilität der betroffenen Daten entsprechende konkrete Schutzmaßnahmen wie z. B. die

Behandlung in nicht-öffentlicher Sitzung (vgl. § 7 DS-O). Darauf mußte ich im Zusammenhang mit der Vorbereitung des Untersuchungsausschusses zu den Vorfällen in der Justizvollzugsanstalt Oslebshausen aufmerksam machen.

3.1.3 Beispiele gelungener Kooperation

Intensive Kooperation der Verwaltung mit meiner Dienststelle hat bei einer Reihe von Vorhaben der Verwaltung zu einer erfreulich weitgehenden Einbeziehung von Datenschutzbelangen geführt. Stellvertretend für den Bereich Neuregelungen seien erwähnt das — besonders sensible Gesundheitsangaben betreffende — Krebsregistergesetz (vgl. u. Ziff. 14.1.) und die Meldedatenübermittlungsverordnung (vgl. u. Ziff. 12.8.2.). Positiv vermerke ich z. B. auch, daß die SKP meine Dienststelle in die Planungen für das Bremische Verwaltungsnetz und die Vorbereitung der zugehörigen Ausschreibungen ebenso wie bei ihren DV-Vorhaben im Personalwesen wie z. B. dem Projekt Gesundheitsförderung im öffentlichen Dienst (vgl. u. Ziff. 11.6.) frühzeitig einbezogen hat.

3.2 ... und minus

3.2.1 Fehlende Regelungen — zu späte Beteiligung

Doch gibt es auch in diesem Berichtsjahr wieder eine Reihe von Anlässen für Kritik. Wichtige bereichsspezifische Regelungen wie etwa die Durchführungsverordnung zum bereits 1995 in Kraft getretenen Gesetz über den Öffentlichen Gesundheitsdienst (ÖGD-G) oder das aufgrund bundesgesetzlicher Vorgaben seit längerem dringend novellierungsbedürftige Landesmeldegesetz (vgl. ausf. u. Ziff. 12.8.1.) kommen nicht voran. Von wichtigen Projekten erfahre ich entgegen der im BrDSG festgelegten Informationspflicht der Verwaltung zu spät wie etwa von der Einrichtung von E-Mail-Kommunikation mit Bürgern (vgl. u. Ziff. 9.1.2.). Zeitverlust und mehr Verwaltungsaufwand ergeben sich auch dann, wenn ich meine Beteiligung ausdrücklich anmahnen muß wie etwa bei der vorgesehenen (Teil-) Privatisierung der Informations- und Datentechnik Bremen. Sie wirft eine Reihe schwieriger und tunlichst im Vorfeld von Verkaufsentscheidungen zu klärender datenschutzrechtlicher Fragestellungen auf, wie sich auch bei der Befassung des Datenschutzausschusses mit diesem Thema gezeigt hat.

Auf die Negativliste gehört auch, wenn Zusagen selbst gegenüber dem Datenschutzausschuß nachträglich in Frage gestellt werden oder sich als nicht eingehalten erweisen. Ein Beispiel dafür sind die zunächst vom Innensenator in Aussicht gestellten, später aber für nicht erforderlich erklärten Regelungen für die Rundfunkberichterstattung von Polizeieinsätzen vor dem Hintergrund der umstrittenen „Stradivari"-Fernsehdokumentation (vgl. u. Ziff. 10.2.2.2.). Oder: Ein versprochenes Schreiben des Innensenators an den Bundesinnenminister zur Verbesserung der Protokollierung von Datenzugriffen auf das Ausländerzentralregister wurde nie abgesandt (vgl. dazu u. Ziff. 10.2.1.). Schließlich betrachte ich es — zurückhaltend ausgedrückt — als unkooperativ, wenn ich auf z. T. ausführliche Stellungnahmen wie die zu den Verwaltungsvorschriften zum Ausländergesetz überhaupt keine Rückäußerung erhalte (vgl. u. Ziff. 12.6.).

3.2.2 Einschränkung der Kontrollbefugnisse des LfD?

Besonders betroffen gemacht hat mich allerdings der Versuch, im Entwurf für ein neues Sicherheitsüberprüfungsgesetz (SÜG) meine Kontrollbefugnisse durch partielle Wiedereinführung der sog. Staatswohlklausel einzuschränken und damit einen für den Landesbeauftragten für den Datenschutz kontrollfreien Raum zu schaffen. Die Einschränkung meiner Überwachungsmöglichkeiten soll entgegen der bisherigen Rechtslage ausgerechnet bei Sicherheitsakten möglich werden, die ungeprüfte Angaben Dritter, subjektive Einschätzungen befragter Referenzpersonen, rufschädigende Gerüchte etc. enthalten können und für die den überprüften Personen selbst das Auskunfts- und Einsichtsrecht vorenthalten wird (vgl. ausf. u. Ziff. 12.1.). Ich habe mich u. a. in Schreiben an die Fraktionsvorsitzenden in der Bürgerschaft und in den Beratungen des Datenschutzausschusses nachdrücklich gegen diese Absichten gewandt. Bei Redaktionsschluß war eine endgültige parlamentarische Entscheidung noch nicht getroffen.

3.2.3 Beanstandungen

Von meinem schärfsten gesetzlichen Instrument, der förmlichen Beanstandung nach § 29 BrDSG, mußte ich (nur) in zwei Fällen Gebrauch machen: In einem Fall ging es um die unberechtigte Beschaffung von Patientendaten unter Mißach-

tung des Arztgeheimnisses — der Fall ist noch nicht abgeschlossen —, im anderen um die Verletzung des Sozialgeheimnisses mit nachteiligen Auswirkungen für den Betroffenen in seinem Kündigungsschutzverfahren. In diesem zweiten Fall, der sich in Bremerhaven abgespielt hat, ist positiv zu vermerken, daß zwar die Leitung des zuständigen Amtes uneinsichtig war, der Magistrat aber dann den Verstoß eingeräumt und bedauert sowie entsprechende Anweisungen getroffen hat (vgl. u. Ziff. 19.1.). In mehreren Fällen mußte ich die förmliche Beanstandung androhen, um die Einhaltung gesetzlicher Vorgaben sicherzustellen oder zu beschleunigen (vgl. z. B. Ziff. 14.8. betr. die Werkstatt Bremen).

3.3 Nach wie vor unverzichtbar: Kontrollen vor Ort

Die Rolle von Datenschutzbeauftragten wird gründlich verkannt, wenn man sie als „Datenstaatsanwälte" versteht, die vorrangig und auch erst im nachhinein nach Gesetzesverstößen und Sicherungsmängeln suchen. Beratung von Behörden und Firmen bei der Vorbereitung von Regelungen und IuK-Projekten muß Schwerpunkt richtig verstandenen Datenschutzes sein. „Prävention geht vor Sanktion" muß die Devise lauten.

Gleichwohl bleiben Kontrollen vor Ort, d. h. die konkrete Prüfung von Akten, Dateien und Netzen in Behörden und Privatfirmen, als komplementäres Instrument unverzichtbar. „Papier ist geduldig"; dies gilt auch und gerade für mir vorgelegte Datenschutzkonzepte. Selten ist es böser Wille, häufiger Nachlässigkeit und Vergeßlichkeit, die zu unzulässigen Verarbeitungsvorgängen oder zu Sicherungsmängeln führen. Für jedes Jahr stelle ich daher einen Prüfplan auf mit den Objekten, die für Kontrollen aufgesucht werden sollen; aus aktuellem Anlaß wird die Liste ggf. ergänzt.

In diesem Bericht werden nur einige Prüfergebnisse herausgegriffen. Sie betreffen im öffentlichen Bereich u. a. den Umgang mit Akten aus Sicherheitsüberprüfungsverfahren (vgl. u. Ziff. 12.2.), das DV-System eines Krankenhauses (vgl. u. Ziff. 14.5.) und das Abrechnungsverfahren für die Sozialhilfe (vgl. u. Ziff. 14.6.). Die Prüfergebnisse in meiner Funktion als Aufsichtsbehörde, also bei privaten Unternehmen, sind unter Ziff. 21.2. zusammengefaßt.

3.4 Reaktionen der Öffentlichkeit

Daß die Aufmerksamkeit und das Interesse der Bürgerinnen und Bürger am Datenschutz keineswegs nachlassen, zeigen die Zahlen der bei mir eingegangenen Eingaben und Beschwerden (vgl. u. Ziff. 5.). Sie häufen sich insbesondere bei unseriösen Fragebogenaktionen von Adreßhandels- und Direktmarketingfirmen (vgl. u. Ziff. 20.3.). Bei diesen Umfragen zu Werbezwecken sind leider meine Interventionsmöglichkeiten beschränkt, sei es wegen örtlicher Unzuständigkeit, weil die Unternehmen ihren Sitz außerhalb Bremens haben, sei es wegen der unbefriedigenden Rechtslage nach § 38 BDSG, die kein Verbot rechtswidriger Datenverarbeitungen vorsieht.

Auch die Bürgersprechstunde in meinem Bremer Büro (donnerstags von 15-18 Uhr; vgl. 19. JB, Ziff. 2.2.) wird nach wie vor gut angenommen. Beleg für die große Nachfrage nach Informationen zum Datenschutz ist schließlich die hohe Zahl von Referaten, die meine Mitarbeiterinnen und Mitarbeiter und ich selbst im Berichtsjahr vor den unterschiedlichsten Auditorien gehalten haben. Die Einzelheiten und die statistische Aufbereitung der Presse- und Öffentlichkeitsarbeit sowie der Vortragstätigkeit sind unter Ziff. 6. und 7. wiedergegeben.

Eine Intensivierung und Beschleunigung der Kontakte sowohl mit Bürgerinnen und Bürgern, aber auch mit den bremischen öffentlichen wie privaten Stellen, erhoffe ich mir von dem E-Mail-Anschluß, mit dem meine Behörde seit kurzem erreichbar ist (officedatenschutz.bremen.de).

4. Redaktionelle Hinweise

Dieser Bericht enthält zwei redaktionelle Neuerungen. Zum ersten Mal habe ich Werbeanzeigen von mir als seriös bekannten Firmen und Verbänden aus dem Bereich Datenschutz und Datensicherung aufgenommen, um einen Teil der Druckkosten abzudecken. Mein knappes Budget stand für diese Idee Pate. Zum anderen habe ich unter Ziff. 23. eine zusammenfassende Auflistung sowohl von verfügbarem Informationsmaterial in Papierform als auch von Internet-Adressen abgedruckt, bei denen Berichte, Stellungnahmen, technische Orientierungshilfen und sonstige für die Öffentlichkeit bestimmte Dokumente der Datenschutzbeauftragten abgerufen werden können.

5. Bürgerberatung, Eingaben, Beschwerden und Hinweise

5.1 Bilanz in Zahlen

5.1.1 Schriftliche Eingaben

Ich kann schon aus arbeitsökonomischen Gründen keine vollständige Statistik aller Arbeitskontakte des LfD und seiner Mitarbeiter mit Bürgerinnen und Bürgern führen. Daher registriere ich die Zahl der telefonischen Anfragen und Hinweise oder die vielen Einzelgespräche bei Gelegenheit von Tagungen oder Fortbildungsveranstaltungen ebensowenig wie die Bitten um Zusendung von Informationsmaterial. Erfaßt und nach Stichworten vermerkt werden lediglich die schriftlichen Eingaben. Zahl und Inhalt dieser Schreiben zeigen, worüber sich die Bürgerinnen und Bürger besonders ärgern, in welchen Bereichen sie ihre Individualrechte einfordern und zu welchen Themen Informationsbedarf besteht.

5.1.2 Öffentlicher Bereich (Verwaltung)

Bis einschl. Januar 1998 habe ich insgesamt 158 Eingaben erhalten. 79 davon betrafen Stellen der öffentlichen Verwaltung in Bremen. Schwerpunkte waren die Bereiche Polizei (8), Krankenhäuser (7), Staatsanwaltschaften (6) sowie Sozialämter (5).

Im Bereich Polizei bezogen sich die Eingaben u. a. auf

- den Hinweis auf die frühere Berufstätigkeit in einer Verkehrsordnungswidrigkeiten-Angelegenheit,
- die Speicherung der Daten einer durch ein Delikt geschädigten Person,
- die Art und Weise der Überprüfung der Identitätsdaten eines Ausländers sowie
- mehrfach die Dauer der Speicherung im polizeilichen Informationssystem.

Die Kritik am Datenumgang im öffentlichen Gesundheitswesen und in den Krankenhäusern bezog sich u. a. auf folgende Fälle:

- die Unterdrückung der ISDN-Rufnummernanzeige bei Telefonaten aus dem Krankenhaus heraus,
- den angeblichen Mitschnitt von Telefongesprächen eines Chefarztes mit einem Patienten,
- die Einschaltung des Medizinischen Dienstes der Krankenkassen bei einer Psychotherapie-Erstattung und
- die Übermittlung von Patientenangaben an Religionsgesellschaften.

5.1.3 Nicht-öffentlicher Bereich (Privatwirtschaft)

79 Schreiben von Bürgerinnen und Bürgern hatten Datenschutzfragen in privaten Unternehmen zum Gegenstand. Die meisten von ihnen bezogen sich auf den Datenumgang von Auskunfteien (14). Jeweils mehrere Briefe betrafen Versicherungen (7), Kreditinstitute (5) und „Haushaltsumfragen" durch Adreßhandelsfirmen (5). Eine kleine Auswahl dieser Fälle ist im Kapitel 20. dargestellt. Insgesamt liegt der Anteil telefonisch abgewickelter Anfragen und Beschwerden im nichtöffentlichen Bereich höher als in bezug auf die Datenverarbeitung der Verwaltung.

5.2 Bremen-Sprechstunde

In meiner Dienststelle in Bremerhaven stehen meine Mitarbeiter und ich jederzeit für persönliche Beratungen auch außerhalb der üblichen Bürostunden zur Verfügung. Auf Wunsch besuche ich Betroffene auch zu Hause oder in ihren Geschäftsräumen. Seit Mai 1996 biete ich jeden Donnerstag von 15.00 bis 18.00 Uhr zusätzlich in meinem Bremer Büro eine Sprechstunde an. Dies gibt den in Bremen lebenden Bürgerinnen und Bürger die Möglichkeit, ihre Hinweise und Beschwerden persönlich und in Ruhe vortragen zu können, ohne jeweils im Einzelfall einen Termin vereinbaren oder ihre Angelegenheit telefonisch — und zwar per Ferngespräch — in Bremerhaven vortragen zu müssen. Die „Bremen-Sprechstunde" ist durch die ständig wiederkehrenden Pressehinweise inzwischen gut bekannt und hat sich als vergleichsweise unbürokratische Kontaktform bewährt.

6. Fortbildungs- und Vortragsveranstaltungen

6.1 Fortbildung

Aus Kapazitätsgründen kann meine Dienststelle kein eigenes Fortbildungsprogramm organisieren. Gleichwohl lege ich großen Wert darauf, daß Grundseminare zum Datenschutz für die bremischen Bediensteten im Rahmen des SKP-

Fortbildungsprogramms angeboten und von meinen Mitarbeitern abgehalten werden (zwei in 1997). Wichtig ist auch, daß die Anforderungen von Datenschutz und Datensicherheit künftigen Informatikern schon in der Ausbildung vermittelt werden. Daher nehme ich gerne die Gelegenheit wahr, daß Bedienstete meiner Dienststelle im Fachbereich Systemanalyse der Hochschule Bremerhaven die Kurse Datenschutz und Datensicherung I und II geben können. In die Kategorie der Schulung von Mitarbeiterinnen und Mitarbeitern für das an ihrem konkreten Arbeitsplatz eingesetzte Fachverfahren gehören die im Amt für Soziale Dienste stattfindenden zweitägigen Veranstaltungen im Rahmen der PROSOZ-Qualifikation (zwei im Berichtsjahr). Zum zweiten Mal habe ich 1997 im Rahmen des SKP-Fortbildungsprogramms für Leitungskräfte in der Verwaltung ein Seminar „Datenschutz als Führungsaufgabe" angeboten.

6.2 Vortragsveranstaltungen, Erfahrungsaustausch

Das Engagement im Bereich der Vortragstätigkeit steht ebenso wie das Angebot an Fortbildung (s. o. Ziff. 6.1.) unter dem Vorbehalt der beschränkten Kapazitäten; zu meinem Bedauern müssen meine Mitarbeiter und ich immer wieder Anfragen zu Veranstaltungen und Referaten ablehnen. Im Berichtsjahr haben wir uns auf Seminaren, Foren und Podiumsveranstaltungen u. a. zu folgenden Themen geäußert:

— „Multimedia und Internet — Was wird aus dem Datenschutz?",

— „Massenmedien und Multimedia — Ende des Medienprivilegs?",

— „Chipkarten — Chancen und Risiken",

— „Bedeutung des Datenschutzes für die bremische Wirtschaft",

— „Datenschutz und Datensicherung im Unternehmen — das BDSG und seine Umsetzung in der Praxis",

— „Verwaltung online — Bürger online".

Einlader der zu diesen Themen organisierten Veranstaltungen waren u. a. Bürgergruppen, Parteien, Kammern, Verbände, und Hochschulen. Der Schwerpunkt im Themenfeld „Multimedia" und „Informationsgesellschaft" entspricht dem des letzten Jahresberichts.

Besonders wichtig für den intensiven, „basisnahen" Kontakt mit interessierten Bürgerinnen und Bürgern sind Veranstaltungen, in denen das Gespräch und der gegenseitige Austausch von Erfahrungen in einer kleinen Gruppe Betroffener im Vordergrund stehen. Beispiel dafür ist eine Veranstaltung der Arbeitsgemeinschaft „Kind" im Ortsteil Lüssum zu Fragen der Nutzung und Weitergabe der Daten von Kindern und Eltern.

Einen weiteren Schwerpunkt versuche ich bei der Information der für den Datenschutz in den Unternehmen der Privatwirtschaft Verantwortlichen zu setzen. Aus diesem Grund informiere ich regelmäßig im Erfahrungskreis der betrieblichen Datenschutzbeauftragten bremischer Unternehmen über aktuelle Rechtsentwicklungen, zuletzt insbesondere über das seit dem 1. August 1997 geltende neue Multimediarecht des Bundes (vgl. o. 2.2.1.). Vom Erfahrungsaustausch mit den betrieblichen Praktikern profitiere ich bei meiner Beratungs- und Kontrolltätigkeit im nicht-öffentlichen Bereich nicht unerheblich.

Ein anderes Beispiel: In Bremerhaven habe ich mit freundlicher Unterstützung des dortigen Arbeitgeberverbands eine Informationsveranstaltung zum Thema „betrieblicher Datenschutz" mit über 30 Teilnehmern durchgeführt. Viele der anwesenden Firmenvertreter baten um weiteres Informationsmaterial, manche auch um Besprechungstermine zur vertieften Erörterung konkreter, ihren Betrieb betreffender Fragen. Auch diesen Veranstaltungstyp möchte ich wiederholen bzw. ausbauen.

7. Presse- und Öffentlichkeitsarbeit, LfD im Internet

Die Unterstützung einer kritischen Medienöffentlichkeit ist für die Schaffung von Problembewußtsein in Politik, Verwaltung und Wirtschaft für die Belange des Datenschutzes von großer Bedeutung. Vor allem aber geben die von den Medien aufgegriffenen aktuellen Fragen einen guten Überblick über die gerade aus der Sicht des Bürgers besonders relevanten Themen.

Meine Pressemitteilungen sowie Hörfunk- und Fernsehauftritte betrafen im Berichtsjahr u. a. die Themen „Verbraucherumfragen" durch Direktwerbefirmen,

die Adreßüberprüfungsaktion der Deutschen Post AG, Wahlwerbung durch die politischen Parteien, das Inkrafttreten der neuen Multimediagesetzgebung, das Recht auf Verschlüsselungsfreiheit, Schutzmöglichkeiten des Netzbürgers im Internet sowie — last but not least — den höchst umstrittenen sog. Großen Lauschangriff (vgl. dazu o. 2.1.2.).

Zusammen mit meinen Kollegen in Bayern, Berlin und Hamburg sowie der Fachhochschule München und der Datenschutzakademie Schleswig-Holstein habe ich das Faltblatt „Der betriebliche Datenschutzbeauftragte" herausgegeben. Es soll vor allem Neulinge in dieser Funktion kurz und bündig über den Datenschutz im Unternehmen sowie ihre Aufgaben und Befugnisse informieren. Dieses Informationsblatt kann bei meiner Dienststelle kostenlos angefordert werden.

Das Internet-Angebot meiner Dienststelle ist derzeit noch im Aufbau. Eine Reihe von Dokumenten ist aber bereits jetzt im „Netz der Netze" abrufbar.

Wichtiger Hinweis: Meine und meiner Kollegen Internet-Adressen sowie eine Gesamtliste der in Papierform verfügbaren und/oder im Internet zugänglichen Texte und Informationen zum Datenschutz finden sich unter Ziff. 23 auf S. 81 ff..

8. Europäischer Datenschutz

8.1 Fortschritte im Amsterdamer Vertrag

Einen wichtigen Schritt zu mehr Datenschutz auf der EG-Ebene macht der neue Amsterdamer Vertrag vom 2. Oktober 1997. Er fügt einen neuen Artikel 250 (vor der Nummernbereinigung Art. 213 b) in den Vertrag über die Europäische Union ein, der vorsieht, daß ab 1999 die für die Mitgliedstaaten geltenden Datenschutzrichtlinien und -verordnungen inhaltlich auch auf die durch den EU-Vertrag selbst oder sekundäres Gemeinschaftsrecht geschaffenen Gemeinschaftsorgane Anwendung finden. Damit wird die „Datenschutzlücke" geschlossen, die bisher für die u. a. von Kommission und Rat verarbeiteten, teilweise sensiblen personenbezogenen Daten — z. B. von Antragstellern, Subventionsempfängern oder den EG-Beamten selbst — bestand und die lediglich durch Interimslösungen wie z. B. interne Erlasse zu schließen versucht wurde. Damit wird auch eine Forderung erfüllt, die die Konferenzen der europäischen und deutschen Datenschutzbeauftragten seit Jahren aufgestellt hatten, die lautete: Die Gemeinschaft darf nach Inkrafttreten der Datenschutzrichtlinie in ihren Organen keinen schlechteren Schutzstandard für das Persönlichkeitsrecht der EG-Bürger aufweisen als die Mitgliedstaaten (vgl. 18. JB, Ziff. 5.1.3 und Ziff. 20.13). Die unabhängige Kontrollinstanz, die die Beachtung der Datenschutznormen durch die EG-Dienststellen überwachen soll — auch dies eine langjährige Forderung der Datenschutzbeauftragten auf deutscher wie auf EG-Ebene — soll sogar bereits vor dem Inkrafttreten des neuen EU-Vertrags am 1. Januar 1999 eingerichtet werden.

8.2 EG-weite Harmonisierung: Arbeitsweise und Themen der „Art. 29-Gruppe"

Auch die harmonisierte Umsetzung der Datenschutzrichtlinie in das einzelstaatliche Recht macht in einer Reihe von EG-Ländern schnelle Fortschritte, allerdings nicht in Deutschland, wo alle Anzeichen dafür sprechen, daß die Novellierung des BDSG nicht bis zum Ende der Anpassungsfrist im Oktober 1998 gelingen wird (vgl. o. Ziff. 2.1.5.). Eine Schlüsselrolle im Harmonisierungsprozeß kommt der auf der Grundlage von Art. 29 der Richtlinie gebildeten Arbeitsgruppe zu, über die ich bereits mehrfach berichtet habe (vgl. 18. JB Ziff. 5.1.4; 19. JB Ziff. 5.2).

Die Gruppe nach Art. 29 der Richtlinie hat zur Aufgabe, deren Umsetzung in das einzelstaatliche Recht zu begleiten und Zweifelsfragen der Interpretation im Interesse einer einheitlichen Anwendung zu beraten. Sie soll weiterhin die Kommission bei allen datenschutzrelevanten Gemeinschaftsmaßnahmen beraten (vgl. Art. 30). Die Gruppe ist unabhängig und besteht aus Vertretern der nationalen Datenschutzinstanzen. Als Sekretariat fungiert die Brüsseler Kommission. Deutschlands Datenschutzbehörden werden durch den Bundesbeauftragten als in der Regel stimmberechtigten „gemeinsamen Vertreter" nach Art. 29 Abs. 2 Satz 3 repräsentiert. Als seinen Stellvertreter für die Landesbeauftragten hat die Datenschutzkonferenz mich benannt.

Schwerpunkt der Arbeit in diesem Berichtsjahr war wie im letzten Jahr die zukünftige Verfahrensweise bei der Datenübermittlung in Staaten außerhalb der Gemeinschaft (Drittstaaten) (dazu sogleich Ziff. 8.3.). Weitere Beratungsthemen waren u. a. die künftige Registrierungspflicht für Datenverarbeitungen und die

dafür möglichen Modelle, die Behandlung von europaweiten Verhaltensrichtlinien für den Datenschutz z. B. in der Branche Direktmarketing und für Reservierungssysteme von Fluggesellschaften sowie gemeinschaftsweite Rahmenbedingungen für die Anonymität von Kommunikation über Internet. Zu allen Themen sind — deren Komplexität halber — die Beratungen noch nicht abgeschlossen.

8.3 Schwerpunktthema Adäquanzprinzip: die transatlantische Debatte

8.3.1 Materielle Adäquanz durch Gesetzgebung?

Art. 25 der Richtlinie verlangt für die Datenübermittlung aus der EG in Drittstaaten ein „angemessenes" Schutzniveau im Zielland. Sonst drohen äußerstenfalls Verbote von Datentransfers durch die Kontrollinstanzen. Wegen der engen internationalen Handelsverflechtungen und der damit verbundenen Datenströme haben dieses Adäquanzprinzip und seine möglichen Konsequenzen für den grenzüberschreitenden elektronischen Geschäftsverkehr eminente praktische Bedeutung. Dementsprechend stark fallen die Reaktionen in den hauptsächlich betroffenen Staaten außerhalb der EG aus, vor allem in den USA.

Die Ausgangspunkte von EG und USA sind kontrovers: Die Europäer zählen zum hard-core materieller Adäquanz vor allem klare Zulässigkeitsbedingungen (insbesondere die Zweckbindung), ein funktionierendes Beschwerdesystem für Bürger und Verbraucher und eine effiziente Aufsichtsinstanz. Die Gewährleistung dieser Verarbeitungsbedingungen soll vorzugsweise durch gesetzliche Querschnittsregelungen erfolgen. Doch liegen Regelungsformen und Regelungsebene nicht zwingend im Sinne der europäischen Systeme fest; „funktionale" Adäquanz des Datenschutzniveaus im Drittstaat soll ausreichen.

8.3.2 Adäquanz durch Selbstregulierung der Wirtschaft?

Die US-amerikanische Seite dagegen — d. h. die am Dialog beteiligten Beamten der Clinton-Administration, Wirtschaftsvertreter und Hochschullehrer — lehnen in ihrer großen Mehrheit gesetzliche Regelungen ab, jedenfalls in der EG üblichen Form allgemeiner Datenschutzgesetze. Dies sei einer common-law-Rechtsordnung systemfremd und im übrigen auch überflüssig; Datenschutz solle und könne ausreichend (nur) durch die Selbstregulierung der betroffenen Wirtschaftskreise sichergestellt werden.

Die Europäer wiederum replizieren, daß die Effizienz des self-regulation- Systems nachhaltig zu bezweifeln ist, was insbesondere durch die von der EG-Kommission in Auftrag gegebene Studie der amerikanischen Rechtsprofessoren Reidenberg und Schwartz über den Stand des Datenschutzes in den USA (Data Privacy Law, 1996) belegt werden könne. Auch die Behauptung der Systemwidrigkeit gesetzlicher Regelung wird bestritten durch Hinweis auf die sektoral zahlreich vorhandene datenschutzbezogene Gesetzgebung etwa im Fair Credit Reporting Act oder im Video Privacy Protection Act. Auch Kanada wird als Gegenbeleg herangezogen insofern, als dieser Staat trotz gemeinsamer common-law-Tradition nicht nur Datenschutzgesetze für den öffentlichen Bereich in Bund und Ländern aufweist, sondern auch seine Bereitschaft erklärt hat, diese Gesetzgebung auf die private Wirtschaft auszudehnen.

Derzeit ist die transatlantische Debatte, die auf einer Vielzahl von Tagungen und Kongressen geführt wurde und wird, in diesen Ausgangspositionen etwas festgefahren. Sicherlich wird es zu Kompromissen kommen, doch bedarf es dazu noch intensiver bilateraler Gespräche nicht zuletzt zwischen EG-Kommission und US-Regierung. Die Art. 29-Gruppe hat zur Versachlichung der Diskussion im Sommer 1997 ein ausführliches Positionspapier als Diskussionsgrundlage vorgelegt („Erste Leitlinien für die Übermittlung personenbezogener Daten in Drittländer — Mögliche Ansätze für eine Bewertung der Angemessenheit, EG-Komm XV D/5020/97-DE endgültig).

9. Technischer Datenschutz

9.1 Bremens Verwaltung am Netz

Während im 19. Jahresbericht nur von bremen.online, dem bremischen Angebot im Internet (www.bremen.de) die Rede war (vgl. 19. JB, Ziff. 6.1), ist inzwischen eine weitere Komponente in der Planung hinzugekommen: Über die o. a. Nutzungsmöglichkeiten hinaus ist beabsichtigt, in Kürze unter Verwendung des technischen Standards des Internet eine ähnliche Infrastruktur für verwaltungsinterne

Kommunikations- und Informationszwecke zur Verfügung zu stellen, also ein sog. Intranet mit der Bezeichnung Bremisches Verwaltungsnetz (BVN) in Betrieb zu nehmen (dazu u. Ziff. 9.1.4.). Beide Entwicklungen sind zwar eigenständig, haben aber gegenseitige Auswirkungen.

Im Bericht des Datenschutzausschusses zum 18. Jahresbericht (Drucksache 14/564 vom 21. Januar 1997), der von der Bürgerschaft angenommen wurde, wurde ich gebeten, bis zur Sommerpause 1997 einen Sachstandsbericht zur Zusammenarbeit von SKP und mir bei der Erstellung eines Sicherheitskonzepts für die Anschlüsse bremischer öffentlicher Stellen an das Internet vorzulegen. Dieser Sachstandsbericht wurde nach der Abstimmung mit der SKP mit Stand vom 7. Juli 1997 dem Datenschutzausschuß übergeben. Die folgende Darstellung greift teilweise in diesem Bericht gemachte Ausführungen auf, soweit sie bei Redaktionsschluß noch aktuell waren.

9.1.1 Mögliche Internetanbindungen

Grundsätzlich sind drei verschiedene Konstellationen der Internetanbindung und -nutzung einer Behörde zu unterscheiden:

1. Eine Behörde nutzt einen Internetzugang nur, um Informationen im Internet suchen zu können.
2. Eine Behörde stellt eigene Informationen im Internet zum (potentiell weltweiten) Abruf zur Verfügung.
3. Eine Behörde stellt eigene Informationen im Internet zum Abruf zur Verfügung und bietet zusätzlich die Interaktion mit Bürgern und Bürgerinnen, z. B. per E-Mail, an.

Diese drei Konstellationen verlangen unterschiedliche Maßnahmen, um den Datenschutz zu gewährleisten. Generell gilt: Die Internettechnik bietet die Möglichkeit, beim Abruf von Informationsseiten im WordWideWeb (WWW, der multimediale Dienst des Internet) mit der Übermittlung der WWW-Seiten Programme oder programmähnliche Anweisungen zu übertragen, die dann auf dem abrufenden Rechner ausgeführt werden. Diese Möglichkeit kann z. B. dazu genutzt werden, die Festplatte des abrufenden Rechners auszuforschen oder gar zu formatieren, was bei fehlender Datensicherung zu einem Verlust aller auf der Festplatte gespeicherten Informationen führen könnte.

Bei der Konstellation unter 1) muß — solange die geplante zentrale Firewallkonzeption (siehe u. Ziff. 9.1.4.) noch nicht umgesetzt ist — sichergestellt werden, daß keine personenbezogenen Daten auf dem Internet-Zugangsrechner gespeichert sind und kein Übergang vom Internet auf evtl. vorhandene Behördennetze möglich ist. Dies kann einfach dadurch realisiert werden, daß der Zugriff auf das Internet von einem Standalone-PC aus erfolgt, der nicht für andere Zwecke genutzt wird.

Bei den anderen Fallvarianten sind weitergehende datenschutzrechtliche Vorkehrungen erforderlich. So sind bei der Konstellation unter 2) u. a. die Datenübermittlungsvorschriften in bezug auf die evtl. betroffenen Mitarbeiter und Mitarbeiterinnen zu beachten, sofern deren Personalien über das Internet (potentiell weltweit) abrufbar gemacht werden sollen.

Bei elektronischer Kommunikation zwischen Verwaltung und Bürger, also bei der Konstellation unter 3), müssen zusätzliche Maßnahmen zur Sicherung der Kommunikation zwischen Behörden und Bürgern bzw. Bürgerinnen getroffen werden, um folgendes grundsätzliches Risiko zu minimieren: Die Sicherheit und Vertraulichkeit von E-Mails kann nicht garantiert werden, da diese auf dem Weg vom Absender zur Empfangsadresse über zahlreiche Vermittlungsstellen, die vielfach auch im Ausland liegen, transportiert werden; auf dem Transportweg können die elektronischen Nachrichten mitgelesen, gespeichert und weiterverarbeitet werden.

9.1.2 Online-Verwaltung - Vertraulichkeit braucht Verschlüsselung

Mit der SKP war im Dezember 1996 vereinbart worden, daß in Abstimmung mit mir ein bis zwei Pilotprojekte herausgesucht werden, um bei ihnen die datenschutzrechtlichen Anforderungen an die Interaktionsmöglichkeiten der Bürgerinnen und Bürger mit der Verwaltung zu erarbeiten und zu testen.

Bereits vor der Benennung von Pilotprojekten präsentierten sich jedoch einige Behörden — ohne Abstimmung mit dem TuI-Referat der SKP und ohne Warten auf

die Ergebnisse der Pilotprojekte — auch mit Möglichkeiten zur interaktiven Kommunikation im WWW. Hervorzuheben sind hier die Angebote der SKP selbst (!) und der Volkshochschule Bremen, bei denen per E-Mail personenbezogene Daten von Bürgern und Bürgerinnen an die Verwaltung übermittelt werden können.

Von der SKP werden aktuelle Stellenanzeigen im WWW veröffentlicht mit der Möglichkeit, fristwahrend online eine Kurzbewerbung abzugeben. Nach meiner Intervention wurde ein unzutreffender Hinweistext („Absolute Diskretion und Beachtung eventueller Sperrvermerke sind selbstverständlich.") verbessert. Meine Anfrage vom 19. März 1997, welche technischen und organisatorischen Maßnahmen zur Datensicherheit für diese online-Bewerbungen getroffen worden sind, wurde — trotz Erinnerung am 11. Juni 1997 — erst Mitte Oktober beantwortet. Die jetzige Warnung weist zwar auf die unverschlüsselte Übertragung hin, aber die in dem Schreiben vertretene Auffassung, die technischen Möglichkeiten für einen verschlüsselten Empfang von E-Mail seien noch nicht gegeben, teile ich nicht.

Sicherlich: Als Sofortmaßnahme ist der Warnhinweis vor der Übersendung von Mitteilungen per E-Mail an die bremischen Behörden, daß elektronische Nachrichten auf dem Transportweg ungesichert sind und mitgelesen werden können, unverzichtbar. Dem elektronisch mit einer Dienststelle kommunizierenden Bürger sollte aber als Maßnahme des „technischen Selbstschutzes" grundsätzlich immer dann, wenn eine Antwort online möglich ist, das Antwortformular und der öffentliche PGP-Schlüssel der jeweiligen Stelle zum Herunterladen angeboten werden als Voraussetzung dafür, daß er wiederum seinen Text an die Behörde verschlüsselt übertragen kann.

Dieses und andere Beispiele zeigen, daß die Verpflichtung der bremischen öffentlichen Stellen, mich über „Planungen zum Aufbau automatisierter Informationssysteme . . . rechtzeitig zu unterrichten" (§ 27 Abs. 4 Satz 2 Nr. 1 BrDSG), auch im Bereich Internet nicht immer eingehalten wird. Eine enge und frühzeitige Zusammenarbeit zwischen der Verwaltung und meiner Dienststelle ist aber gerade im Bereich der Vernetzung erforderlich, um die datenschutzrelevanten Risiken und Lösungsmöglichkeiten rechtzeitig zu erörtern. Inzwischen wurde eine Arbeitsgruppe bestehend aus Vertretern von SKP, der Universität Bremen und meiner Dienststelle eingerichtet, die eine Problemlösung erarbeiten soll.

9.1.3 „bremen.online" als Public-Private-Partnership — Anforderungen an private Betreiber

Von der SKP wird ein Ausschreibungstext vorbereitet, dessen Entwurf mir vorliegt und der im Frühjahr 1998 dem Senat vorgelegt werden soll. Ziel ist es, für „bremen.online" einen privaten Anbieter zu finden, der das Stadtinformationssystem in eigener wirtschaftlicher Verantwortung übernimmt. Die Aufgabe der bremischen Verwaltung würde sich dann überwiegend auf die Bereitstellung der Informationen aus dem Behördenbereich sowie die Kontrolle, daß die Interessen des Landes Bremen gewahrt werden, beschränken.

Ich habe zu den datenschutzrechtlichen Fragen dieses Vorhabens gegenüber der SKP Stellung genommen und mich dabei insbesondere zu den Anforderungen des neuen Multimediarechts geäußert. In meiner Stellungnahme legte ich dar, daß der Anbieter von bremen.online dem Teledienstegesetz (TDG) und dem Teledienstedatenschutzgesetz (TDDSG) unterliegt, die am 1. August 1997 in Kraft getreten sind (Art. 1 und 2 des IuKDG, BGBl. I S. 1870). Soweit es nicht um individuellen Datenaustausch zwischen Bürger und Anbieter geht, sondern um an die Allgemeinheit gerichtete Informations- und Kommunikationsangebote, kommt der Mediendienstestaatsvertrag (MDStV; BrGBl. Nr. 24 vom 30. Juni 1997, S. 206) zur Geltung.

Daraus ergeben sich Konsequenzen u. a. für die Form der Anbieterkennzeichnung, für Umfang und Zweck der zulässigen Verarbeitung der Nutzerdaten, für die Gestaltung und Auswahl der technischen Einrichtungen sowie für die dienstespezifischen Datensicherungsvorkehrungen. Von Bedeutung ist vor allem die Pflicht des Anbieters, soweit technisch möglich und zumutbar, die Nutzung anonym oder unter Pseudonym zu ermöglichen (§ 4 TDDSG, § 12 Abs. 1 MDStV). Die Konsequenzen aus dieser neuen Rechtslage erfordern also frühzeitige Berücksichtigung bei der System- und Programmgestaltung; deshalb ist ihre Aufnahme in das Konzept und in den Vertrag mit dem Anbieter sinnvoll und notwendig.

Aus den o. a. rechtlichen Anforderungen läßt sich u. a. ableiten, daß bei allen interaktiven Anwendungen verschlüsselte Übertragungen möglich sein sollten. Für E-Mail sollte ein Public-Key-Verfahren (wie z. B. PGP) eingebunden werden. Die öffentlichen Schlüssel der Verwaltung sollten im Stadtinformationssystem zu finden sein; ein Link im Behördenwegweiser auf den jeweiligen Schlüssel wäre sinnvoll. Wenn PGP, für das eine Landeslizenz vorliegt, verwendet wird, sollte dieses zum Download zur Verfügung stehen.

Nicht nur für den Zugriff selbst, sondern auch für die Bezahlung von Gebühren und sonstigen Kosten sollten anonyme Verfahren vorgesehen sein, um der Forderung aus dem TDDSG nach anonymer Nutzung gerecht zu werden.

Soweit die o. a. bereichsspezifischen Regelungen wie das TDDSG und die Datenschutzbestimmungen aus dem Mediendienste-Staatsvertrag, für Anbieter von TK-Dienstleistungen wie z. B. E-Mail auch das Telekommunikationsgesetz, nicht gelten und zulässigerweise von einem privaten Anbieter personenbezogene Daten im Auftrag bremischer Behörden verarbeitet werden, muß sich dieser vertraglich zur Einhaltung des BrDSG verpflichten sowie der Kontrolle durch meine Dienststelle unterwerfen (§ 9 Abs. 1 BrDSG).

9.1.4 Ausschreibung eines Internet-Serviceproviders

Ich nahm mit beratender Stimme an der Arbeitsgruppe zur Auswahl eines verwaltungsinternen Internetserviceproviders für die bremische Verwaltung teil. Dieser Dienstanbieter soll nicht nur Behörden sicher an das Internet, sondern auch an das Intranet anschließen. Das Intranet wird dadurch zum „Zubringer" des Internet. Damit wird der Aufbau einer Doppelinfrastruktur soweit wie möglich vermieden. Aufeinander abgestimmte Sicherheitsmaßnahmen sind für Intra- und Internet erforderlich. Dabei ist nicht nur eine Abschottung gegen das Internet erforderlich (durch eine zentralen Firewall, s. u.), sondern auch innerhalb der Verwaltung müssen Teilbereiche voneinander abgeschottet werden.

Die Arbeitsgruppe hat bei der Diskussion der vorgestellten Konzepte der Anbieter wichtige sicherheitsrelevante Gesichtspunkte erarbeitet, die Grundlage für die Auswahlempfehlung geworden sind. Hierzu zählen insbesondere:

- Ein zentraler Internetzugang: Nur wenn sichergestellt wird, daß der Übergang von allen Behörden zum Internet über einen zentralen Zugang erfolgt, lassen sich das dahinter liegende Bremer Verwaltungsnetz (BVN — Intranet) und die einzelnen Netze der Behörden sicher vom Internet abschotten. Internetanbindungen über Modemverbindungen oder ISDN-Karten, die direkt über andere Provider — z. B. AOL, Compuserve, IS-Bremen oder T-Online — erfolgen, bieten „Hintertüren", die das zentrale Sicherheitskonzept gefährden können. Behörden, die eigene dezentrale Internetzugänge nutzen wollen, dürfen nicht an das Intranet angeschlossen werden.

- Ein gestaffeltes Firewallkonzept: Der zentrale Firewall, der den zentralen Internetzugang für die gesamte bremische Verwaltung absichert, ist zu kombinieren mit dezentralen Firewalls in den einzelnen Behörden, um diese — auch im Intranet — gegenseitig voneinander informationell abzugrenzen.

- Der öffentlich zugängliche Server wird vor Angriffen so geschützt, daß das unbefugte Ändern der Inhalte wesentlich erschwert wird.

Schon früh haben die Datenschutzbeauftragten weitere Sicherheitsanforderungen aufgestellt, die in der „Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet" des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zusammengefaßt sind (abgedr. im 18. Jahresbericht, Ziff. 9.2.2, vollständig verfügbar unter http://www.datenschutz-berlin.de/jahresbe/95/sonstige/inhinter.htm). Dieser Forderungs- und Maßnahmenkatalog ist auch die Basis meiner Bewertungen der bremischen Projektplanungen.

Die Arbeit der o. a. Arbeitsgruppe ist inzwischen abgeschlossen worden. Der Vorschlag der Arbeitsgruppe, eine hierfür eigens gegründete Arbeitsgemeinschaft bestehend aus ID Bremen und BreKom mit den Aufgaben des internen Internet- und Intranetserviceproviders zu beauftragen, wurde von der Verwaltung umgesetzt. Als weiterer Arbeitsschritt soll ein Regelwerk erarbeitet werden, mit dessen Hilfe der passende Zugang zum Internet über ein standardisiertes Verfahren möglich sein wird.

Wie nach Redaktionsschluß in der Sitzung des TuI-Ausschusses vom 18. März 1998 mitgeteilt wurde, hat die Arbeitsgemeinschaft aus BreKom und ID-Bremen ihre Tätigkeit aufgenommen und bietet ihre Dienstleistungen der Verwaltung an. Ich wies darauf hin, daß für den Betrieb des BVN bislang weder das Datenschutz- noch das Firewallkonzept auch nur im Entwurf vorliegen (s. u. Ziff. 9.1.5.). Der Senatsbeschluß zum BVN entbindet die einzelnen Dienststellen nicht von der Verpflichtung, in jedem Einzelfall die Zulässigkeit der Nutzung von E-Mail und anderen Internetdiensten sowie die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere § 7 BrDSG (technische organisatorische Maßnahmen) zu prüfen. Ebenso ist unter Einbeziehung meiner Dienststelle jeweils ein örtliches Datenschutzkonzept zu erstellen.

9.1.5 TuI-Richtlinien für das bremische Verwaltungsnetz

Die Bedingungen für den Einsatz technikunterstützter Informationssysteme (TuI) in der Bremer Verwaltung werden durch das sog. TuI-Regelwerk festgelegt (vgl. Amtsblatt der Freien Hansestadt Bremen, Nr. 7 vom 25. Januar 1996).

Ergänzend hierzu sollen Querschnittsvorgaben für das bremische Verwaltungsnetz erstellt werden. Im April 1997 hat die SKP den Entwurf eines ersten Abschnitts „Zielsetzung" verteilt. Hierin sind wichtige Anwendungs- und Sicherheitsgrundsätze genannt, deren Umsetzung in weiteren Kapiteln der neuen Richtlinie geregelt werden soll. Die für meine Bewertung besonders relevanten Abschnitte betr. die Konzepte für E-Mail, Firewalls und allgemeine Datenschutzanforderungen werden derzeit vom TuI-Referat der SKP erarbeitet.

9.2 Präventiver Datenschutz — Vorgaben für Geräte und Programme auf der Beschaffungsliste

9.2.1 Hardwareausschreibung

Ich habe 1997 an der Arbeitsgruppe beratend teilgenommen, in der mit Hilfe einer EU-weiten Ausschreibung die Hardwarekomponenten (wie z. B. Rechner, Bildschirme, Tastaturen) für die zentrale EDV-Beschaffungsliste der bremischen Verwaltung ausgewählt werden. Diese Teilnahme bezog sich sowohl auf die Erarbeitung des Anforderungsprofils im Ausschreibungstext als auch auf die Bewertung der Angebote sowie der zum Test angeforderten Rechner in Hinblick auf Einrichtungen, die der Datensicherheit und dem Datenschutz dienen. Besonderes Augenmerk lag hierbei auf den Sicherheitsfunktionen im BIOS und auf dem Gehäuse. Als Ergebnis der Ausschreibung sind Rechner mit drei verschiedenen Gehäusevarianten mit unterschiedlichem Sicherheitsstandard ausgewählt worden:

Der ausgewählte Desktoprechner ist mit einem sicheren Gehäuseschloß versehen, das allerdings nicht vor einem Diebstahl des kompletten Systems schützen kann. Das BIOS dieses Rechners bietet Sicherheitsmaßnahmen, die entsprechend den jeweiligen Datenschutz- und Datensicherheitsanforderungen konfiguriert werden können. Das geht soweit, daß bei entsprechender Aktivierung der Rechner dann, wenn der Netzstecker gezogen wurde, nur nach Eingabe des Systempaßwortes wieder in Betrieb genommen werden kann und die dreimalige falsche Eingabe des Paßwortes dazu führt, daß der Rechner nur noch von einem Wartungstechniker wieder zum Laufen gebracht werden kann.

Die beiden zur Auswahl stehenden Towergehäuse sind zwar nicht mit einem Schloß versehen. Allerdings haben sie eine Öse, die dazu genutzt werden kann, um mit einem Vorhängeschloß das unbefugte Öffnen des Gehäuses zu erschweren und/oder um mit einem Stahlseil oder einer Kette das komplette Gehäuse festzuschließen.

Die bei diesen Rechnern vorhandenen Möglichkeiten schützen allerdings nicht davor, daß z. B. eine aus dem Rechner entwendete Festplatte in einem anderen Rechner ausgelesen werden kann. Insbesondere bei sensiblen Daten bleiben weitergehende Schutzmaßnahmen wie z. B. Verschlüsselung auf der Festplatte erforderlich.

9.2.2 Betriebssystem- und Sicherungssoftware

Zwischen der SKP und mir besteht Einigkeit darüber, daß Windows '95 ohne zusätzliche Sicherungssoftware nicht als Betriebssystem geeignet ist, sofern personenbezogene Daten verarbeitet werden sollen. Als Alternative, die bei entsprechender Konfiguration eine gewisse Sicherheit bietet, findet sich auf der Beschaf-

fungsliste Windows NT 4.0 als Client- oder Stand-Alone-PC-Betriebssystem. Für zusätzlichen Sicherheitsbedarf ist das Programm SAFEGuard easy für Windows NT in der überarbeiteten Beschaffungsliste enthalten.

Wie eine Anfrage der SKP bei den Lieferanten ergab, ist im dritten Quartal 1997 die Zahl der von der Verwaltung georderten Windows NT-Client-Lizenzen mehr als dreimal so hoch wie die Zahl der bestellten Windows 95 Lizenzen. Hinzu kommen für ca. ein Viertel der Windows NT-Client-Lizenzen Bestellungen der dazu passenden SAFEGuard-Lizenzen. Daraus folgt, daß die Dienststellen deutlich überwiegend die Programme mit höherer Sicherheitsstufe anschaffen. Abzuwarten bleibt indessen, ob dieser erfreuliche Trend anhält oder nur durch einige Projekte verursacht wurde. Ebenso muß sich erst noch herausstellen, ob die Betriebssysstemsoftware auf den Behördencomputern auch tatsächlich entsprechend den Datenschutz- und -sicherheitsanforderungen konfiguriert sowie ob die beschaffte und vorhandene Sicherungssoftware auch wirklich installiert und korrekt konfiguriert wurde.

9.3 Zukunftstrend „datenschutzfreundliche Technologien" — Arbeitsergebnisse der Datenschutzbeauftragten

Der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zum Thema „Datenschutzfreundliche Technologien" zwei Arbeitspapiere vorgelegt. Mit diesen Texten wollen die Datenschutzbeauftragten vor allem Hersteller und Anbieter für eine datenschutzfreundlichere Gestaltung von Software und Systemen sensibilisieren, aber auch den Anwendern Informationen zum „technischen Selbstschutz" geben.

Die Ausarbeitung „Datenschutzfreundliche Technologien" gibt anhand konkreter Beispiele aus dem Medienbereich, dem elektronischen Zahlungsverkehr, dem Gesundheitsbereich, der Telekommunikation sowie aus den Bereichen Transport und Verkehr Empfehlungen für technische Schutz- und Sicherungsmöglichkeiten in dem jeweiligen Bereich. Dieser Text kann im Internet unter der Adresse http://www.datenschutz-berlin.de/to/datenfr.htm abgerufen werden.

Das Arbeitspapier „Datenschutzfreundliche Technologien in der Telekommunikation" ist spezieller. Es beschreibt die bei verschiedenen Telekommunikationsdiensten anfallenden personenbezogenen Daten und gibt Hilfestellung bei der Bewertung von neuen Telekommunikationsformen. Die angebotenen Lösungen beschränken sich bewußt auf Beispiele der Datenvermeidung und Datenreduzierung, eine Zielrichtung, die der neuen Multimediagesetzgebung entspricht (vgl. o. Ziff. 2.2.1.). Die Internet-Quelle für diesen Text lautet http://www.datenschutz-berlin.de/to/tk/ds—123.htm.

10. Bürgerschaft

10.1 Datenschutzordnung in Kraft

Die Bremische Bürgerschaft hat sich für den Umgang mit persönlichen Daten der Bürgerinnen und Bürger zu parlamentarischen Zwecken eine Datenschutzordnung als Bestandteil (Anlage) der Geschäftsordnung gegeben (vgl. Bericht und Antrag des Datenschutzausschusses vom 8. Juli 1997, Drucks. 14/731, sowie Protokoll der 47. Sitzung der Bürgerschaft (Landtag) am 18. September 1997, S. 2918 D). Sie gilt, sofern das „Gesetz über Einsetzung und Verfahren von Untersuchungsausschüssen" von 1982 keine Sonderregelungen trifft, auch für die Tätigkeit der Untersuchungsausschüsse. Bei den Gesprächen über den Umgang mit den vom Senator für Justiz und Verfassung an den Untersuchungsausschuß zu den Vorgängen in der JVA Oslebshausen übergebenen Akten hatte ich Gelegenheit und Veranlassung, auf die zu beachtenden neuen Vorgaben der Datenschutzordnung für den Umgang mit den den Parlamentariern übergebenen Unterlagen hinzuweisen.

Hintergrund und Zielsetzung der Datenschutzordnung sind oben Ziff. 3.1.2. kurz beschrieben. Sie verlangt in ihrer wohl wichtigsten Bestimmung, daß die Bürgerschaft bzw. ihre Gremien und Abgeordneten gegen das Bekanntwerden personenbezogener Daten an Unbefugte die erforderlichen Vorkehrungen zu treffen haben (§ 7). Die bloße Existenz parlamentsinterner Regelungen reicht also nicht aus, vielmehr müssen in der konkreten Ausschuß- und Fraktionstätigkeit jeweils im Einzelfall spezielle Datenschutzmaßnahmen realisiert werden, bei denen zwischen den schutzwürdigen Belangen der Betroffenen und dem Interesse an der öffentlichen parlamentarischen Verhandlung abzuwägen ist.

Zu den Geheimhaltungsvorkehrungen gehören insbesondere die Behandlung in nicht-öffentlicher Sitzung, die Löschung von Tonbandprotokollen, die Anonymisierung in Unterlagen sowie die Einschränkung zugangsberechtigter Personen und zu verteilender Kopien.

Es ist die Aufgabe des Datenschutzausschusses, die Einhaltung der Datenschutzordnung zu überwachen (§ 10). Er ist Ansprechpartner für Bürger, die wegen der Behandlung ihrer persönlichen Daten in der Bürgerschaft Fragen oder Beschwerden haben. Der Ausschuß hat Anhaltspunkten für Verstöße nachzugehen und ggf. den Präsidenten zu unterrichten. Auch ich als Landesbeauftragter werde mich bei Hinweisen auf eine mangelnde Beachtung der neuen Regelungen an den Ausschuß wenden.

10.2 Die Arbeit des Datenschutzausschusses

10.2.1 Die Beratung des 19. Jahresberichts

Der Datenschutzauschuß hat meinen 19. Jahresbericht (Bürgerschafts-Drucks. 14/627) und die zugehörige Stellungnahme des Senats (Drucks. 14/779) in seinen Sitzungen am 18. November 1997 und am 22. Januar 1998 beraten. Der Bericht des Ausschusses über seine Beratungen wurde am 11. März 1998 verabschiedet und soll der Bürgerschaft in der Plenumssitzung in der letzten März-Woche, also nach Redaktionsschluß dieses Berichts, vorgelegt werden (Drs. 14/981). Der vom Ausschuß verabschiedete Text hat folgenden Wortlaut:

„Die Bürgerschaft (Landtag) hat in ihrer Sitzung am 15. Mai 1997 den 19. Jahresbericht des Landesbeauftragten für den Datenschutz und in ihrer Sitzung am 20. November 1997 die Stellungnahme des Senats zur Beratung und Berichterstattung an den Datenschutzausschuß überwiesen. Zusätzlich zur Beratung dieser Berichte hat der Ausschuß Themen aus früheren Jahresberichten wieder aufgegriffen, bei denen es keine zufriedenstellende Lösung gegeben hat. Der Ausschuß hat zu den einzelnen Verhandlungsgegenständen den Landesbeauftragten für den Datenschutz und Vertreter der betroffenen Ressorts angehört.

Die in diesem Bericht verwendeten Überschriften und Ziffern sind identisch mit denjenigen der Jahresberichte des Datenschutzbeauftragten.

bremen.online — auf dem Weg zum interaktiven Bürgerinformationssystem (6.1)

Der Landesbeauftragte für den Datenschutz hat den von der Bürgerschaft erbetenen Sachstandsbericht zur Anbindung der bremischen Verwaltung an das Internet und zum Sicherheitskonzept für das bremische Verwaltungsnetz am 7. Juli 1997 vorgelegt. Dieser Bericht zeigt datenschutzrechtliche Risiken auf, die bei der Veröffentlichung und Übertragung von Daten sowohl im Internet als auch beim Intranet — dem bremischen Verwaltungsnetz — auftreten können.

Ein besonderes Problem sieht der Ausschuß bei den sogenannten Schwarzen Brettern im Stadtinformationssystem bremen.online, mit denen gelegentlich Mißbrauch getrieben wird, indem dort z. B. falsche oder anzügliche Mitteilungen verbreitet werden, ohne daß der Urheber feststellbar ist.

Der Datenschutzausschuß ist der Auffassung, daß zu diesem Problem eine Lösung gefunden werden muß, und erwartet, daß, unabhängig von der Rechtsform, in der bremen.online betrieben wird, ausreichende Sicherheitsanforderungen gewährleistet werden. Im übrigen begrüßt der Ausschuß die gute Zusammenarbeit zwischen dem Landesbeauftragten für den Datenschutz und der Senatskommission für das Personalwesen bei der Entwicklung von bremen.online.

SIJUS-Straf: Stand der Einführung bei der Staatsanwaltschaft Bremen (10.1.1)

Zwischen dem Senator für Justiz und Verfassung und dem Landesbeauftragten für den Datenschutz bestehen hinsichtlich des Datenschutzkonzeptes für das staatsanwaltschaftliche Informationssystem SIJUS-Straf in einigen Punkten unterschiedliche Auffassungen. Der Ausschuß hat den Senator für Justiz und Verfassung dazu um einen Sachstandsbericht bis zum 4. Mai 1998 gebeten.

Sozialpsychiatrischer Dienst: Softwareanpassung an Vorgaben des ÖGD-Gesetzes (11.4)

Nach dem Gesetz über den öffentlichen Gesundheitsdienst, das seit 1995 in Kraft ist, ist eine Rechtsverordnung zu erlassen, die unter anderem einen Katalog der Daten, die im Bereich der Gesundheitsämter gespeichert werden dürfen, bestimmen muß. Die Vorarbeiten zu dieser Verordnung haben sich verzögert. Das

Fehlen der Verordnung führt dazu, daß die Möglichkeiten der automatisierten Datenverarbeitung in der Gesundheitsverwaltung nicht genutzt werden können, was insbesondere beim Sozialpsychiatrischen Dienst Probleme mit sich bringt.

Der Senator für Frauen, Gesundheit, Jugend, Soziales und Umweltschutz hat gegenüber dem Ausschuß erklärt, er gehe davon aus, daß bis zur Sommerpause 1998 ein mit dem Landesbeauftragten für den Datenschutz abgestimmter Entwurf einer Rechtsverordnung erarbeitet werden könne. Der Ausschuß bittet den Senat, diesen Termin unbedingt einzuhalten.

Ausländerzentralregister (11.2 des 18. Jahresberichts)

Der Landesbeauftragte für den Datenschutz hatte in seinem 18. Jahresbericht moniert, daß entgegen dem im Bundesgesetz über das Ausländerzentralregister vorgeschriebenen Datenverarbeitungsverfahren das Register weiterhin nach dem früheren Verfahren geführt werde, das den geltenden rechtlichen Vorgaben nicht entspreche. Dies habe zur Folge, daß z. B. keine hinreichende Protokollierung der Abrufe und Dateneingaben gewährleistet sei, was die Kontrollmöglichkeit sowohl der Dienststellen selbst als auch des Datenschutzbeauftragten erschwere.

Der Senator für Inneres hatte seinerzeit dem Datenschutzausschuß erklärt, er werde den Bundesminister des Innern schriftlich auf die ordnungsgemäße Umsetzung der Protokollierungspflicht hinweisen. Dies ist, wie der Senator für Inneres dem Ausschuß auf entsprechende Nachfrage mitgeteilt hat, nicht geschehen. Die Problematik sei jedoch mit dem Bundesminister des Innern mehrmals im Rahmen der Besprechungen der Ausländerreferenten und auch telefonisch erörtert worden. Nachdem der Ausschuß daraufhin gebeten hat, die Protokolle der Besprechungen der Ausländerreferenten zur Verfügung zu stellen, erhielt er als Antwort, daß eine Protokollierung hierüber nicht stattgefunden habe.

Der Ausschuß erwartet, daß Zusagen, die ihm gegenüber gemacht werden, künftig auch vom Senator für Inneres eingehalten werden.

Wahlkampf mit Wählerdaten (9.4.1 des 17. Jahresberichts, 8.2 des 18. Jahresberichts)

Bereits mit ihrem Beschluß zum Bericht des Datenschutzausschusses vom 6. Februar 1996 zum 17. Jahresbericht des Landesbeauftragten für den Datenschutz (Drs. 14/214) hatte die Bürgerschaft den Senator für Inneres gebeten sicherzustellen, daß Wählerdaten nicht an Parteigliederungen außerhalb Bremens weitergegeben werden. Nachdem der Landesbeauftragte für den Datenschutz anläßlich der Beratungen des 18. Jahresberichts in der Ausschußsitzung am 26. November 1996 kritisiert hatte, daß ein entsprechendes klarstellendes Schreiben an die Meldebehörden im Lande Bremen bisher nicht ergangen sei, sagte der Senator für Inneres die gewünschte Klarstellung zu.

In seiner Sitzung im 18. November 1997 mußte der Ausschuß zur Kenntnis nehmen, daß ein entsprechender Hinweis nicht schriftlich ergangen ist. Der Senator für Inneres hat immerhin im Rahmen von Dienstbesprechungen mit den Leitern der Meldestellen in Bremen und Bremerhaven klargestellt, daß derartige Übermittlungen künftig nicht mehr erfolgen dürfen.

Der Ausschuß erwartet, daß entsprechend der Ankündigung des Senators für Inneres in der Ausschußsitzung in dem an das geänderte Melderechtsrahmengesetz des Bundes anzupassenden Meldegesetz eine Bestimmung aufgenommen wird, die die Weitergabe von Wählerdaten auf Parteigliederungen innerhalb des Landes Bremen beschränkt.

Vorlage des Steuerbescheides statt Nachweis von Einzelangaben (9.4.1 des 17. Jahresberichts, 8.2 des 18. Jahresberichts)

Um bestimmte öffentliche Leistungen, wie z. B. Beitragsermäßigungen für Kindergartenplätze oder Mittel nach dem Bundesausbildungsförderungsgesetz, in Anspruch nehmen zu können, wird bisher regelmäßig die Vorlage des Steuerbescheids verlangt. Dieser enthält eine Fülle von Daten, deren Mitteilung für die Gewährung der Leistung größtenteils nicht erforderlich ist. Der Datenschutzausschuß unterstützt deshalb den Landesbeauftragten für den Datenschutz bei seinen Bemühungen zu erreichen, daß jeweils nur die notwendigen Einzelangaben, wie z. B. die Höhe des Einkommens, nachgewiesen werden müssen.

Der Senator für Frauen, Gesundheit, Jugend, Soziales und Umweltschutz hat gegenüber dem Ausschuß angekündigt, er werde für den Bereich der Kindertagesheime künftig entsprechend verfahren. Der Ausschuß wird die Thematik für die Bereiche Wohngeld und Ausbildungsförderung weiter verfolgen."

10.2.2 Aktuelle Themen

10.2.2.1 Beispiele

Der Datenschutzausschuß hat im Berichtszeitraum eine Reihe aktueller Fragen behandelt. Anlaß waren entweder Schilderungen in den Medien oder Problemlagen, die bei den Ausschußmitgliedern in ihrem beruflichen Umfeld oder in ihrer (sonstigen) parlamentarischen Tätigkeit aufgetaucht sind. Manche Tagesordnungspunkte schlage auch ich zur Beratung vor. Behandelt wurden u. a. die Themen

- Rechtslage bei der Änderung von Kfz-Scheinen in städtischen Meldestellen/Ortsämtern,
- Nachfrage zum Verbleib ehemaliger BIQ-Teilnehmer und -Teilnehmerinnen,
- Datenschutz im Mediendienste-Staatsvertrag,
- Konsumentenbefragung der Infas-Lifestyle AG,
- Verletzung von Patientendatenschutz durch Telefonsysteme in Krankenhäusern,
- Weitergabe von Daten von Asylbewerbern an die Türkei.

10.2.2.2 Der „Stradivari-Fall" — Persönlichkeitsrecht bei Filmdokumentation

Besonders eingehend befaßte sich der Ausschuß mit einem Fall, der in Bremen großes Auftreten und tiefe Betroffenheit ausgelöst hat. Einer bekannten Geigenlehrerin war bei einem Überfall ihre wertvolle Stradivari entrissen worden. Sie wurde am Tatort tot aufgefunden. Am 28. Mai 1997 wurde in der ARD-Serie „Unter deutschen Dächern" ein in seiner fachlichen Qualität weitgehend positiv beurteilter Filmbeitrag über die kriminalpolizeilichen Ermittlungen in diesem Todesfall gesendet. Grundlage waren Aufnahmen, die bei der Begleitung der Ermittlungshandlungen des zuständigen Kommissariats des Polizeipräsidiums Bremen gemacht wurden. Nach der ersten Ausstrahlung hatte das Landgericht Hamburg Radio Bremen mit einer einstweiligen Verfügung vom 3. Juli 1997 untersagt, einige Passagen des Films wegen Verstoßes gegen das Persönlichkeitsrecht weiter zu verbreiten.

Der Fernsehbeitrag war sowohl Gegenstand einer parlamentarischen Anfrage als auch der Behandlung im Rundfunkrat von Radio Bremen. Der Datenschutzausschuß konnte und wollte sich nur mit den spezifisch datenschutzrechtlichen Fragen beschäftigen.

Da die Erhebung und Verwendung persönlicher Daten im Rahmen publizistischer Tätigkeit dem Datenschutzrecht nicht unterliegt (sog. Medienprivileg), konnte es m. a. W. nur um die Übermittlung von Informationen über Geschädigte, Tatverdächtige oder Zeugen durch die Polizei an das Fernsehteam gehen. Bedenklich war beispielsweise, daß die Vortaten eines Tatverdächtigen aus einem vertraulichen INPOL-Ausdruck verlesen wurden. Oder: Das Journalistenteam durfte bei einer Hausdurchsuchung in den Privaträumen eines Betroffenen filmen. Teile eines hinter verschlossenen Türen geführten Verhörs wurden vom Flur aus abgehört, aufgezeichnet und gesendet. Äußerungen zum früheren Gesundheitszustand des Tatopfers im Rahmen der Obduktion wurden mitgesendet.

In den Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) ist zwar geregelt, daß bei der Unterrichtung der Öffentlichkeit über Presse, Hörfunk und Fernsehen im Einzelfall zu prüfen ist, ob das Interesse der Öffentlichkeit an einer vollständigen Berichterstattung gegenüber den Persönlichkeitsrechten des Beschuldigten oder anderer Beteiligter, insbesondere auch des Verletzten, überwiegt. Eine unnötige Bloßstellung der Personen sei zu vermeiden. Diese Regelungen beziehen sich aber auf die Reaktion der Strafverfolgungsbehörden auf Auskunftswünsche der Medien bzw. auf deren Pressemitteilungen oder -konferenzen.

Die Begleitung polizeilicher Ermittlungstätigkeit durch ein Fernsehteam ist geeignet, viel weitgehender in die Persönlichkeitssphäre der Betroffenen einzugreifen als Presseverlautbarungen. Auf diese Situation zugeschnittene Regelungen gibt es aber derzeit nicht. Nach Auskunft des Senators für Justiz und Verfassung im Datenschutzausschuß gab es auch keine Drehgenehmigung oder sonstige Autorisierung durch die Staatsanwaltschaft, die ja die „Herrin des Ermittlungsverfahrens" ist.

Der Datenschutzausschuß hatte seine Beratungen zunächst abgeschlossen mit der Bitte an den Senator für Inneres, in Abstimmung mit dem Senator für Justiz und Verfassung und meiner Dienststelle entsprechende Regelungen zu erarbeiten

und bis zum Januar 1998 einen Sachstandsbericht vorzulegen. Der Senator für Inneres hat mir jedoch nach und entgegen der Bitte des Ausschusses mitgeteilt, er halte Ergänzungen oder Präzisierungen vorhandener Dienstanweisungen oder sonstige weitere Bestimmungen über die bestehenden Regelungen hinaus zur Zeit für nicht sinnvoll.

Ich teile diese Auffassung nicht. Ich habe daher in meinem Antwortschreiben vom November 1997 die Position wiederholt, daß nur dann, wenn im vorhinein in einem klaren Verfahren der Zulässigkeitsrahmen für ermittlungsbegleitende Filmaufnahmen im Dialog zwischen Strafverfolgungsbehörden und Journalisten abgesteckt oder ggf. auch vor der Sendung überprüft wird, sichergestellt werden kann, daß nicht durch die Ausstrahlung gegen datenschutz- und strafrechtliche Bestimmungen verstoßen wird.

Um die Angelegenheit voranzubringen, habe ich dem Innensenator vorgeschlagen, möglichst umgehend mit dem Justizressort und der Staatsanwaltschaft zunächst die Frage zu klären, in welchen Fällen bereits die Strafprozeßordnung und das Strafgesetzbuch eine begleitende Dokumentation durch Medien ausschließen, etwa weil mit dem Zulassen dokumentarischer Aufnahmen zwangsläufig ein Verstoß gegen das Amtsgeheimnis oder ein Berufsgeheimnis verbunden ist. Der Justizsenator jedoch hielt seinerseits weitere Festlegungen ebenfalls nicht für erforderlich; die Klarstellung der Verantwortlichkeit der Staatsanwaltschaft bei der Begleitung repressiv-polizeilicher Ermittlungen durch die Medien reiche aus.

Der Datenschutzausschuß hat sich nicht damit zufriedengegeben, daß der Ball zwischen den beteiligten Ressorts hin und hier gespielt wird, ohne daß Vorkehrungen dafür getroffen werden, daß sich Datenschutzverstöße in vergleichbaren Fällen nicht wiederholen. Er hat seine Aufforderung wiederholt, konkrete Regelungen bzw. Maßnahmen zu treffen, und die Senatoren für Inneres und Justiz in die Mai-Sitzung des Ausschusses gebeten.

11. Personalwesen

11.1 Zukunftstrend Teleheimarbeit?

11.1.1 Überlegungen zu den datenschutzrechtlichen Anforderungen

Die Einführung von Telearbeitsplätzen in Privatwohnungen wirft eine Fülle datenschutzrechtlicher Fragen auf, die bisher noch nicht im Gesamtzusammenhang geklärt sind. Fest steht jedenfalls, daß das Risiko des Datenmißbrauchs erhöht wird und daß die rechtlichen Bedingungen der Auslagerung bisheriger Büroarbeitsplätze vorher festgelegt werden müssen. Vor der Einrichtung eines Tele-Heimarbeitsplatzes ist zunächst zu prüfen, ob die Verarbeitung personenbezogener Daten dort zwingend erforderlich ist. Personenbezogene Daten, die Berufs- und besonderen Amtsgeheimnissen unterliegen (z. B. Sozial-, Personal- und Steuerdaten sowie medizinische Daten), sollten nicht „zu Hause" verarbeitet werden.

Welche technischen und organisatorischen Maßnahmen im einzelnen zu treffen sind, hängt von der Sensitivität der in der Wohnung zu verarbeitenden Daten ebenso ab wie von den räumlichen und möglicherweise auch persönlichen Verhältnissen des Beschäftigten. Die Maßnahmen zur Sicherung der Authentizität und Integrität der Datenübertragung etwa durch Verschlüsselung und Verwendung digitaler Signaturen sowie zum Schutz vor unbefugtem Zugriff durch Familienmitglieder oder sonstige Anwesende müssen vor der Inbetriebnahme im Detail getroffen werden.

Weiter muß festgelegt werden, ob überhaupt und ggf. welche Arbeitszeitdaten und Arbeitsergebnisse mit welchen technischen Einrichtungen zu Aufsichts- und Kontrollzwecken von den Vorgesetzten in der Zentrale verarbeitet werden dürfen.

Schließlich geht es um die Wahrung meiner Kontrollbefugnisse. Nach § 27 Abs. 3 Satz 2 Nr. 2 Bremisches Datenschutzgesetz (BrDSG) können meine Mitarbeiter/-innen und ich lediglich die Dienst- und Geschäftsräume öffentlicher Stellen unangemeldet aufsuchen und betreten. Wegen des Grundrechts auf Unverletzlichkeit der Wohnung nach Art. 13 GG bedarf es demzufolge der Zustimmung des betroffenen Beschäftigten, damit meine Mitarbeiter/-innen und ich deren Privaträume betreten und die dienstliche Datenverarbeitung dort überprüfen dürfen. Wird eine solche Einwilligung nicht erteilt bzw. später widerrufen, muß dies zur Folge haben, daß die Teleheimarbeit jedenfalls mit personenbezogenen Angaben nicht erlaubt bzw. beendet wird.

11.1.2 Ansätze in der bremischen Verwaltung

Daß diese Überlegungen sehr bald konkrete Relevanz gewinnen könnten, zeigen die jüngsten Initiativen des Bremer Senats. Er hat in seiner Antwort auf eine Kleine Anfrage der CDU-Fraktion in der Bremischen Bürgerschaft vom 4. Februar 1997 (Drucksache 14/606) erklärt, die Telearbeit sei grundsätzlich auch für den öffentlichen Dienst von großem Interesse. Die juristischen, organisatorischen, technischen und sozialen Bedingungen für die Einrichtung von Telearbeitsplätzen sollten von der Senatskommission für das Personalwesen (SKP) geprüft werden.

Eine Arbeitsgruppe unter Federführung der SKP hat daraufhin ein Grundsatzpapier für einen Modellversuch „Telearbeit" erstellt. Darin werden als Nachteile u. a. mögliche Defizite bei Datensicherung und Datenschutz erwähnt. Auf meinen Wunsch ist jedenfalls der Hinweis aufgenommen worden, daß die jeweils geltenden datenschutzrechtlichen Regelungen einzuhalten und im Einzelfall in Absprache mit mir zu konkretisieren sind.

Die Staatliche Deputation Verwaltungsreform und Öffentlicher Dienst hat sich dann in ihrer Sitzung am 15. Juli 1997 dafür ausgesprochen, verbindliche Rahmenbedingungen zur Durchführung des Modellversuchs in einer auf dessen Dauer befristeten Dienstvereinbarung mit dem Gesamtpersonalrat (GPR) zu regeln.

Auf meine Anfrage Ende Januar 1998 hat die SKP mitgeteilt, die Gespräche mit dem GPR seien noch im Gang, und zugesagt, mich rechtzeitig vor dem Abschluß verbindlicher Vereinbarungen zu beteiligen. Meine — noch nicht abschließenden — Vorstellungen habe ich sowohl dem GPR als auch der SKP zugeleitet.

11.2 Vorlage von Personal(akten)daten an Personalräte

Die Oberfinanzdirektion (OFD) hat mich um Stellungnahme gebeten zu der Frage, ob die Bekanntgabe von Beurteilungsplänen an den Personalrat in der Steuerverwaltung zulässig ist. Wenn in einer Dienstelle die Anzahl der zu einer Besoldungsgruppe gehörigen Beamten entsprechend klein ist, kann aus dem aufgegliederten Plan die Beurteilungsnote einzelner Beamter und damit eine personenbezogene Information abgeleitet werden.

Die Verarbeitung der persönlichen Daten von Beamten richtet sich nach §§ 93 ff. Bremisches Beamtengesetz (BremBG). Sie ist neben den in § 93 Satz 1 BremBG genannten Zwecken auch zulässig, soweit eine Rechtsvorschrift dies erlaubt. Eine solche Rechtsvorschrift ist auch § 54 Abs. 3 Satz 1 Bremisches Personalvertretungsgesetz (BremPersVG), wonach dem Personalrat auf sein Verlangen die zur Durchführung seiner Aufgaben erforderlichen Unterlagen einschließlich der notwendigen personenbezogenen Angaben vorzulegen sind. Zwar darf der Personalrat die — herkömmlicherweise in Papierform geführte — Personalakte eines Bediensteten, die ein umfassendes Bild der Persönlichkeit des Betroffenen liefert, nur mit dessen Einverständnis einsehen. Den erst durch die Novellierung des Beamtenrechts eingeführten und wesentlich weiter gefaßten Begriff der Personalaktendaten (vgl. § 93 a Abs. 1 Satz 2 BremBG) enthält und meint das Personalvertretungsrecht jedoch nicht.

Ich habe der OFD daher mitgeteilt, daß es sich bei den Beurteilungsplänen um Unterlagen handelt, die dem Personalrat auf Verlangen nach § 54 Abs. 3 Satz 1 BremPersVG vorzulegen sind. Die personenbezogenen Beurteilungsdaten sind zwar nach dem Beamtenrecht besonders zu schützende Personalaktendaten, nicht aber gegenüber dem Personalrat mit Zustimmungsvorbehalt des einzelnen Bediensteten zurückzuhaltende Personalakten. Voraussetzung des Vorlageanspruchs ist selbstverständlich, daß der Personalrat sie zur Durchführung konkreter Aufgaben nach dem BremPersVG benötigt und nicht ein allgemeines Informationsinteresse befriedigen will.

11.3 Organisationsuntersuchungen durch externe Beratungsfirmen — Arbeitshilfe mit Datenschutzteil

In der bremischen Verwaltung werden zunehmend Organisations- und Wirtschaftlichkeitsuntersuchungen durch externe Beratungsunternehmen durchgeführt. Die Senatskommission für das Personalwesen (SKP) hat im Juni 1997 zu dieser Thematik eine Arbeitshilfe herausgegeben, an deren Erarbeitung ich beteiligt war.

Die Ziffer 12 der Anlage 1 zur Arbeitshilfe (Muster für eine Leistungsbeschreibung zur Durchführung einer Untersuchung) erläutert die Anforderungen an Geheimhaltung und Datenschutz. Danach ist der Auftragnehmer verpflichtet,

alle mit der Ausführung des Auftrages bekanntwerdenden Vorgänge geheimzuhalten und nicht an Dritte weiterzugeben. Die Verpflichtung erstreckt sich auf alle Mitarbeiter der Beratungsfirma sowie auf evtl. Unterauftragnehmer und bleibt auch nach der Beendigung des Vertrags- bzw. Beschäftigungsverhältnisses bestehen.

Personenbezogene Erhebungsunterlagen, insbesondere Fragebögen und Interviewniederschriften, sind vom Auftragnehmer zu vernichten, sobald sie für die jeweilige Untersuchung nicht mehr benötigt werden, spätestens bei Abnahme des Gutachtens. Elektronisch gespeicherte Daten dieser Art sind unter den gleichen Voraussetzungen zu löschen. Die Vernichtung bzw. Löschung ist auf Verlangen rechtsverbindlich zu bestätigen.

Entsprechend meiner Anregung ist ebenfalls festgelegt worden, daß sich die Beratungsunternehmen verpflichten müssen, die Bestimmungen des Bremischen Datenschutzgesetzes zu beachten und sich der Kontrolle des Landesbeauftragten für den Datenschutz zu unterwerfen. Diese Pflichten des Auftragnehmers bestehen auch nach Beendigung des Vertragsverhältnisses fort. (Vgl. zur Bewertung einer konkreten Organisationsuntersuchung für den Bereich des Lehrereinsatzes u. Ziff. 15.1.)

11.4 Zentrale Arbeitszeiterfassung - Anforderungen der Datensicherung

Bereits im 19. JB habe ich unter Ziff. 8.2.1 über die geplante zentrale Arbeitszeiterfassung für die bremische Verwaltung berichtet und auf Diskrepanzen zu den als Gesamtdienstvereinbarung verbindlichen „Grundsätzen für die gleitende Arbeitszeit" (ABl. Nr. 59 vom 29. Mai 1995) hingewiesen.

Im Berichtszeitraum wurde die Realisierung der zentralen Arbeitszeiterfassung weitergeführt. Zunächst wurde mir die Senatsvorlage für die Einführung der elektronischen Arbeitszeiterfassung in der bremischen Verwaltung, die auch eine in wenigen Punkten geänderte Neufassung der „Grundsätze für die gleitende Arbeitszeit" enthielt, zur Kenntnis zugeleitet. Da der erforderliche Hard- und Softwarebedarf noch nicht absehbar war, konnte ich zunächst noch keine konkreten Datenschutzanforderungen stellen. Ich habe deshalb keine Bedenken gegen die vorgeschlagene Neukonzeption geäußert, aber meine Beteiligung zur Klärung der Datenschutzfragen bei der technischen Umsetzung eingefordert.

Die Senatskommisson für das Personalwesen (SKP) hat die Informations- und Datentechnik (ID) Bremen mit der Ausschreibung und Realisierung der zentralen Arbeitszeiterfassung beauftragt. Im Sommer hat mich die ID Bremen über den Sachstand unterrichtet; allerdings war zu diesem Zeitpunkt die Ausschreibung bereits erfolgt, so daß ich keinen Einfluß auf den Ausschreibungstext nehmen konnte.

Im Rahmen des Projektes wurde ein Ausschreibungsbeirat zur Angebotsauswertung und Entscheidungsfindung eingerichtet. Ich habe an diesem Gremium teilgenommen, meine Datenschutzanforderungen formuliert und die Systemvorführungen begleitet.

Im Herbst 1997 habe ich die aus meiner Sicht erforderlichen organisatorischen und technischen Maßnahmen gegenüber der SKP schriftlich konkretisiert. Sie betreffen u. a. die Beschränkung der Datenfelder, Bildschirmmasken und Auswertungen, die Verschlüsselung der Datenübertragung, die Löschung von Arbeitszeit- und Protokolldaten, die systemseitigen Protokollierungen sowie eine transparente Rechtevergabe für die verschiedenen Benutzergruppen.

Zur Zeit erfolgt die Implementierung des Testsystems. Nach Aufnahme des Testbetriebes werde ich die Umsetzung meiner Forderungen überprüfen.

11.5 Neues Abrechnungsverfahren für Bezüge (KIDICAP) — organisatorische Übergangslösung

Im Berichtszeitraum ist die bereits seit längerer Zeit beabsichtigte Ablösung der bisher von der SKP eingesetzten Bezügeabrechnungsverfahren durch Senatsbeschlüsse beschleunigt worden. Die bisher eingesetzten Verfahren werden den Praxisanforderungen nicht mehr gerecht (z. B. fehlende Dialogfunktion). Zudem müßten sie mit erheblichem Programmieraufwand auf die Jahrtausendwende umgestellt werden.

Die Dienststellen haben über Terminalanbindung Zugriff auf das bei der ID Bremen implementierte Großrechnerverfahren PAADIS, das durch die Standard-Software KIDICAP 2000 (vgl. dazu bereits 17. JB, Ziff. 8.1) ersetzt werden soll.

KIDICAP 2000 bietet allerdings nicht die Möglichkeit, die bisher unter PAADIS realisierten, je nach Aufgabenbereich differenzierten Zugriffsmöglichkeiten für die mit diesem System arbeitenden Mitarbeiter/-innen der SKP abzubilden. Deshalb soll über die im Produkt vorhandenen Schnittstellen für den Datenim- und -export eine Verbindung mit dem in Bremen entwickelten dezentralen Verfahren zum Personalkostenmanagement und -controlling und zur Unterstützung der dezentralen Personalverwaltung (PuMa, vgl. dazu 18. JB, Ziff. 10.1; 19. JB, Ziff. 8.1) geschaffen werden, um einen ausreichenden Zugriffsschutz sicherzustellen. Die für die Abrechnung erforderlichen Daten werden aus KIDICAP in die PuMa-Datenbank übernommen, so daß die Anwender/-innen zur Berechnung der Bezüge (Besoldung, Vergütung und Lohn, Versorgung) lediglich auf das Verfahren PuMa zugreifen.

Die Einführung von KIDICAP soll beginnend ab 1. Juli 1998 im Bereich Besoldung in drei Stufen erfolgen und bis zum 1. Januar 2000 im Bereich Versorgung abgeschlossen sein. Da die erste Stufe bereits im 2. Halbjahr 1998 realisiert werden soll, die PuMa-Erweiterung voraussichtlich erst zum 1. Januar 1999 mit Einführung der 2. Stufe im Bereich Vergütung und Lohn zur Verfügung stehen wird, entsteht voraussichtlich für ein halbes Jahr eine Übergangszeit, in der der beim bisherigen Verfahren PAADIS gegebene, hier aber fehlende technische Zugriffsschutz durch organisatorische Regelungen ersetzt werden soll.

Organisatorische Vorkehrungen sind grundsätzlich gegenüber technischen Maßnahmen die schlechtere Alternative. Gleichwohl habe ich der Übergangslösung bis zum 31. Dezember 1998 zugestimmt, da ich davon ausgehe, daß mir vor Einführung der ersten Stufe das KIDICAP-Datenschutzkonzept vorgelegt wird und ich über die getroffenen organisatorischen Regelungen (Dienstanweisungen) frühzeitig informiert werde. Eine Antwort der SKP steht noch aus.

11.6 Gesundheitsförderung im bremischen öffentlichen Dienst

Der Senat hat im Frühjahr 1997 ein Konzept zur Gesundheitsförderung im bremischen öffentlichen Dienst beschlossen. Danach werden Arbeits- und Gesundheitsschutz als unverzichtbare Bestandteile eines modernen Personalmanagements betrachtet. Hierzu sollen Rahmenbedingungen, Empfehlungen und Handlungshilfen festgelegt sowie Maßnahmen zur Gesundheitsförderung auf der Basis von Fehlzeitenstatistiken und -analysen sowie Mitarbeiterbefragungen entwickelt werden. Außerdem ist vorgesehen, für Langzeitkranke Rückkehrergespräche mit den unmittelbaren Vorgesetzten einzuführen.

Zur Umsetzung dieses Vorhabens hat die Senatskommission für das Personalwesen (SKP) eine Projektgruppe eingerichtet, der ich angehört habe, weil bei diesem Vorhaben zahlreiche Datenschutzaspekte beachtlich sind und teilweise sensible Angaben über die Bediensteten erhoben und genutzt werden sollen. In der Projektgruppe ist eine Reihe aus datenschutzrechtlicher Sicht akzeptabler Ergebnisse erarbeitet worden. Sie betreffen u. a. die Mindestzahl an Bediensteten bei der Erfassung und Auswertung krankheitsbedingter Fehlzeiten, das Verfahren der Entgegennahme von Krankmeldungen, die Form der Anzeige über die Durchführung von Rückkehrergesprächen und die Möglichkeit zusätzlicher freiwilliger schriftlicher Gesundheitsbefragungen nach Zustimmung des Personalrats.

Die Beratungen in der Projektgruppe waren im Sommer 1997 abgeschlossen. Zuletzt hat die SKP Anfang Februar 1998 auf meine Anfrage hin mitgeteilt, die Verhandlungen mit dem Gesamtpersonalrat über den Abschluß einer Dienstvereinbarung zum Rahmenkonzept seien noch im Gang.

11.7 Produktbezogener Zeitaufwand und „sonstige Abwesenheiten"

Bei der Vorbereitung und Durchführung von Organisationsstudien (s. Ziff. 11.3.) muß der von den Beschäftigten mit Hilfe von Interviews oder Fragebögen erhobene Datenkatalog präzise auf Ziel und Zweck der Untersuchung abgestimmt werden. Die Verarbeitung von Beschäftigtendaten im Zusammenhang mit organisatorischen Maßnahmen, insbesondere auch zu Zwecken der Personalplanung, ist im jeweils erforderlichen Umfang durch § 22 Abs. 1 BrDSG i. V. m. § 93 Satz 1 Bremisches Beamtengesetz (BremBG) gedeckt. Voraussetzung ist dabei nach diesen Vorschriften, daß durch die Aufzeichnung und Nutzung der persönlichen Angaben der Mitarbeiter deren schutzwürdige Belange nicht beeinträchtigt werden. Anders ausgedrückt: Der Zulässigkeitsrahmen ergibt sich aus einer Abwägung der Verarbeitungsinteressen von Dienstherr bzw. Arbeitgeber einerseits und Belegschaft andererseits.

Illustrativ dazu ist der folgende Fall: In einer Abteilung des Senators für Frauen, Gesundheit, Jugend, Soziales und Umweltschutz war im Rahmen der Einführung des sog. Neuen Steuerungsmodells festgelegt worden, daß alle Beschäftigten dieser Abteilung auf ca. 15 Minuten genau die Zeiten aufschreiben sollten, die sie für von ihnen erarbeitete Produkte bzw. produktunabhängige Projekte aufwenden. Alle nicht direkt aufgabenbezogenen Zeitaufwendungen innerhalb der normalen Arbeitszeit, wie z. B. Fortbildung, Krankheit, Urlaub oder personalrechtliche Vertretungen, sollten im einzelnen in die Spalte „Sonstiges" eingetragen werden.

Auf Anfrage nach der Erforderlichkeit einer derart detaillierten Ausfüllung der Spalte „Sonstiges" erklärte mir der Abteilungsleiter, die Zeiten für Krankheit, Urlaub und andere sonstige Abwesenheiten seien für Plausibilitätskontrollen der Notizen notwendig. Sie würden aber nicht in die abschließende Dokumentation aufgenommen. Außerdem werde die vollständige Auswertung spätestens nach zwei Monaten erfolgen, so daß die von den Mitarbeitern abzugebenden Abschnitte dann unverzüglich vernichtet würden. Im übrigen sei nicht beabsichtigt, die Daten automatisiert zu verarbeiten.

Nach dieser Klarstellung waren insoweit meine Bedenken im Hinblick auf schutzwürdige Interessen der Beschäftigten ausgeräumt. Den Abteilungsleiter habe ich gebeten, die Bediensteten auf die vielfach nicht bekannte Rechtsgrundlage (s. o.) hinzuweisen.

11.8 Umfang der Auskunftspflicht bei Kindergeldzahlungen

Ein Kindergeldempfänger legte Einspruch ein gegen den Aufhebungsbescheid der Senatskommission für das Personalwesen (SKP) als Familienkasse für die Zahlung von Kindergeld. Er hatte Kindergeld für seine Tochter für die Beurlaubung während eines Semesters geltend gemacht. Zur Bearbeitung des Einspruchs verlangte die SKP je eine Bescheinigung der Hochschule über Zeit und Grund der Beurlaubung sowie des behandelnden Arztes über das Vorliegen der Schwangerschaft.

Die SKP verwies zur Begründung auf die Mitwirkungspflicht der Zahlungsempfänger nach dem Einkommenssteuerrecht sowie auf eine die Weiterzahlung von Kindergeld regelnde Dienstanweisung des Bundesfinanzministeriums. Bei einem für die Betroffene besonders sensiblen Punkt habe ich nachgehakt: Bei der Bescheinigung der Hochschule war zwar unstreitig der Zeitraum der Beurlaubung relevant. Ich konnte jedoch nicht erkennen, warum die Tochter des Kindergeldempfängers auch den Grund ihres Beurlaubungswunschs, d. h. ihre Schwangerschaft, gegenüber der Hochschulverwaltung offenbaren mußte.

Die SKP hielt meinen Einwand für berechtigt und will künftig auf die Bestätigung der Hochschule, daß die Beurlaubung aufgrund einer bestehenden Schwangerschaft erfolgte, verzichten.

12. Inneres

12.1 Sicherheitsüberprüfung I — Lückenhafte Datenschutzkontrolle im Gesetzentwurf

Die Bremische Bürgerschaft hat im Juli 1997 den Entwurf eines Bremischen Sicherheitsüberprüfungsgesetzes (Bürgerschafts-Drucks. 14/682) nach Unterbrechung der ersten Lesung dem Datenschutzausschuß zur weiteren Beratung zugeleitet.

Mit der Vorlage des Entwurfs ist der Senat der vom Datenschutzausschuß und von der Bürgerschaft im Zusammenhang mit der Beratung meiner Jahresberichte wiederholt geäußerten Bitte nachgekommen, das Verfahren der Sicherheitsüberprüfung wegen der Intensität des Grundrechtseingriffs gesetzlich zu regeln (vgl. zuletzt dazu 19. JB Ziff. 9.8.). Nach mehrmonatigem intensiven Meinungsaustausch mit dem Innensenator ist eine Reihe meiner Anregungen in den Entwurf aufgenommen worden.

Neben anderen verbleibenden Änderungswünschen, etwa zum Umfang des Auskunftsrecht von Betroffenen, blieben jedoch vor allem zwei aus meiner Sicht besonders bedeutsame Dissenspunkte, die eine weitere Beratung erforderlich machten.

Der erste betrifft den Status des Landesbeauftragten für den Datenschutz (LfD). So soll der LfD in den Anwendungsbereich des SÜG einbezogen und damit einer Überprüfung durch eine von ihm zu kontrollierende Behörde unterzogen werden, obwohl und nachdem er von der Bremischen Bürgerschaft gewählt worden ist.

Dies bedeutet, daß er nach seinem Amtsantritt mit der Kontrolle von als geheim eingestuften und von mit nachrichtendienstlichen Mitteln (V-Leute, Observation u. a.) gewonnenen Daten nicht beginnen kann, bis das möglicherweise mehrere Woche oder Monate dauernde Verfahren abgeschlossen ist. Schließlich kann nicht ausgeschlossen werden, daß der von der Bürgerschaft bestimmte LfD nachträglich zum „Sicherheitsrisiko" erklärt wird und sein Amt wieder aufgeben muß.

Weiter unterliegt er dann einer fortwirkenden Überprüfung, d. h. auch für ihn gilt die gesetzliche Verpflichtung der Verfassungsschutzbehörde, fortlaufend Daten über sicherheitsüberprüfte Personen zu sammeln und zu bewerten.

Diese Regelung halte ich für nicht vereinbar mit der besonderen Legitimation des LfD durch die parlamentarische Wahl und mit seiner gesetzlich gewährleisteten und vom Bundesverfassungsgericht in der Volkszählungsentscheidung von 1983 bestätigten Unabhängigkeit. Mit der Wahl dokumentiert die Bürgerschaft ein besonderes Vertrauensverhältnis zum gewählten Amtsinhaber, das sich nicht zuletzt darin ausdrückt, daß sie den LfD nach dem Bremischen Datenschutzgesetz mit Gutachten und der Durchführung von Untersuchungen in Datenschutzfragen betrauen kann.

Ich habe daher als alternative Regelungen angeboten, entweder den LfD ganz aus dem Anwendungsbereich des SÜG herauszunehmen oder zumindest vorzusehen, daß der Senat das Überprüfungsverfahren mit Einverständnis des Kandidaten vor Zuleitung seines Ernennungsvorschlags an die Bürgerschaft (§ 24 BrDSG) durchführen läßt. Die Gesetzentwürfe in Berlin und Niedersachsen gehen darüber hinaus und nehmen — wie ich finde konsequent — alle vom Volk oder vom Landtag gewählten Personen aus dem Überprüfungsverfahren heraus.

Zweiter Punkt: Nach dem SÜG-Entwurf (§ 24 Abs. 5 Satz 2) sollen weiterhin die nach der jetzigen Rechtslage bestehenden Kontrollbefugnisse des LfD eingeschränkt werden (vgl. o. Ziff. 3.2.2.). Wird einem anfragenden Bürger — dies kann ein Sicherheitsüberprüfter selbst ebenso sein wie ein Familienangehöriger, eine Referenzperson oder eine Auskunftsperson — keine Auskunft über die im Rahmen einer Sicherheitsüberprüfung gespeicherten Daten erteilt, verweist ihn der Entwurf ausdrücklich auf die Einschaltung des LfD. Dessen Bemühungen drohen aber ins Leere zu laufen, denn die Auskunft kann auch und gerade dem LfD gegenüber verweigert werden, soweit die oberste Landesbehörde im Einzelfall eine Gefährdung der Sicherheit des Bundes oder eines Landes (durch die Einsichtnahme des LfD!) feststellt.

Diese sog. Staatswohlklausel ist bei der letzten Novellierung des Bremischen Datenschutzgesetzes im Mai 1995 nach intensiver Beratung des Für und Wider gestrichen worden. Gerade in diesen besonders sensiblen Fällen der Auskunftsverweigerung aus Sicherheitsgründen sollte kein kontrollfreier Raum entstehen, sondern dem Betroffenen die Möglichkeit zur Einschaltung des LfD gegeben werden, der alleine das datenschutzrechtlich korrekte Handeln der Verfassungsschutzbehörde oder des Geheimschutzbeauftragten überprüfen kann. Für eine gesonderte und verschlechternde Regelung außerhalb des BrDSG besteht daher kein Anlaß. Der Verzicht auf das Sperrecht der senatorischen Behörden stellt auch keinen Bremer Sonderweg dar, wie im Rahmen der Deputationsbefassung suggeriert wurde. Eine uneingeschränkte Überprüfungsmöglichkeit zumindest des LfD persönlich sehen auch die Datenschutzgesetze von Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Sachsen und Schleswig-Holstein vor.

Bei Redaktionsschluß waren die Beratungen im Datenschutzausschuß noch nicht abgeschlossen.

12.2 Sicherheitsüberprüfung II — „Geheimschutzbeauftragte" als Schwachstelle

Die Vorbereitung und parlamentarische Behandlung der neuen gesetzlichen Regelung für Sicherheitsüberprüfungen (s. o. Ziff. 9.1.) habe ich zum Anlaß genommen, sowohl beim Landesamt für Verfassungsschutz (LfV) als auch bei „Geheimschutzbeauftragten" in einigen Dienststellen den Umgang mit den persönlichen Daten der von diesen Überprüfungen Betroffenen auf der Grundlage der bisherigen Rechtslage zu überprüfen. Dabei ergaben sich erhebliche Mängel „vor Ort" in den Beschäftigungsbehörden, während die Abwicklung im LfV keinen Anlaß zu Beanstandungen gab.

12.2.1 Schwachstelle Geheimschutzbeauftragte

Der sog. Geheimschutzbeauftragte der einzelnen Dienststelle spielt für die Sicherheitsüberprüfung eine entscheidende Rolle. Er legt zunächst fest, welche Beschäftigten für welche Stufe überprüft werden sollen, und begleitet dann das weitere Verfahren bis zur Ermächtigung. Er händigt den Bediensteten, die für eine gewisse Sicherheitsstufe ermächtigt werden sollen, die entsprechenden Formulare aus und nimmt die vom Beschäftigten ausgefüllte Sicherheitserklärung in Empfang. Diese leitet er nach Überprüfung der Angaben an das Landesamt für Verfassungsschutz (LfV) weiter. Nach Abschluß der dortigen Überprüfung teilt das LfV dem Geheimschutzbeauftragten dann das Ergebnis mit. Dieser ermächtigt dann, wenn keine Bedenken bestehen, den jeweiligen Mitarbeiter für die angegebene Sicherheitsstufe. Der Geheimschutzbeauftragte führt Akten und Bücher, in denen er diese Vorgänge vermerkt.

Meine Stichprobenkontrolle hat folgende Mängel aufgezeigt:

- Keiner der von mir aufgesuchten Geheimschutzbeauftragten war vorher für diese Aufgabe geschult oder durch seinen Vorgänger darauf vorbereitet worden.
- Dem LfV als Geheimschutzbeauftragte genannte Behördenleiter übten diese Funktion nicht selber aus, sondern hatten diese Aufgabe an Mitarbeiter delegiert.
- Mitarbeiter auf vor Jahren als sicherheitsempfindlich eingestuften Dienstposten wurden überprüft, obwohl in den letzten zehn Jahren dort kein einziger geheimschutzrelevanter Vorgang angefallen war.
- Die obligatorischen Mitteilungen der Geheimschutzbeauftragten an das LfV über ermächtigte Personen, die zwischenzeitlich aus dem betroffenen Aufgabengebiet oder aus der Dienststelle insgesamt ausgeschieden waren, erfolgten teilweise verspätet. Eine solche „Abmeldung" ist nicht zuletzt deshalb so wichtig, weil sie Voraussetzung ist für den Beginn der Laufzeit der Löschfrist für die beim LfV geführten Sicherheitsakten.
- In den Akten mehrerer Geheimschutzbeauftragter fanden sich z. T. Jahrzehnte alte Unterlagen, die längst hätten vernichtet sein müssen.
- Die von den Geheimschutzbeauftragten in eigener Verantwortung festgelegten Stufen der Sicherheitsüberprüfung waren nicht immer nachvollziehbar. So kann es nicht hingenommen werden, wenn bei einer Behörde seit 1950 kein einziger Eintrag über einen als „geheim" eingestuften Vorgang zu finden ist, gleichwohl seitdem „Generationen" von Beamten und Angestellten der umfangreichen und weit in die Privatsphäre reichenden Prozedur für die Stufe „Geheim" unterzogen worden sind.

12.2.2 Landesamt für Verfassungsschutz — keine Beanstandungen

Das LfV als sog. mitwirkende Behörde überprüft die in der Sicherheitserklärung des Betroffenen gemachten Angaben in verschiedenen Informationssystemen. Dies gilt auch für die Angehörigen und Lebensgefährten, soweit diese in die Sicherheitsüberprüfung einbezogen sind. Soweit eine Ermächtigung auf die Stufe „Streng geheim" beabsichtigt ist, werden darüber hinaus Informationen durch die Befragung von sogenannten Referenz- und Auskunftspersonen eingeholt.

Das gesamte Verfahren wird sowohl in den Informationssystemen des Verfassungsschutzes als auch in Akten und Karteien dokumentiert. Die Aufbewahrungsregelungen des LfV sehen vor, daß die Daten je nach Sicherheitsstufe drei bzw. fünf Jahre nach der Entpflichtung des Ermächtigten bzw. nach dem Erlöschen der Ermächtigung aufgrund Ausscheidens aus dem öffentlichen Dienst gelöscht bzw. vernichtet werden können.

Bei meiner Stichprobe beim LfV Bremen habe ich sowohl in eine Auswahl von Geheimschutzakten als auch in die automatisierten Informationssysteme Einblick genommen. Insgesamt machten Organisation und Abwicklung des Aufgabenbereichs Sicherheitsüberprüfungen im Landesamt einen geordneten und korrekten Eindruck.

Ein Grundproblem der Sicherheitsüberprüfung ist allerdings erneut deutlich geworden: Die durch Ermittler des LfV Bremen oder anderer Ämter für Verfassungsschutz gefertigten Berichte enthalten Angaben, die weit in die Privatsphäre, z. T. bis in die Intimsphäre, hineinreichen. Aufgezeichnet sind Angaben z. B. über religiöse Anschauungen, politische Einstellungen, den Umgang mit Geld und

Alkohol, den beruflichen Werdegang von Ehepartnern, Lebensgefährten, Geschwistern und Eltern usw.. Zwar waren die von mir beim LfV überprüften Berichte in aller Regel distanziert neutral abgefaßt. Doch bleibt bei einer Reihe der o. a. Eigenschaften und biographischen Faktoren — die zudem häufig von Referenzpersonen stammen, deren Einstellung zur überprüften Person, dem Interviewer nicht bekannt ist — unklar, warum sie überhaupt ein mögliches Sicherheitsrisiko indizieren können.

12.2.3 Empfehlungen

Ich werde meine Prüfergebnisse dem Senator für Inneres und dem LfV mitteilen und meine Bereitschaft erklären, an der notwendigen Änderung der bestehenden Praxis mitzuwirken. Das Inkrafttreten des neuen SÜG (s. o. Ziff. 12.1.) bietet die geeignete Gelegenheit, Organisation und Verfahrensabläufe zu verbessern, um den Schutz des Persönlichkeitsrechts der betroffenen Bediensteten zu erhöhen.

Eine meiner Empfehlungen bezieht sich auf den Informationsfluß von den Geheimschutzbeauftragten an das LfV. Die Daten beim LfV können nur aktuell sein, wenn die Geheimschutzbeauftragten ihre Änderungsmitteilungen zeitnah machen. Beispielhaft für diese Schwachstelle ist eine Bitte des LfV vor rund drei Jahren an die Geheimschutzbeauftragten, den von ihnen gemeldeten Personenkreis zu überprüfen. Aufgrund der Rückläufe mußte das LfV ein Viertel (!) der als ermächtigt registrierten Personen löschen.

Anders ausgedrückt: Die Geheimschutzbeauftragten haben die Pflicht, regelmäßig festzustellen, ob überhaupt und ggf. für welche Sicherheitsstufe Überprüfungen weiterhin erforderlich sind bzw. bestehende Ermächtigungen aufrecht erhalten werden müssen. Keinen Anlaß sehe ich auch für die Praxis, Unterlagen über Sicherheitsüberprüfungen vor Ort zum Teil bis weit nach Ausscheiden des Betroffenen aufzubewahren, obwohl sie beim LfV bereits gelöscht worden sind. Als Aufgabe des Senators für Inneres sehe ich es an, die Kenntnislücken der Geheimschutzbeauftragten über ihre Aufgaben und Pflichten zu schließen und ihnen insbesondere für Art und Dauer der Aufbewahrung der Sicherheitsakten klare Hinweise zu geben.

12.3 Telefonüberwachung — Überarbeitung der Richtlinien stagniert

Im 19. Jahresbericht hatte ich über das Ergebnis der Prüfung der Durchführung von Telefonüberwachungs-Maßnahmen durch die Polizei in Bremen und Bremerhaven berichtet (19. JB Ziff. 9.2.). Eine wichtige Konsequenz, um die festgestellten Ablaufdefizite zu beseitigen, war für mich, die Überarbeitung der „Richtlinien für das taktische Vorgehen anläßlich einer Überwachung des Fernmeldeverkehrs nach §§ 100 a und 100 b StPO vom 1. Juli 1990" vorzuschlagen.

In seiner Stellungnahme zum 19. Jahresbericht hat der Senat diese Überarbeitung zugesagt; sie solle durch eine neu zu gründende Arbeitsgruppe unter Berücksichtigung meiner Vorschläge erfolgen. Leider ist dieses Gremium noch nicht einberufen worden. Der Senator für Inneres verweist zur Begründung auf einen Personalengpaß. Ich habe dem Polizeipräsidium meine Bereitschaft zur Mitwirkung mitgeteilt und erwarte, daß in Kürze nach Lösung des Stellenproblems mit der Arbeit an der Ergänzung der Richtlinien begonnen wird.

12.4 Zugriffsprotokollierung bei der Polizei — Löschungsfrist

Über das Verfahren ISA-D (Informationssystem Anzeigen dezentral) haben alle angeschlossenen Polizeidienststellen in Bremen und Bremerhaven die Möglichkeit, Informationen aus Landes- bzw. Bundesverfahren abzufragen. Eine sorgfältige automatische Protokollierung z. B. von Veranlasser und Zeitpunkt eines Datenzugriffs ist unverzichtbar, weil fast alle verarbeiteten Daten einen Personenbezug, vielfach sogar sensiblen Charakter, haben und die Zuordnung der Abfragen zu Zwecken der Dienstaufsicht und der Datenschutzkontrolle sonst nicht möglich wäre. Bleiben die Zugriffsdaten allerdings zulange im Computer, verlängert sich auch das Risiko, daß sie zu anderen unzulässigen Zwecken, z. B. für Leistungskontrollen, genutzt werden.

Bei einer Überprüfung der Speicherungspraxis auf dem Landespolizeirechner habe ich festgestellt, daß noch alle seit Einführung des Verfahrens ISA-D im Jahre 1993 entstandenen Protokolldateien auf der Festplatte gespeichert waren. Die Protokolldaten der letzten zwei Jahre befanden sich auf Sicherungsbändern. Die Einhaltung des Vier-Augen-Prinzips beim Zugriff auf die Protokolldaten kann nicht gewährleistet werden, da das vollständige Systemverwalterpaßwort mehreren Beschäftigten bekannt ist.

Ich halte die Speicherung der Protokolldateien für längstens sechs Monate auf der Festplatte für ausreichend. Auch habe ich angeregt, die Aufbewahrung der Bandsicherungen in die Zuständigkeit des behördlichen Datenschutzbeauftragten zu verlagern.

Das Polizeipräsidium hat zugesagt, daß die Protokolldaten auf der Festplatte nach Ablauf von sechs Monaten automatisiert gelöscht werden. Die Lagerung der Sicherungsbänder beim behördlichen Datenschutzbeauftragten wird vom Polizeipräsidium als nicht erforderlich betrachtet. Diese Frage muß noch geklärt werden.

12.5 „Chaostage" — nur noch ermittlungsrelevante Daten übrig

Im 19. Jahresbericht (vgl. Ziff. 9.1.2. a.E.) hatte ich berichtet, daß das Kommissariat 7 (Staatsschutzdelikte) des Polizeipräsidiums die Aufbereitung der eingegangenen Unterlagen Anfang 1997 als abgeschlossen betrachtete. Wegen des Verbleibs bzw. der Löschung der nicht ermittlungsrelevanten Unterlagen habe ich noch einmal nachgehakt. Nach Angaben des Polizeipräsidiums befinden sich in dem o. a. Kommissariat nur noch die Daten, die für Ermittlungszwecke in Strafverfahren gebraucht werden. Nicht mehr benötigte Unterlagen seien vernichtet worden; dazu wurden mir die entsprechenden Formulare über den Aktenverbleib übersandt. Schließlich sei die auf einem abgeschotteten Einzelplatz-PC geführte Datei mit den Personalien der Betroffenen gelöscht worden.

12.6 Verwaltungsvorschriften zum Ausländergesetz — Entwurf mit Mängeln

Auf das Fehlen von Verwaltungsvorschriften zum 1991 in Kraft getretenen Ausländergesetz und die daraus resultierende Gefahr von Behörde zu Behörde unterschiedlicher Interpretation der Datenverarbeitungsvorschriften zu Lasten der Betroffenen habe ich wiederholt hingewiesen (vgl. bereits 14. JB Ziff. 2.2.5.2). Seit Herbst 1997 liegt ein neuer Entwurf für eine bundeseinheitliche Verwaltungsvorschrift vor, der in manchen Vorschriften den Eindruck erweckt, die Interpretationsspielräume des Ausländergesetzes ausschließlich zuungunsten der Betroffenen und aus der Interessenlage der Ausländerbehörden zu nutzen.

Wichtigstes Beispiel: Auch im Ausländergesetz (§ 75 Abs. 2) steht der verfassungsrechtlich fundierte datenschutzrechtliche Grundsatz, daß Angaben über einen Betroffenen zunächst bei ihm selbst zu erheben sind (vgl. § 13 Abs. 2 Bundesdatenschutzgesetz, restriktiver § 10 Abs. 2 BrDSG); der Bürger soll möglichst weitgehend wissen bzw. erfahren, was die Verwaltung über ihn weiß. Das Ausländeramt ist m. a. W. gehalten, für das jeweilige Verwaltungsverfahren relevante Daten zunächst von dem Ausländer zu erfragen und erforderliche Unterlagen bzw. Dokumente direkt bei ihm anzufordern. Die Datenerhebung bei Dritten, also auch die Rückfrage bei anderen Behörden, ist nur unter im Gesetz fixierten einschränkenden Voraussetzungen zulässig. Liegt keine die Einschaltung der anderen Behörde vorschreibende oder zwingend voraussetzende Norm vor, muß die datenverarbeitende Stelle prüfen, ob die Erhebung am Betroffenen vorbei nicht dessen schutzwürdige Belange verletzt. Der Entwurf der Verwaltungsvorschriften enthält jedoch einen Katalog von Erhebungsregelungen bei dritten Stellen, der so lang ist, daß dieser Grundsatz in sein Gegenteil verkehrt erscheint.

Die Entwurfsverfasser scheinen davon auszugehen, daß Ausländer in der Regel nicht bereit sind, die für die Bearbeitung der sie betreffenden Verwaltungsvorgänge notwendigen Daten zu offenbaren. Statt dessen sollen die Informationen nicht nur bei Meldebehörden, Sozialbehörden und Arbeitsämtern, sondern auch z. B. bei kirchlichen und freien Wohlfahrtseinrichtungen direkt beschafft werden, ohne daß vorher der Versuch gemacht wird, sie vom Ausländer selbst zu erhalten. Die Begründung für diese Handhabung, damit werde die Informationsbeschaffung beschleunigt, reicht aber als Rechtfertigung für eine Abweichung vom Prinzip der Erhebung beim Betroffenen selbst dann nicht aus, wenn sie zuträfe.

Weitere Einwände betreffen u. a. die m. E. zu weit gehenden Möglichkeiten telefonischer Ermittlungsersuchen und Unklarheiten in der Begrifflichkeit bei anzugebenden Sozialhilfeleistungen.

Ich bedaure, daß der Senator für Inneres auf meine Stellungnahme nicht reagiert hat (vgl. Ziff. 3.2.1.).

12.7 Bonitätsprüfung mit deutscher Gründlichkeit

Nach dem Ausländergesetz (§§ 82 bis 84) kann man behördlich dazu verpflichtet werden, alle mit dem Aufenthalt eines nach Deutschland eingeladenen Ausländ-

ders zusammenhängenden Kosten z. B. für Lebensunterhalt, notwendige medizinische Versorgung und Rückreise zu übernehmen, wenn der Ausländer selbst dazu nicht in der Lage ist oder nicht die entsprechenden Versicherungen abgeschlossen hat.

Im Vorgriff auf die in Ziff. 12.6. erwähnten Verwaltungsvorschriften zum Ausländergesetz hat der Senator für Inneres mit Erlaß vom 22. Oktober 1997 die Ausländerbehörden in Bremen und Bremerhaven angewiesen, vor der Abgabe der Verpflichtungserklärung nach § 84 Ausländergesetz die jeweiligen Gastgeber einer Bonitätsprüfung zu unterziehen.

Dieses Verfahren war in Bremen bisher vergleichsweise unbürokratisch, die Gastgeber gingen entweder zum Stadtamt oder zu ihrem Ortsamt und unterschrieben dort in der Regel ohne weitere Formalitäten die Verpflichtungserklärung, die dann von einem Beamten beglaubigt wurde.

Nach dem neuen Erlaß muß der Einladende umfassend seine wirtschaftliche und soziale Situation offenlegen. So sind die Einkommensverhältnisse durch Vorlage des Steuerbescheides, des Rentenbescheides, des Bescheides des Arbeitsamtes über das Arbeitslosengeld oder einer Verdienstbescheinigung nachzuweisen; auch die Wohnverhältnisse (Eigentum oder Miete) werden abgefragt. Außerdem ist der Nachweis über eine für den ausländischen Gast bestehende Krankenversicherung vorzulegen, obwohl ja noch gar nicht feststeht, ob der Besucher tatsächlich später ein Visum erhält.

Kritikwürdig ist zum einen der zu große Umfang der von den deutschen Gastgebern offenzulegenden Informationen. Mir konnte auf Nachfrage kein Fall genannt werden, in dem nach dem bisherigen einfacheren Verfahren ausgestellte Verpflichtungserklärungen ins Leere gingen, weil die finanzielle Situation der Gastgeber nicht genügend geprüft worden wäre. Hinzu kommt, daß die Angaben über Arbeitgeber, Beruf, Wohnungseigentum usw. des Gastgebers in das Formular eingetragen werden, das dem Einzuladenden selbst zugeschickt wird, damit dieser wiederum sie der deutschen Auslandsvertretung in seinem Heimatland vorlegt. Sowohl der potentielle ausländische Besucher als auch — etwa in Diktaturen — staatliche Stellen seines Landes, die über die Zulässigkeit seiner Ausreise zu entscheiden haben, erfahren sensible Angaben, die sie nichts angehen. Die Risiken, die sich für den Einlader daraus ergeben, daß eine unbekannte Zahl dritter Personen im Ausland Kenntnis von seiner Finanzlage erhält, sind für ihn nicht einschätzbar. Es ist schwer nachzuvollziehen, warum den deutschen Konsulaten nicht die schlichte Bestätigung der hiesigen Ausländerbehörden ausreichen soll, daß eine Verpflichtungserklärung vorliegt.

Meine Einwände gegen diese neue, unverhältnismäßige Kontrollprozedur, die auch die Mehrzahl meiner Kollegen gegenüber ihren jeweiligen Innenressorts geäußert hat, habe ich dem Senator für Inneres vorgetragen, ohne eine Antwort zu erhalten.

12.8 Melderecht — Probleme und Reformbedarf

12.8.1 Novellierung des Bremischen Meldegesetzes überfällig

12.8.1.1 Anpassung an Bundesrecht

Ich habe in der Vergangenheit schon mehrfach (zuletzt in meinem 17. Jahresbericht, Ziff. 9.4.1) darauf hingewiesen, daß das Bremische Meldegesetz den neuen rechtlichen und technisch-organisatorischen Gegebenheiten angepaßt werden muß. So wurde bereits im Jahre 1994 (!) das Melderechtsrahmengesetz des Bundes (MRRG) geändert, mit dem u. a. die Aufgaben und Befugnisse der Meldebehörden präzisiert, die Krankenhausmeldepflicht sowie die Einsichtnahme der Polizei in die Krankenhausunterlagen neu gestaltet wurden und neben dem in Bremen bereits realisierten Widerspruchsrecht für Betroffene bei Datenübermittlungen an politische Parteien auch eine Löschungsverpflichtung der Parteien für die übermittelten Meldedaten (spätestens vier Wochen nach einer Wahl) eingeführt wurde. Die Neufassung des MRRG hat also die datenschutzrechtlichen Situation des Bürgers im Meldewesen deutlich verbessert.

Die gesetzliche Übergangsfrist von zwei Jahren zur Anpassung des Landesmeldegesetzes ist seit langem, d. h. seit März 1996, abgelaufen mit der Folge, daß das Bundesland Bremen seine Angleichungsverpflichtung aus Art. 75 Abs. 3 Grundgesetz nicht einhält. Außerdem gilt, daß die Regelungen des Landesmeldegesetzes,

die den Änderungen des MRRG nicht mehr entsprechen, seit März 1996 außer Kraft sind, vielmehr insoweit die geänderten Bestimmungen des MRRG unmittelbar greifen.

In der Datenschutzausschußsitzung am 26. November 1996 hatte zwar der Senator für Inneres die Novellierung des Landesmeldegesetzes für das Jahr 1997 angekündigt; in der Sitzung des Datenschutzausschusses am 18. November 1997 wurde dagegen seitens des Innensenators erklärt, daß mit einer Novellierung des Landesmeldegesetzes 1998 nicht zu rechnen sei. Ich bin der Auffassung, daß die Übernahme der datenschutzrechtlichen Verbesserungen des Bundesrahmenrechts in das bremische Landesrecht überfällig ist und daher eine Novellierung des Landesmeldegesetzes dringend geboten ist.

Hinzu kommt: Auch das Schengener Abkommen zwingt, was z. B. die Meldepflicht für Hotelgäste sowie mitreisende Personen anbetrifft, zur Überprüfung bzw. Anpassung der Regelungen des Bremischen Meldegesetzes. Gleiches gilt für das geänderte Wehrpflichtgesetz mit seinen neuen Regelungen zur Erfassung der Wehrpflichtigen.

12.8.1.2 Datenübermittlung an Parteien — mehr Wahlmöglichkeiten für den Wahlbürger

Darüber hinaus ergibt sich aus der systemtechnischen und organisatorischen Entwicklung und aus der allgemeinpolitischen Diskussion Anlaß, über weitere Korrekturen des Melderechts nachzudenken.

Immer wieder Gegenstand von Bürgeranfragen, Beschwerden sowie Mängelrügen meinerseits sind die Meldedatenübermittlungen an politische Parteien im Vorfeld der Wahlen (vgl. hierzu 14. Jahresbericht, Ziff. 2.2.3.3; 17. Jahresbericht, Ziff. 9.4.1). Die Bürger Bremens werden in diesem und im nächsten Jahr mehrfach an die Wahlurnen gerufen: Im September 1998 zur Bundestagswahl, im Frühjahr 1999 zur Bürgerschafts- und Beirätewahl und kurz darauf zur Europawahl sowie im Herbst 1999 zur Kommunalwahl in Bremerhaven (sofern nicht wieder eine Ankoppelung dieser Wahl an die Bürgerschaftswahl erfolgt). Es steht zu befürchten, daß die Bürgeranfragen und Beschwerden über die Meldedatenübermittlung an die politischen Parteien, insbesondere die des rechtsradikalen Spektrums, dann wieder stark zunehmen werden.

Nach der gegenwärtigen Rechtslage in Bremen können die wahlberechtigten Bürger der Weitergabe ihrer Daten an die politischen Parteien widersprechen. Die Parteien ihrerseits müssen aufgrund des MRRG die übermittelten Wählerdaten spätestens vier Wochen nach der Wahl löschen. Im übrigen dürfen nach einer Anweisung des Senators für Inneres, mit der er einem Beschluß der Bürgerschaft (Landtag), folgte (Drs. 14/214 vom 13. Februar 1996), die Wählerdaten nicht an Parteiorganisationen außerhalb des Landes übermittelt und ausschließlich zu Wahlwerbezwecken verwendet werden. In der Sitzung des Datenschutzausschusses am 18.11.1997 wurde dies ausdrücklich nochmals bestätigt (vgl. o. Ziff. 10.2.1.). Melderechtlich nicht geregelt ist die Art der Übermittlung, ob in Papierform (z. B. Liste, Aufkleber) oder in elektronisch verwertbarer Form (z. B. Diskette, Magnetband, CD-ROM).

Im Hinblick auf die vielen Beschwerden und die z. T. auch in meinen Jahresberichten dokumentierten Verstöße bei der Durchführung dieser Melderechtsregelung hatte ich nicht nur landeseinheitliche Durchführungsbestimmungen gefordert, sondern auch eine Neuregelung der Gesetzesbestimmung selbst angeregt mit dem Ziel, anstelle der Widerspruchslösung für die Betroffenen die Einwilligungslösung einzuführen. Die meisten Beschwerden könnten mit einer solchen Neuregelung, bei der die Bürgerinnen und Bürger vorher, etwa bei der Anmeldung, ihr Einverständnis erklären müssen, beseitigt werden.

Möglich wäre aber auch, politisch interessierten Bürgern, die sich nicht generell, sondern nur gegen bestimmte Formen der Wahlwerbung wenden, jedenfalls entsprechende Wahlmöglichkeiten zu eröffnen. Mindestens müßte die Information über das Widerspruchsrecht, die derzeit nur einmal und im „Kleingedruckten" der „Amtlichen Bekanntmachungen" der Tagespresse stattfindet, deutlich verbessert werden.

Im Zusammenhang mit den Überlegungen zur Neuregelung des § 33 Abs. 1 Bremisches Meldegesetz sollte auch versucht werden, die Diskrepanz der Fristen zwischen dem Melderecht und dem Wahlrecht zu beseitigen. So dürfen bereits sechs

Monate vor dem Wahltermin Wählerdaten an eine Partei übermittelt werden, obwohl zu diesem Zeitpunkt noch nicht feststeht, ob diese sich überhaupt an der Wahl beteiligt und damit die erhaltenen Angaben zu „Wahlwerbezwecken" verwenden wird.

12.8.1.3 Datenübermittlungen an Adreßbuchverlage — Einwilligung statt Widerspruch

Regelmäßig werden Meldedaten auch an Adreßbuchverlage übermittelt, wobei hierbei ebenfalls ein Widerspruchsrecht der — volljährigen — Einwohner besteht. Auch dieses Widerspruchsrecht ist den wenigsten Einwohnern bewußt, obwohl bei der Anmeldung und vor den Datenübermittlungen an die Adreßbuchverlage amtlich auf dieses Recht hingewiesen wird. Diese Bekanntmachungen werden kaum wahrgenommen mit der Folge, daß viele Einwohner davon keinen Gebrauch machen. Bei den volljährig werdenden Einwohnern wird automatisch Zustimmung zur Datenübermittlung unterstellt, obwohl dies keineswegs als Regel angenommen werden kann.

Die Art der Meldedatenübermittlung an die Adreßbuchverlage und die Art der Weiterverwendung der Daten durch die Adreßbuchverlage ist gesetzlich nicht näher beschrieben, so daß z. B. neue informationstechnische Möglichkeiten der Datenpräsentation wie etwa auf CD-ROM oder Einstellung ins Internet „Begehrlichkeiten" der Verlage auslösen. Auch hierzu hatte ich schon berichtet (vgl. 19. JB, Ziff. 9.3.2). Es freut mich, daß der Senat in seiner Stellungnahme zu meinem 19. Jahresbericht sich meiner Auffassung angeschlossen hat, wonach die schutzwürdigen Interessen der Betroffenen die Weitergabe ihrer Meldedaten auf CD-ROM ausschließen.

Datenschutzrisiken ergeben sich vor allem daraus, daß Adreßbücher von vielen Stellen für die unterschiedlichsten und für den Bürger nicht transparenten Zwecke verwendet werden, vor allem auch von Adreßhandelsunternehmen, Auskunfteien und vom Versandhandel. Einige Bundesländer wie z. B. das Saarland und Nordrhein-Westfalen haben die Rechtsposition der Betroffenen in diesem Bereich dadurch verstärkt, daß ihr Melderecht bei den Datenübermittlungen an Adreßbuchverlage anstelle des Widerspruchsrechts eine ausdrückliche Einwilligung in die Datenübermittlung vorsieht. Dies entspricht den Vorstellungen der informationellen Selbstbestimmung der Betroffenen wesentlich besser als die derzeitige Widerspruchslösung und sollte deshalb auch in das Bremische Meldegesetz übernommen werden.

12.8.1.4 Melderegistersperren — Fristen verlängern

§ 32 Abs. 5 Bremisches Meldegesetz sieht die Eintragung einer Melderegistersperre vor, wenn ein Betroffener glaubhaft macht, daß ihm oder einer anderen Person Gefahr für Leib und Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange droht. Eine zeitliche Befristung sieht das Gesetz nicht vor, was bedeutet, daß die Frist zumindest solange andauert, wie die Gefahr droht. Nicht sachgerecht erscheint mir, diese Frist pauschal auf ein Jahr festzusetzen, wie dies in der Praxis der bremischen Meldebehörden geschieht. Zwar werden die Einwohner in solchen Fällen angeschrieben und gefragt, ob der Eintragungsgrund für die Sperre noch besteht. Erfolgt aber überhaupt keine Reaktion, wird die Auskunftssperre aufgehoben; die Meldedaten stehen also wieder für Auskünfte zur Verfügung. Bei verzogenen Einwohnern, die nicht reagieren, aber weiterhin auf die Wirksamkeit der Auskunftssperre vertrauen, kann dies bisweilen zu unangenehmen Überraschungen führen, wie ich in einem Beschwerdefall feststellen mußte.

Bei der Melderegistersperre des § 32 Abs. 6 Bremisches Meldegesetz, die keine persönliche Gefährdung, sondern nur das Vorliegen eines „berechtigten Interesses" voraussetzt, sieht das Gesetz dagegen eine längere, nämlich zweijährige Sperre vor. Nach meiner Auffassung liegen diese unterschiedlichen Fristen angesichts der umgekehrten Gewichtung der beiden Tatbestände nicht im Interesse der sperrberechtigten Bürger.

12.8.2 Meldedatenübermittlungsverordnung — Wird das Melderegister zum „Selbstbedienungsregister"?

Im Berichtsjahr hatte ich mich mit einem umfangreichen Paket von Änderungen der Bremischen Meldedatenübermittlungsverordnung (Brem. MeldDÜV) zu beschäftigen. Dabei ging es u. a. um

- eine neuerliche Ausweitung des jetzt schon sehr umfangreichen Katalogs von Behörden, die Meldedaten im automatisierten Abrufverfahren erhalten dürfen, z. B. die Steuerfahndungsstellen, Einbürgerungs- und Staatsangehörigkeitsbehörden, Standesämter, Feuerwehr, Kataster- und Vermessungsverwaltung, Entsorgungsbetriebe, Straßenverkehrsbehörde zur Ausstellung von Parkerlaubnissen, Amtsgerichte,

- eine Ausweitung der regelmäßigen Datenübermittlungen an die Jugendämter und an die statistischen Ämter der beiden bremischen Gemeinden,

- die Einführung einer regelmäßigen Meldedatenübermittlung an Radio Bremen.

Ich hatte zu den Änderungsvorschlägen ausführlich Stellung genommen und dabei viele der geplanten Änderungen als nicht erforderlich problematisiert angesichts der bestehenden Möglichkeiten, im Einzelfall Auskünfte bzw. Daten aus dem Melderegister zu erhalten.

Insbesondere der Katalog der Behörden, die im automatisierten Abrufverfahren, d. h. im Wege der „Selbstbedienung", Meldedaten abrufen können, verlängert sich immer mehr. Betrachtet man die bisherigen Änderungen der Brem. MeldDÜV, so muß man feststellen, daß sich das Melderegister immer mehr zu einem allgemeinen Informationsregister für beliebig viele Stellen und Behörden entwickelt und sich damit von der ursprünglichen Zielsetzung, die Einwohner lediglich zu registrieren, um ihre Identität und Wohnungen feststellen und nachweisen zu können, immer weiter entfernt. Diese Entwicklung verändert den traditionellen Charakter und die Funktion dieses Registers und zwingt zu neuen Überlegungen zur Einwohnermeldepflicht und zur Zugänglichkeit der ja vom Bürger zwangsweise erhobenen Meldedaten.

Das Bundesverfassungsgericht hatte im Volkszählungsurteil von 1983 ein aus dem Grundgesetz abgeleitetes informationelles Selbstbestimmungsrecht des Bürgers reklamiert, in das nur im überwiegenden Allgemeininteresse und auf normenklarer gesetzlicher Grundlage eingegriffen werden darf. Eine zu weite Öffnung des Melderegisters für alle möglichen Stellen und Zwecke erfüllt mit Sicherheit nicht die Anforderung des Bundesverfassungsgerichts an das Vorliegen eines überwiegenden Allgemeininteresses. Viele der regelmäßigen Übermittlungen aus dem Melderegister basieren zwar auf für sich genommen verständlichen arbeitsökonomischen oder organisatorischen Überlegungen, rechtfertigen aber nicht den vor allem mit dem Direktabruf verbundenden Eingriff in die geschützte Grundrechtsposition. Viele der regelmäßigen Datenübermittlungen ließen sich durch ein Verwaltungshandeln, das stärkeres Vertrauen in die Angaben des Bürgers setzt, vor allem aber durch Melderegisteranfragen im konkreten überprüfungsbedürftigen Einzelfall erledigen, sind also entbehrlich.

Gegen Ende 1997 erhielt ich einen neuen überarbeiteten Entwurf zur Änderung der Brem. MeldDÜV mit einem umfangreichen Stellungnahmepaket der Verwaltung. Praktisch zeitgleich wurde mir ein Auszug aus dem neuen Änderungsentwurf als eigenständiger Entwurf zur Änderung der Brem. MeldDÜV mit eiligen bzw. weitgehend unstreitigen Änderungsvorschlägen zugeleitet. Unter anderem ging es hier um

- redaktionelle oder formale Anpassungen,

- Änderungen bei einigen übermittelbaren Datenkatalogen,

- die Ausweitung des Katalogs von Behörden, die Meldedaten im automatisierten Abrufverfahren erhalten dürfen (Standesämter, Feuerwehr),

- die Einführung der regelmäßigen Übermittlung von Meldedaten an Radio Bremen.

Auch zu diesem Änderungsentwurf habe ich mich geäußert. In der Sitzung der staatlichen Deputation für Inneres Mitte Januar 1998 wurde schließlich ein auf der Verwaltungsebene abgestimmter Änderungsentwurf einvernehmlich beschlossen. Die hierbei nicht berücksichtigten Änderungsvorschläge sollen im weiteren Verfahren beschlossen werden. Ich hoffe, daß meinen kritischen Anmerkungen zu diesen Änderungsvorschlägen dabei Rechnung getragen wird.

12.9 Zweitwohnungssteuer in Bremen — Datenübermittlung en masse, aber kaum Einnahmen

In meinem 18. Jahresbericht (Ziff. 7.1.4) hatte ich die Tauglichkeit und Treffsicherheit des Melderegisters hinsichtlich der für die Zweitwohnungsbesteuerung

relevanten Fälle bezweifelt und empfohlen, die diesbezügliche Änderung der Brem. MeldDÜV nur befristet einzuführen. Dieser Anregung wurde damals nicht gefolgt.

Inzwischen liegen erste Erfahrungen mit der Erhebung der Zweitwohnungssteuer vor. Diese bestätigen die von mir damals vorgetragenen Zweifel: Das Aufkommen der Zweitwohnungssteuer in Bremen liegt nur geringfügig über ihren Erhebungskosten. Der Hauptgrund dafür ist die Bestimmung der Steuerpflichtigen, die nach einem Wohnungsbegriff (Zweitwohnung) definiert werden, der mit dem Wohnungsbegriff des Melderechts (Nebenwohnung) wenig zu tun hat. Die Zahl der Steuerpflichtigen liegt deutlich unter der Zahl, die erwartet wurde und die in Bremen mit Nebenwohnung gemeldet sind. Um ein Steueraufkommen in praktisch gleicher Höhe wie die Erhebungskosten zu erzielen, wird ein riesiger Übermittlungsvorgang aus dem Melderegister (ca. 35.000 Fälle) in Gang gesetzt, bei dem der größte Teil überflüssig ist.

Bleibt es bei dieser Relation, stellt sich für mich die Frage, ob die massenhafte Datenweitergabe weiterhin gerechtfertigt werden kann. Ich empfehle daher, in diesem Sinne das bremische Ortsgesetz über die Erhebung einer Zweitwohnungssteuer und damit zugleich auch die entsprechende Bestimmung in der Brem. MeldDÜV zu überprüfen.

12.10 Sperrvermerke und Wählerverzeichnis — Problem noch immer ungelöst

Aus Anlaß der Beratungen meines 17. Jahresberichts (Ziff. 9.4.2) im Datenschutzausschuß am 26. November 1996 hatte der Senator für Inneres zugesagt, das Bremische Wahlgesetz so zu ändern, daß Sperrvermerke, die zum Schutz vor Belästigungen oder Bedrohungen im Melderegister eingetragen worden sind, auch bei der Erstellung des öffentlich auszulegenden Wählerverzeichnisses beachtet werden. Anderenfalls drohen diese Sperrhinweise wirkungslos zu bleiben.

Trotz mehrmaliger Nachfrage habe ich bisher noch keinen entsprechenden Änderungsentwurf erhalten.

13. Justiz

13.1 Video im Gerichtsverfahren — datenschutzrechtliche Folgeprobleme

Die Anlässe und der Umfang, in dem die Videotechnik bei der Durchführung von Gerichtsverfahren genutzt werden sollen, sind umstritten. In Bremen haben sich nach Auskunft des Senators für Justiz und Verfassung die Gerichte u. a. wegen des hohen technischen und finanziellen Aufwandes und wegen der Auswirkung auf die Unmittelbarkeit und Mündlichkeit der Verhandlung eher zurückhaltend geäußert.

Inzwischen ist der Gesetzgeber tätig geworden und hat Anfang März 1998 das Gesetz zum Schutz von Zeugen bei Vernehmungen im Strafverfahren (Zeugenschutzgesetz — ZSchG) (vgl. BR-Drs. 212/98; Einverständnis des Bundesrates in BR-Drs. 212/98 — Beschluß) verabschiedet. Eines der Ziele der Neuregelung ist der Schutz kindlicher Zeugen, denen erspart bleiben soll, mehrfach zu der gleichen Sache eine Aussage zu machen oder aber im Gerichtssaal erneut auf den Tatverdächtigen zu stoßen.

Datenschutzprobleme ergeben sich vor allem dann, wenn von Zeugenvernehmungen Videoaufzeichnungen gefertigt werden, die später nach Abschluß des Prozesses zu den Akten genommen und archiviert werden. Zu klären sind auch die Zulässigkeit und die Bedingungen der Übersendung dieser Videomitschnitte an und des Kopierens durch den Verteidiger.

Ich habe in einem Arbeitskreis mitgearbeitet, der die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Informationelle Selbstbestimmung und Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren" vorbereitet hat. Diese Entschließung ist unter Ziff. 22.7. abgedruckt.

13.2 Verdienstausfallbescheinigung — Formular änderungsbedürftig

Eine Bürgerin übersandte mir den Vordruck zur Ladung als Zeugin für ein Verfahren vor dem OLG Bremen. Die sog. Verdienstausfallbescheinigung zur Vorlage beim Arbeitgeber, die in diesem Fall Angaben über ein Darlehen der Zeugin enthielt, war das Beweisthema vorangestellt, zu dem sie vernommen werden sollte. Diese Formulargestaltung hat zur Konsequenz, daß dem Arbeitgeber zwangsläufig sensible private Informationen seiner Arbeitnehmer bekannt werden.

Ich habe mich daraufhin an das Hanseatische Oberlandesgericht gewandt und die datenschutzrechtlichen Einwände vorgetragen. Der Präsident des OLG hat daraufhin erklärt, aufgrund meiner Bedenken solle in Zukunft für die „Bescheinigung über Verdienstausfall" ein gesondertes Blatt verwandt und separat der Ladung beigefügt werden.

13.3 Elektronisches Grundbuch

In Bremen ist die flächendeckende Einführung des maschinell geführten, vollelektronischen Grundbuches zum 1. Januar 1999 geplant. Direktzugriff sollen zunächst nur die Grundbuchämter im Land Bremen erhalten. Realisiert werden soll das Verfahren über eine Client-Server-Lösung mit dem Softwareprodukt SOLUM-STAR. Dieses Programmpaket enthält eine Reihe wichtiger Funktionen zur Datensicherung, insbesondere Möglichkeiten der Verschlüsselung und der Verwendung elektronischer Unterschriften. Deshalb bin ich an der Begleitung dieses DV-Projekts besonders interessiert.

Inwieweit die Programmfunktionen, die einen online-Zugriff durch z. B. Notare, Gerichte, Behörden, Banken und Versicherungen in Bremen ermöglichen, realisiert werden, muß noch festgelegt werden. Ich gehe davon aus, daß ich in regelmäßigen Abständen vom Senator für Justiz und Verfassung über den Verfahrensstand informiert werde und mir so rechtzeitig ein Datenschutzkonzept zur Stellungnahme vorgelegt wird, daß es vor Beginn des Echtbetriebes am 1. Januar 1999 mit mir abgestimmt ist.

13.4 Versorgungswerk der Hanseatischen Rechtsanwaltskammer — Satzung mit Lücken

Im letzten Jahr hat die Bremische Bürgerschaft das Gesetz über die Rechtsanwaltsversorgung in der Freien Hansestadt Bremen (RAVG) verabschiedet (BremGBl. Nr. 43 vom 30. September 97, S. 329). § 10 des Gesetzes sieht vor, daß die Rechtsanwaltsversorgung ihre Angelegenheiten durch Satzung regelt. Gem. § 10 Abs. 2 des Gesetzes trifft die Satzung besondere Bestimmungen über den Datenschutz. In meiner Stellungnahme zu der einschlägigen Satzungsbestimmung habe ich empfohlen, eine Reihe von Präzisierungen sowohl für die Verarbeitungsmodalitäten beim Versorgungswerk selbst als auch für die Datenflüsse zwischen der Kammer und dem Versorgungswerk aufzunehmen.

Meine Beteiligung erfolgte allerdings sehr spät. Die Satzung ist bereits am 1. Januar 1998 in Kraft getreten (BremABl. 98, 17 ff.). Meine Empfehlungen zur Satzung wurden nicht aufgegriffen. Ich werde die Angelegenheit weiter verfolgen.

13.5 Strafvollzug — neue Entwicklungen

Seit meiner umfangreichen Datenschutzprüfung in der Justizvollzugsanstalt Oslebshausen im Jahr 1993 (vgl. 16. JB, Ziff. 6.1.) und den daraus in der Folgezeit sowohl vom Justizsenator als auch von den in der JVA Verantwortlichen gezogenen Konsequenzen (vgl. 17. JB, Ziff. 10.4) verfolge ich die Entwicklungen in diesem Bereich mit verstärkter Aufmerksamkeit.

Ich habe anläßlich der Bestellung einer neuen Anstaltsleitung der JVA Bremen in einem Gespräch verschiedene Fragen des Datenschutzes im Strafvollzug erörtert. Thematisiert wurde dabei auch der Modellversuch zum Einsatz privater Sicherheitsdienste. Dieser ist zwar zum Hofdienst und außerhalb der Pforte zur Überprüfung der Besucher eingesetzt, erhält aber zu personenbezogenen Daten der Insassen keinen Zugang, da seinen Mitarbeitern der Zutritt zu den Häusern verboten ist. Angestrebt wird der Einsatz allerdings auch innerhalb der Pforte. Die Anstaltsleitung hat mir zugesichert, sich dann zur Klärung der Datenschutzfragen mit mir in Verbindung zu setzen.

Inzwischen hat sich auch der Gesetzgeber eines Teils der Datenschutzprobleme in Gefängnissen angenommen. Im Februar 1998 wurde der Entwurf eines 4. Gesetzes zur Änderung des Strafvollzugsgesetzes (4. StVollzG) im Bundesrat beraten (BR-Drs. 57/98). In einer Stellungnahme habe ich dazu gegenüber dem Senator für Justiz und Verfassung Verbesserungsvorschläge für Detailregelungen gemacht. Der Entwurf enthält in den §§ 179-187 eigene bereichsspezifische Regelungen über den Datenschutz, z. B. über die Zweckbindung und über die besondere Geheimhaltung religiöser und medizinischer Daten. Der Entwurf greift auch die von mir seit langem erhobene Forderung auf, die Aufbewahrungsfristen von Krankenakten und Gefangenenbüchern zu verkürzen. Die abschließende Stellungnahme des Bundesrates erging am 6. März 1998 (BR-Drs. 57/98 — Beschluß).

13.6 Mitteilungen aus dem Straf- und Zivilverfahren — die Justiz als Informationsdienstleister

Auf Grundlage der Regelungen im Justizmitteilungsgesetz [JuMiG (BGBl 1997, 1430 ff)] erarbeiten die Justizverwaltungen der Länder Richtlinien für die Ausführung der Mitteilungspflichten aus dem Straf- und Zivilverfahren.

Die Mitteilungen in Zivilsachen (MiZi) schreiben für 110 Fallkonstellationen Übermittlungen aus Zivilverfahren insbesondere an andere öffentliche Stellen vor. Hierzu zählen zum Beispiel Mitteilungen über Unterbringungsmaßnahmen, über Klagen auf Räumung von Wohnraum bei Zahlungsverzug des Mieters oder an das Kraftfahrtbundesamt und das Bundeszentralregister bei Namensänderung.

In meiner Stellungnahme gegenüber dem Justizsenator habe ich u. a. um die Berücksichtigung folgender Gesichtspunkte gebeten:

- Möglichst direkte Mitteilungswege an die Stellen, die die Informationen benötigen, d. h. keine langen Dienstwege,
- Benachrichtigungspflicht an Betroffene, soweit sie mit der Datenübermittlung durch das Gericht nicht rechnen können,
- Dokumentationspflicht über Mitteilungen und Entscheidungen in der jeweiligen Akte,
- Begrenzung von Umfang und Inhalt der Mitteilungen auf das unbedingt Erforderliche,
- Korrekturmitteilungen bei Änderung der mitgeteilten Daten sowie bei Änderung von Sachverhalten im Laufe des Prozesses.

Die mir übersandten Regelungsentwürfe zu den Mitteilungen in Strafsachen (MiStra) enthalten rund 60 Vorschriften mit Übermittlungspflichten aus verschiedensten Anlässen und an eine kaum übersehbare Vielzahl von Behörden und privaten Stellen. Für diesen Bereich habe ich z. T. ähnliche Vorschläge gemacht wie für die MiZi. So ist es z. B. notwendig, bei Mitteilungen an Firmen so gezielt zu adressieren, daß nicht der gesamte Betrieb Kenntnis erhält. Je nach Sensibilität der übermittelten Angaben müssen innerhalb der Justiz die Anordnungsbefugnisse unterschiedlichen Ebenen (z. B. Geschäftsstelle/Staatsanwaltschaft/Richter) zugewiesen werden.

Da es sich um bundeseinheitlich zu handhabende Regelungen handelt, müssen sich die Justizverwaltungen der Länder gemeinsam auf die Inhalte verständigen. Vorgesehen ist das Inkraftreten für den Sommer 1998. Ob meine Anregungen berücksichtigt werden, stand bei Redaktionsschluß noch nicht fest.

14. Gesundheit, Jugend und Soziales

14.1 Krebsregister des Landes Bremen

14.1.1 Bundesrechtliche Vorgaben

Ärzte, Wissenschaftler, insbesondere Epidemiologen und Verantwortliche in Politik und Verwaltung versprechen sich und der Bevölkerung mit der Einrichtung von Krebsregistern in ganz Deutschland mit den Daten möglichst aller an Krebs erkrankten Menschen eine bessere Erforschung der Ursachen und in Folge wirksamere Maßnahmen zur Prävention und Therapie der Krankheit. Deshalb hat Ende 1994 der Bund in seinem Krebsregistergesetz (KRG) die Länder verpflichtet, bis zum Beginn des Jahres 1999 flächendeckende Krebsregister einzurichten mit dem Ziel fortlaufender und einheitlicher Erhebung von Daten über das Auftreten von Krebserkrankungen. Zwecks Nutzung der Daten zu Forschungszwecken soll es auch möglich sein, den Personenbezug der gespeicherten Daten herzustellen, z. B. um den Verursachungsfaktoren in Einzelfällen auf die Spur zu kommen und um einzelne Krankheitsverläufe zu untersuchen.

Zugleich war und ist man sich mit den Datenschutzbeauftragten darin einig, daß es sich um höchst sensible Daten handelt, daß der entgegenstehende Wille Betroffener zu beachten ist und alles nur mögliche zu tun ist, um zu verhindern, daß mit personenbezogenen Registerdaten Mißbrauch betrieben wird, d. h. sie zu anderen als zu den gesetzlich vorgesehenen Zwecken genutzt werden.

Der Bund machte hierfür im KRG bestimmte mit den Datenschutzbeauftragten von Bund und Ländern abgestimmte Vorschläge, er erlaubte es zugleich aber den Ländern, davon abzuweichen, soweit die Vergleichbarkeit der registrierten Daten gewahrt bleibe. Ich habe über diese Rechtsentwicklung bereits wiederholt berichtet (vgl. 18. JB, Ziff. 7.2.; 19. JB, Ziff. 11.1.2).

Die Regelungen des Bundes und Bremens (Gesetz über das Krebsregister der Freien Hansestadt Bremen, BremKRG, vom 18. September 1997, Brem.GBl. S. 337) stimmen darin überein, daß die Daten, deren Meldung von den Ärzten erwartet wird, aufgeteilt werden in Identitätsdaten (personenbezogene Daten ohne medizinische Aussagen) und in epidemiologische Daten (medizinische Daten ohne Personenbezug). Das Register wird von der Vertrauensstelle und der Registerstelle geführt, beide sind voneinander personell und organisatorisch getrennt. Die Vertrauensstelle nimmt die Meldungen der Ärzte entgegen, prüft sie auf Schlüssigkeit und Vollständigkeit und übermittelt die epidemiologischen Daten an die Registerstelle. Die Registerstelle wertet die registrierten Daten aus und hält sie vor für die bundesweite Auswertung durch das Robert-Koch-Institut oder für Forschungsprojekte. Darüber hinaus ist es Aufgabe der Vertrauensstelle, den Personenbezug der epidemiologischen Daten wiederherzustellen, soweit dies für Forschungsprojekte erforderlich ist und die einzelnen Betroffenen eingewilligt haben. Diese Aufteilung soll sicherstellen, daß in die Persönlichkeitsrechte der Krebspatienten nur soweit unbedingt erforderlich eingegriffen wird.

14.1.2 Besonderheiten im Landesgesetz

Das BremKRG weicht aber in wichtigen Regelungen von den Vorgaben des Bundesgesetzes ab. Auf meine Vorschläge hin hat man den hierdurch bedingten Abbau von Datenschutzgarantien an anderer Stelle des Gesetzes zu kompensieren versucht. Während des dem Gesetzesbeschluß vorangegangenen Abstimmungsprozesses habe ich mich mit Rücksicht darauf den vom Gesundheitsressort für die Abweichungen vorgebrachten Gründen nicht verschließen können. Ich sehe es aber als meine Aufgabe an, Aufbau und Betrieb des Bremischen Krebsregisters besonders sorgfältig zu begleiten und notfalls auf eine Korrektur des Gesetzes zu dringen.

Hinzukommt, daß eine Durchführungsverordnung mit den Aufgaben der Vertrauensstelle und der Registerstelle Institutionen beauftragt hat, die bereits andere Aufgaben der gesundheitlichen Versorgung bzw. Forschung wahrnehmen, so daß auch deshalb geboten ist, auf Vorkehrungen zur Gewährleistung der gesetzlichen Zweckbindungen bei der Verarbeitung der an das Register gemeldeten Daten besonderen Wert zu legen.

14.1.3 Kleinräumige Auswertungen der Registerdaten

Im Lande Bremen sollen zusätzlich zum Katalog des Bundes für den medizinischen Datensatz epidemiologisch notwendige Angaben zum Wohnsitz gemeldet werden (§ 3 lit.b Nr.3 BremKRG). Damit will man kleinräumige Forschungen ermöglichen, um örtliche krebsverursachende Faktoren (etwa Luftverschmutzung durch Straßenverkehr oder Elektrosmog) identifizieren zu können. Es darf aber nicht möglich sein, anhand dieser Angaben die Identität derjenigen Person zu ermitteln, deren Wohnsitz näher bestimmt wird. Deshalb schreibt das BremKRG fest, daß aufgrund der Angaben jedoch nicht die Anschrift feststellbar sein darf. Erst die Kenntnis der genauen Ausgestaltung des Datensatzes und seiner Auswertungsverfahren wird es mir gestatten, die Einhaltung dieser Garantie zu überprüfen.

14.1.4 Krebsregister und Tumornachsorgeleitstelle bei Kassenärztlicher Vereinigung

Durch Rechtsverordnung ist die Trägerschaft der Vertrauensstelle der Kassenärztlichen Vereinigung Bremen (KV) übertragen worden. Diese hat originär Aufgaben nach dem SGB V im Rahmen der vertragsärztlichen Versorgung wahrzunehmen, z. B Zulassungsverfahren, Abrechnung und Wirtschaftlichkeitsprüfung. Die Datenverarbeitungssysteme für die Aufgaben nach SGB V und der Vertrauensstelle müssen räumlich, technisch, organisatorisch und personell völlig voneinander abgeschottet sein.

Darüber hinaus hat die KV jüngst von der Bremer Krebsgesellschaft die Bremer Tumordokumentations-/Nachsorgeleitstelle (vgl. hierzu 13. JB, Ziff. 2.6.4.) übernommen. An diese Stelle melden seit sieben Jahren Bremer Ärzte mit deren Einwilligung Daten ihrer Krebspatienten zum Zwecke der Verbesserung ihrer Behandlung und Nachsorge. Auch insoweit ist Abschottung geboten. Dies gilt umsomehr, als man aus Gründen der Praktikabilität und zur Kostenreduzierung die Meldewege zum Register und zur Tumordokumentations-/Nachsorgeleitstelle zusammenfassen will. Hier ist sicherzustellen, daß die unterschiedlichen Meldevoraussetzungen (Register: Patient darf nicht widersprechen/andere Stelle: Pa-

tient muß einwilligen), die unterschiedlichen Meldezwecke (hier Forschung, dort Behandlung und Nachsorge) sowie die daraus resultierenden Unterschiede der jeweiligen Datensätze und der vorgesehenen Nutzungszwecke sich in unterschiedlichen Meldebögen und deren eindeutiger Zuordnung zu ihrem jeweiligen Bestimmungsort (Register oder andere Stelle) niederschlagen.

14.1.5 Speicherung der Identitätsdaten durch Vertrauensstelle auf Dauer

Nach dem Bundesmodell soll die Vertrauensstelle nach Überprüfung der Meldebögen und Weiterleitung der epidemiologischen Daten an die Registerstelle die bei ihr verbliebenen Identitätsdaten nicht etwa auf Dauer speichern, sondern unverzüglich löschen (§ 4 Abs. 1 Nr. 5 und § 7 KRG). Die Nutzung personenbezogener epidemiologischer Daten zu Forschungszwecken soll dadurch möglich bleiben, daß die Vertrauensstelle die Identitätsdaten nach einem bestimmten Verfahren verschlüsselt (asymmetrische Verschlüsselung) und der Registerstelle diesen Datensatz ebenfalls übermittelt (§ 4 Abs. 1 Nrn. 4, 5 und § 6 Abs. 1 Nr. 1, Abs. 2 KRG). Den Personenbezug der epidemiologischen Daten kann nur die Vertrauensstelle anhand der ihr von der Registerstelle zurückübermittelten verschlüsselten Identitätsdaten und mithilfe des Schlüssels herstellen, der bei einer dritten Stelle aufzubewahren ist (§ 4 Abs. 1 Nr. 6 und § 8 Abs. 5 KRG). Vor der Übermittlung der auf diese Weise deanonymisierten Daten an ein Forschungsinstitut sind eine behördliche Genehmigung und die Einwilligung der einzelnen betroffenen Person einzuholen (§ 7 Abs. 1,2 KRG).

Das BremKRG verzichtet in Folge von Zweifeln an dessen Praktikabilität weitgehend auf dieses Verschlüsselungsverfahren und sieht vor, daß die Vertrauensstelle die Identitätsdaten auf Dauer, d. h. bis zum Ablauf von 50 Jahren nach dem Tod oder von 130 Jahren nach der Geburt des Betroffenen, speichert und so zum Ausschluß von Doppelmeldungen, zum Zwecke der personenbezogenen Nutzung der epidemiologischen Daten für die Forschung und für Auskünfte an die Betroffenen vorhält (§ 4 Abs.1, 5 BremKRG). Ich will nicht verhehlen, daß mir diese Regelung erhebliches Kopfzerbrechen verursacht. Ich habe mich letztendlich den fachlichen Erwägungen der verantwortlichen bremischen Stellen nicht verschlossen, nachdem § 4 Abs. 1 BremKRG die aufgeführten Zwecke als „ausschließliche" bezeichnet und § 6 Abs. 2 BremKRG die Vertrauensstelle verpflichtet hat, im Rahmen der gesetzlich ohnehin gebotenen Datensicherungsvorkehrungen sicherzustellen, daß die Identitätsdaten nicht unbefugt eingesehen und nur zu den erlaubten Zwecken verarbeitet werden können. Umsomehr liegt es mir am Herzen, die Umsetzung dieser Gebote aufmerksam zu begleiten.

14.1.6 Registerstelle beim Bremer Institut für Präventionsforschung und Sozialmedizin (BIPS)

Durch Rechtsverordnung ist das BIPS damit beauftragt worden, die Registerstelle zu betreiben. Dies ist plausibel, verfügt dieses Forschungsinstitut doch über langjähriges know how in der Verarbeitung hochsensibler medizinischer Patientendaten unter Entwicklung und Beachtung von Vorkehrungen zur Gewährleistung der Persönlichkeitsrechte der Betroffenen. Zugleich aber ist nicht von der Hand zu weisen, daß gerade das BIPS gehalten ist, besonders penibel darauf zu achten, daß es seine Rollen als Träger der Registerstelle und als Forschungsinstitut sauber trennt. So darf der Personenbezug der in anonymisierter Form registrierten epidemiologischen Daten nicht mithilfe von Zusatzwissen aus anderen Projekten doch wieder hergestellt werden, auch nicht anhand der Angaben zum Wohnsitz (vgl. o. Ziff. 14.1.3.). Dies ist durch technische und organisatorische Vorkehrungen zu gewährleisten (zu den entsprechenden Anforderungen an die KV vgl. o. Ziff. 14.1.4.).

14.1.7 Umsetzungen der Datenschutzgebote des BremKRG

Das Gesetz ist am 1. Oktober 1997 in Kraft getreten. KV und BIPS sind mit Wirkung vom 4. Dezember 1997 mit den Aufgaben der Vertrauens- bzw. Registerstelle betraut worden. Laut Bericht des WESER-KURIER vom 16. Januar 1998 hat die zuständige Senatorin erklärt, rückwirkend ab 1. Januar 1998 sollten die vorgesehenen Daten registriert werden. Ich hatte bereits am 23. September 1997 die Geschäftsführer der beiden Träger darauf hingewiesen, daß rechtzeitig, d . h. vor Anfang 1998, die gebotenen Datenschutzkonzepte mir zur datenschutzrechtlichen Bewertung vorliegen müßten. Mit Schreiben vom 21. Januar 1998 habe ich die Verantwortlichen daran erinnert. Zwar ist inzwischen die Vergütung der

zum Register meldenden Ärzte geregelt, es sind aber noch nicht die Vorkehrungen zum Schutz der Persönlichkeitsrechte der betroffenen Krebskranken erarbeitet worden. Auf keinen Fall dürfen Meldungen entgegengenommen oder deren Inhalte ins Krebsregister übernommen werden, solange nicht sichergestellt ist, daß Zweckbegrenzungen und Datensicherheit gewährleistet sind.

14.2 Voreilige Aufregung über „Todescomputer"

Anfang 1997 wurde in den Medien darüber berichtet, daß in drei deutschen Krankenhäusern, darunter auch in der Intensivstation des Zentralkrankenhauses Links der Weser in Bremen, erstmals ein Computerprogramm „Riyadh-ICU" getestet werden solle, das über Leben und Tod eines Patienten auf der Intensivstation mitentscheide. Deshalb war auch von „Todescomputern" die Rede.

Daß diese Formulierung für den Einsatz des Programms im Zentralkrankenhaus Links der Weser nicht zutrifft, hat sich im Laufe einer datenschutzrechtlichen Überprüfung herausgestellt. Richtig ist, daß das Programm Riyadh in der Intensivmedizin nur zur Qualitätssicherung genutzt werden soll.

Bei einem durch die Berichterstattung in den Medien veranlaßten Prüfbesuch wurde mir das Programm vorgeführt. Dabei habe ich mich davon überzeugen können, daß im Zentralkrankenhaus Links der Weser die durch das Programm erhobenen und gespeicherten Patientendaten nur für eine vierteljährliche und interne statistische Auswertung zur Qualitätssicherung genutzt werden.

Ein Rückgriff auf die Krankenakten einzelner Patienten ist allerdings über die im Programm gespeicherte Aufnahmenummer möglich. Allerdings wurde versichert, daß dies erst im Nachhinein in Einzelfällen zur Überprüfung extremer Abweichungen aus dem Normbereich bei der statistischen Auswertung vorgesehen ist.

Nachdem auch das Datenschutzkonzept um noch fehlende Punkte ergänzt wurde, bestanden aus meiner Sicht nunmehr keine Bedenken gegen den Einsatz von Riyadh in dem uns dargestellten Umfang. Ähnlich begründet übrigens auch die Ethik-Kommission der Ärztekammer Bremen ihren Beschluß, keine Einwände gegen den Einsatz von Riyadh im Zentralkrankenhaus Links der Weser zu erheben.

Sollte Riyadh für Entscheidungen im Rahmen der Behandlung einzelner Patienten genutzt werden, müßte das Programm datenschutzrechtlich, aber sicher auch aus Sicht der Ethik-Kommission, völlig neu beurteilt werden.

14.3 Übergabe der Arztpraxis an einen Nachfolger — wie wird die Schweigepflicht gewahrt?

Einen großen Teil des materiellen Wertes einer Arzt- oder Zahnarztpraxis macht der Patientenstamm aus einschließlich der Aufzeichnungen und Dokumente, die der Arzt oder Zahnarzt zu seinen einzelnen Patienten in Erfüllung seiner Dokumentationspflicht aufbewahrt hat. Deshalb werden diese Unterlagen regelmäßig zusammen mit der Praxis an den übernehmenden Arzt verkauft. Dies geschah lange Zeit, ohne daß gefragt worden wäre, ob denn auch jeder Patient damit einverstanden sei.

Der Bundesgerichtshof hat dies 1991 in einem Grundsatzurteil als Verletzung der ärztlichen Schweigepflicht bezeichnet und vom Arzt verlangt, daß er vor Übergabe der Unterlagen die Zustimmung des Patienten in eindeutiger und unmißverständlicher Weise einholt (vgl. zuletzt 16. JB, Ziff. 13.4). Seither hat sich dies zur ständigen Rechtsprechung verfestigt. Ebenso hat sich aber bundesweit die Absicht der Ärzte- und Zahnärztekammern verfestigt, die Regelungen zur Schweigepflicht bei Praxisaufgabe in den ärztlichen Berufsordnungen nicht an diesem eindeutigen und höchstrichterlichen Urteil auszurichten, sondern darauf zu beschränken, daß der Praxisnachfolger die ihm übergebenen Unterlagen unter Verschluß halten müsse und nur mit Einwilligung des Patienten, die auch durch Aufsuchen des Praxisnachfolgers erklärt werde, einsehen oder weitergeben dürfe. So lauten die Formulierungen in den Musterberufsordnungen der Bundesärzte- und der Bundeszahnärztekammer aus dem Jahr 1997 sowie in den gleichlautenden Beschlüssen der Mitgliederversammlungen der Bremischen Kammern.

Die Verantwortung soll also vom schweigepflichtigen Arzt auf seinen Nachfolger abgeschoben werden. Begründet wird dies damit, daß die Unterlagen beim Praxisnachfolger am besten aufgehoben seien, aber auch mit der z. T. großen Zahl der Patienten und den Schwierigkeiten, sie zwecks Einholung ihres Einverständnisses

zu erreichen. Dabei wird außer acht gelassen, daß die Zahl der Bürger wächst, die sich ihren Arzt bewußt aussuchen und das Vertrauen, das sie in den einen Arzt setzen, nicht jedem anderen Arzt gegenüber aufbringen.

Der Senator für Gesundheit hat sich deshalb bislang geweigert, die ihm von den Bremischen Kammern vorgelegten Berufsordnungen zu genehmigen. Er hat den Kammern vorgeschlagen, ihre Mitglieder wenigstens zu verpflichten, die Patienten, die nach Verkauf, aber vor Übergabe, die Praxis aufsuchen, mündlich und die Patienten, die im Verlauf der vergangenen zwei Jahre die Praxis aufgesucht haben, durch Anschreiben um ihre Einwilligung zu bitten. Für die Unterlagen der Patienten, die schon längere Zeit die Praxis nicht aufgesucht haben, und der Patienten, die sich nicht äußern, soll der o. a. Vorschlag der Kammern gelten.

Ich habe diesen Ansatz unterstützt, weil er sich an der Praktikabilität orientiert und deshalb für die Ärzteschaft akzeptabel sein sollte, aber gleichwohl das persönliche Vertrauensverhältnis zwischen Patient und Arzt ernst nimmt. Die Geschäftsführungen der Ärzte- und der Zahnärztekammer Bremen haben gleichwohl den Vorschlag des Senators für Gesundheit abgelehnt. Sollte dieser auf seiner Rechtsauffassung beharren, was ich begrüßen würde, so zeichnet sich ein Rechtsstreit über die Genehmigungsfähigkeit der Kammerbeschlüsse vor dem Verwaltungsgericht ab.

14.4 Kindertagesheim und Datenschutz — ein schwieriges Verhältnis?

14.4.1 Steuerbescheide als Grundlage der Berechnung der Beiträge?

14.4.1.1 Parallelproblematik in mehreren Verwaltungszweigen

Bereits in meinem 17. Jahresbericht für 1994 hatte ich unter Ziff.16.1 darüber zu berichten, daß immer wieder Behörden zur Festsetzung von Beiträgen und Gebühren die Vorlage eines kompletten Steuerbescheides verlangen, obwohl sie daraus nur einzelne Angaben wie z. B. die Höhe des positiven Einkommens benötigen. Hinzukommt, daß die Bescheide bzw. deren Kopien nach erfolgter Berechnung nicht etwa zurückgegeben, sondern zu den Akten genommen werden. In der Folgezeit beschäftigte diese Problematik mehrmals auch den Datenschutzausschuß der Bremischen Bürgerschaft. Auch er wollte dem behördlichen Sammeleifer vor allem bei der Ermittlung des Einkommens zur Berechnung des Kindertagesheimbeitrags, aber auch der Ausbildungsförderung und des Wohngeldes, Schranken setzen (vgl. den Bericht des Ausschusses zu meinem 17. JB, Drs. 14/210).

Nachdem die Vorschläge, die Finanzämter könnten doch zwecks Vorlage für die genannten Zwecke Teilausdrucke der Steuerbescheide zur Verfügung stellen, oder die Steuerbescheide sollten den Eltern nach Erhebung der erforderlichen Daten sogleich wieder zurückgegeben werden, beim Senator für Finanzen mit Blick auf zusätzliche Kosten bzw. die Anforderungen der Rechnungsprüfung auf wenig Gegenliebe stießen, schlug ich vor, die vorlagepflichtigen Eltern bzw. Mieter darüber zu informieren, welche Teile des Steuerbescheides sie schwärzen bzw. abtrennen und zurückbehalten dürfen.

Am wenigsten bewegt hat sich die BAföG-Verwaltung. Das zuständige Landesamt räumt zwar ein, daß nicht alle Daten in den Einkommenssteuerbescheiden der Eltern für die Berechnung der Ausbildungsförderung benötigt werden, beruft sich aber auf eine Verwaltungsvorschrift zum BAföG des Bundesministeriums für Bildung und Wissenschaft, die in der Tat von der Vorlage „des Steuerbescheids" spricht. Daraus schließt das Amt, was für mich nicht zwingend ist, der vollständige Bescheid sei gemeint. Ich werde die Gespräche für diesen Bereich fortsetzen.

Zur selben Problematik bei der Berechnung von Wohngeld wird auf den Abschnitt 17.3. in diesem Bericht verwiesen.

14.4.1.2 Sonderentwicklung bei den KTH-Beiträgen

Das Jugendressort dagegen beharrte lange darauf, man benötige die kompletten Steuerbescheide für die Berechnung der Kindertagesheimbeiträge (KTH-Beiträge). Im Juni 1997 entschied aber das Oberverwaltungsgericht Bremen, die in der Stadtgemeinde Bremen praktizierte, auf jeden Einzelfall bezogene soziale Differenzierung der Beitragshöhe widerspreche der Vorgabe des Bundesgesetzgebers, die Höhe der KTH-Beiträge pauschalisiert zu berechnen. Die Aufforderung des Gerichts, die bremischen Gesetze und Verordnungen zu überarbeiten, eröffneten auch dem Schutz der Elterndaten eine Chance, vor allem deshalb, weil das Gericht an den alten Regelungen kritisierte, sie hätten einen „intensiven Informationseingriff" zur Folge, der wohl bei der Sozialhilfe, aber nicht bei der Beitragsberechnung gerechtfertigt sei.

Daraufhin paßten zwar Bürgerschaft und Senat die rechtlichen Grundlagen an. Es hieß auch, man wolle nunmehr eine „Schwärzungsregelung" treffen; in der neuen Verwaltungsanweisung aber hieß es weiterhin ohne Einschränkungen, die Eltern müßten die Steuerbescheide vorlegen, wollten sie in den Genuß der sozialen Beitragsstaffelung kommen.

Nach erneuter Intervention des Datenschutzausschusses (vgl. o. Ziff. 10.2.1. a. E.) scheint das Eis gebrochen. Senator für Jugend und Amt für Soziale Dienste erarbeiten derzeit in Abstimmung mit mir neue Anweisungen und Formblätter mit der Zielsetzung, die Datenerhebung für die Beitragsberechnung auf das erforderliche Maß zu begrenzen. Bereits im Aufnahmeverfahren für das neue Kindergartenjahr 1998/1999 werden die Eltern in einem neugefaßten Informationsblatt erfahren, welche Daten benötigt werden und welche Teile der Steuerbescheide sie schwärzen oder abtrennen können (vgl. auch u. Ziff. 17.3.).

Im KTH selbst, dessen Leitung künftig die Beiträge berechnen wird, sollten, so war zunächst die Zusicherung des Ressorts, die Unterlagen nur bis zum Ablauf der Widerspruchsfrist verbleiben, dann aber in verschlossenen Umschlägen an die zuständige Regionalabteilung des Amtes für Soziale Dienste gehen, um dort archiviert zu werden. Damit wären Datensicherheit und Begrenzung der Nutzung für Beitragsberechnung einschließlich Rechnungsprüfung besser gewährleistet gewesen als bei einer Lagerung im KTH selbst.

Neuerdings heißt es, die Unterlagen müßten doch bis zum Beginn des nächsten Kindergartenjahres oder sogar, bis das betreffende Kind die Einrichtung verläßt, dort aufbewahrt werden. Dies wird damit begründet, daß die Heimleitungen die KTH-Beiträge nicht nur einmal zu berechnen hätten, sondern sie auch bei Einkommensänderungen neu zu berechnen und über Ermäßigungsanträge zu entscheiden hätten. Dies mag zwar plausibel sein, räumt aber die Befürchtungen wegen der längerfristigen Lagerung der Unterlagen in den Einrichtungen nicht aus. Obgleich die Einrichtungen aufgefordert wurden, für die sichere Aufbewahrung Sorge zu tragen, ist u. a. wegen ungelöster Finanzierungsfragen deshalb das Problem noch längst nicht gelöst. Notfalls — so habe ich gefordert — müssen die Unterlagen doch schon vorher an die Regionalabteilungen abgegeben werden. Zu begrüßen ist wiederum, daß sich der Rechnungshof damit einverstanden erklärt hat, daß die Unterlagen nur bis zum Ablauf von zwei Jahren — und nicht von fünf Jahren — nach Ende des KTH-Besuchs durch ein Kind aufzubewahren sind.

14.4.2 Kindergarteninformationssystem (KIS) ohne Datenschutz?

14.4.2.1 Neugestaltung der Erhebungsbögen

Bereits bei der Erörterung der Erhebungsbögen für das Aufnahmeverfahren 1998/1999 fiel auf, daß man auf ein und demselben Vordruck mehr Daten abfragen will, als für die Beitragsberechnung erforderlich sind. Vor allem gilt dies für Daten, die sich auf die sozialen Verhältnisse der Familien beziehen (Geschwister, Wohnungsgröße, Berufstätigkeit der Eltern). Früher wurden diese Daten zur Entscheidung herangezogen, ob bei Mangel an Kindergartenplätzen ein Kind aus sozialen Gründen vorrangig aufzunehmen sei. Seit Realisierung des Rechts jeden Kindes auf einen Kindergartenplatz können diese Daten nur noch für die Aufnahme im Hort erheblich sein, im übrigen allenfalls für statistische Zwecke und für die pädagogische Arbeit im Kindertagesheim selbst.

Ich habe deshalb vorgeschlagen, für das Aufnahmeverfahren selbst sowie für statistische und für pädagogische Zwecke unterschiedliche Erhebungsvordrucke zu verwenden, die die Eltern über den jeweiligen Erhebungszweck informieren sowie darüber, ob und wenn ja, aufgrund welcher Rechtsvorschrift sie zur Auskunft verpflichtet sind, oder ob die Auskunft freiwillig ist. Je nach Erhebungszweck ist dann unterschiedlich zu regeln, wer Zugriff auf die Bögen hat sowie wo und wie lange sie aufzubewahren sind.

14.4.2.2 PC ohne Datenschutzkonzept

Derzeit wird die Ausstattung aller KTH mit PC vorbereitet. Ziel ist es, auf ihnen mittels KIS Daten von Eltern und Kindern für die Aufnahme, die Beitragsberechnung, für statistische und für pädagogische Zwecke zu verarbeiten. Zuvor aber müssen die Konfiguration des vorgesehenen Betriebssystems Windows-NT und die Zugriffsstruktur der Datenbank gewährleisten, daß Datenkataloge, Zugriffsberechtigungen und Löschungsfristen die oben dargestellten rechtlich gebotenen Nutzungsbegrenzungen umsetzen. Trotz meiner wiederholten Aufforderung,

zuletzt Mitte Februar 1998, hat der Senator für Jugend bis heute kein Datenschutzkonzept vorgelegt. Dies ist um so befremdlicher, als KIS in einigen KTH bereits mit Echtdaten im Probebetrieb läuft und freien Trägern zum Einsatz in ihren KTH angeboten und dort auch eingesetzt wird.

Ich kann den Hinweis des Ressorts auf angeblich vordringlichere Arbeiten der ADV-Abteilung als Rechtfertigung nicht akzeptieren. Rechtlich gebotene Konsequenz ist es vielmehr in dieser Situation, die Inbetriebnahme des Systems so lange zu verschieben, bis die personellen Ressourcen für die Erarbeitung des Datenschutzkonzepts zur Verfügung stehen.

14.5 ZKH Bremen-Ost — Datenschutz als Geduldsprobe

Daß die Realisierung eines der Sensibilität von Patientendaten angemessenen Datenschutzniveaus in Krankenhäusern eine langwierige Angelegenheit sein kann, aber auch, daß ich in solchen Fällen nicht locker lasse, zeigt das Beispiel des ZKH Bremen-Ost.

Im Jahr 1995 überprüfte ich die Umsetzung einiger datenschutzrechtlicher Forderungen, die sich u. a. aus dem Ergebnis eines Kontrollbesuchs im Jahr 1993 (dazu 16. JB., Ziff. 8.4.1.3) ergeben hatten (vgl. 18. JB, Ziff. 15.4.3.). Neben einigen Verbesserungen waren erhebliche Mängel bestehen geblieben. Aufgrund der von seiten des Krankenhauses geplanten umfassenden Veränderungen im EDV-Bereich im Zusammenhang mit der Erstellung eines neuen Organisationskonzepts sah ich von einer Beanstandung gem. § 29 BrDSG ab und verlangte von der Verwaltungsleitung eine Beseitigung der festgestellten Mängel.

Als schriftliche Dokumentation hierfür sollte mir ein alle Anwendungsbereiche des Hauses umfassendes Datenschutzkonzept vorgelegt werden, wofür ich eine Fristverlängerung bis zum Ende des letzten Berichtsjahres einräumte (vgl. 19. JB, Ziff. 11.2.).

Mein in diesem Berichtsjahr auf der Grundlage des dann fristgemäß erhaltenen Konzeptes durchgeführter Prüfbesuch führte zu dem Ergebnis, daß Verbesserungen in den Bereichen Eigenentwicklung, Funktionstrennung und Transparenz/Kontrolle der Systemverwaltung vorgenommen worden sind.

Problematisch bleibt das weiterhin genutzte Verfahren zur Verwaltung und Abrechnung stationärer Patientenaufenthalte. Es ermöglicht keinen differenzierten Zugriff durch unterschiedliche Fachbereiche, d. h. die später eingegebenen Archivdaten sind für den Anmeldebereich (Folgediagnosen etc.) abrufbar, ohne daß hierfür eine Erforderlichkeit gegeben ist. In diesem Verfahren gibt es auch keine Protokollierung.

Im Herbst 1998 soll ein neues Verfahren zur stationären Patientenverwaltung eingesetzt werden. Aufgrund der dazu von seiten des Krankenhauses gegebenen Informationen gehe ich davon aus, daß das zukünftige Verfahren die erforderlichen Features zur Realisierung des angemessenen technischen Datenschutzes enthalten wird. Im Hinblick darauf werde ich das aktuelle Verfahren nicht (mehr) beanstanden. In dem neuen Verfahren sollte im Rahmen der Dokumentation bzw. Protokollierung die Transparenz der Systemverwaltung durch eine Reihe von Maßnahmen, die ich im einzelnen benannt habe, nachhaltig erhöht werden. Grundsätzlich sollten in jedem Fall alle datenschutzrelevanten Aktivitäten im Rahmen der Netzadministration, Benutzerverwaltung, Konfigurationsänderungen usw. protokolliert werden.

Der Datenschutzbeauftragte des Krankenhauses sollte, wie bereits in der Stellungnahme des Senats zum 18. Jahresbericht zugesagt, routinemäßig anhand von definierten Verfahren bzw. Abläufen eingeschaltet werden. Dies gilt auch für die Bearbeitung von externen Anfragen durch Forschungseinrichtungen.

14.6 PROSOZ-Bremen — die Nachbesserung der Nachbesserung

Im November 1994, also vor mehr als drei Jahren, wurde mir ein neues Datenschutzkonzept für das dialogorientierte Sozialhilfeberechnungsverfahren PROSOZ vorgelegt, das eine Anpassung der Konzeption an die Weiterentwicklung und Erweiterung des Systems darstellte.

Eine von mir daraufhin durchgeführte Prüfung ergab,

— daß durch die Integration von Textverarbeitungsfunktionen neue Kontrollücken entstanden waren, die neue Datenschutzmaßnahmen erforderten, und

— daß sich das laufende Verfahren und das mir zugeleitete Konzept bereits ohne Erweiterungen durch Textverarbeitungsfunktionen in einigen Punkten nicht deckten.

Eine diesen Anforderungen angepaßte ergänzte Datenschutzkonzeption habe ich dann 1995 hinsichtlich ausgewählter Schwerpunkte auf ihre praktische Umsetzung hin überprüft. Als Ergebnis habe ich die Umsetzung nur einiger weniger der von mir geforderten und im Datenschutzkonzept vom Sozialressort selbst festgelegten (!) Maßnahmen (wie z. B. Verhinderung der Einsichtnahme von Paßworten) festgestellt. Ein Großteil der ausgehandelten Maßnahmen, was bereits Ergebnis eines Kompromisses zwischen mir und der senatorischen Dienststelle war (vgl. 17.JB Ziff. 12.3.1.2), war nicht umgesetzt worden.

Daran änderte sich auch im folgenden Berichtsjahr nichts (vgl. 19. JB. Ziff. 11.5). Die daraufhin erforderlich gewordene erneute datenschutzrechtliche Bestandsaufnahme legte dann einen Datenschutzverstoß offen, nämlich die Abschaltung der bei ID-Bremen zu führenden Protokollierung. Diese wurde auf meine Intervention hin wieder aktiviert; ein von mir zur Prüfung angeforderter Protokollausdruck über gespeicherte Änderungen, Neufälle und Abgänge in der ADV-Verbindungsstelle für den Zeitraum vom 7. bis 11. April 1997 wurde mir übergeben. Von einer Beanstandung gem. § 29 Abs. 2 BrDSG konnte ich daher absehen.

Für das Jahr 1998 wird in der Stellungnahme des Senats zu meinem 19. Jahresbericht der Einsatz eines Tools „Quick Lock für Windows" zur Aktivierung der Bildschirmdunkelschaltung angekündigt. Damit wird die Einsicht im Raum anwesender unbefugter Dritter (z. B. Besucher) verhindert. Diese Funktion (damals noch geplant durch Aktivierung des Bildschirmschoners unter MS-Windows) war bereits 1994 (!) Bestandteil des Konzepts.

Einige Maßnahmen des ursprünglichen Konzeptes wie z. B. Sperrung von Diskettenlaufwerken an den Arbeitsplätzen der Dienststellenkoordinatoren/-innen, stichprobenartige Kontrollen durch den Datenschutzbeauftragten der senatorischen Dienststelle und Sperrung der Speicherfunktion für die ADV-Verbindungsstelle, so daß von dort aus keine Veränderungen in den Datensätzen der Falldatenbank vorgenommen werden können, wurden bis zum Redaktionsschluß nicht realisiert.

Am Verlauf der Entwicklung des PROSOZ-Verfahrens wird das grundsätzliche Problem der datenschutztechnischen Absicherung eines nachgebesserten Verfahrens deutlich:

Zwar bestand kein Dissens zwischen mir und der senatorischen Dienststelle hinsichtlich der Notwendigkeit zusätzlicher technischer und organisatorischer Datenschutzmaßnahmen. Dennoch verhinderten „Verfahrenszwänge", angebliche Plausibilitätsgründe und insbesondere der zu erwartende Aufwand eine vollständige Umsetzung des Datenschutzkonzeptes.

Meine anfängliche These, daß der einmal erreichte Datenschutzstandard bei einer Erweiterung und Öffnung des Systems durch nachträgliche Maßnahmen und technische Restriktionen nicht gehalten werden kann, wurde im Verlauf dieses Verfahrens bestätigt.

Verzögerungen und Verschleppungen über einen so langen Zeitraum und bei derart sensiblen Daten sind nicht akzeptabel. Ich werde daher bei der Einführung eines neuen Verfahrens nicht mehr akzeptieren, daß Korrekturen an der Datensicherheit nachträglich und unzureichend realisiert werden. Erforderliche technische Maßnahmen müssen weitgehend in das Fachverfahren selbst (d. h. größtmöglicher Datenschutz auf Applikationsebene) integriert werden.

14.7 Sozialpsychiatrischer Dienst — Keine umfassende Automation ohne Rechtsverordnung

Als sozialpsychiatrische Institutsambulanz muß der sozialpsychiatrische Dienst des Gesundheitsamtes Bremen Abrechnungsunterlagen bei den Krankenkassen edv-gerecht einreichen. In diesem Zusammenhang wurde ein Standardprogramm mit umfassenden Datenverarbeitungsfunktionen beschafft (vgl. 18. JB, Ziff. 15.3.3.; 19. JB, Ziff. 11.4.).

Die datenschutzgerechte Nutzung dieses Funktionsumfanges (Verarbeitung von Diagnosen, Arztberichten, Rehabilitationsgesamtplänen, Gutachten etc.) setzt die Vereinbarkeit mit dem ÖGDG (Bremisches Gesetz über den öffentlichen Gesund-

heitsdienst, insb. §§ 31-33) und der zu erlassenden Rechtsverordnung (§ 33 Abs.3 ÖGDG) hinsichtlich Umfang, Dauer und zugelassener Zwecke von Erhebung und Speicherung von Patientendaten voraus.

Nach Vorlage der Rechtsverordnung sollte eine Entwicklungsfirma beauftragt werden, den Funktionsumfang des Programms entsprechend anzupassen. Da eine nur auf die zulässige Abrechnungsfunktion beschränkte Nutzung des Systems technisch und/oder organisatorisch nicht zu gewährleisten war, konnte es nicht zur Anwendung kommen.

Im Berichtsjahr wurde die Rechtsverordnung nicht erlassen; ein Auftrag durch den sozialpsychiatrischen Dienst an die Entwicklungsfirma zur Anpassung der Standardsoftware konnte deshalb nicht erfolgen. Gleichzeitig verstärkte sich der (Kosten-) Druck zur Einführung einer edv-gerechten Abrechnung.

Ich habe daher ein Datenschutzkonzept des Gesundheitsamtes Bremen, das eine Übergangslösung beschreibt, mit einigen zusätzlichen Anforderungen meinerseits akzeptiert. Grundlage hierfür ist insbesondere die Nutzung des Sicherheitssystems des Betriebssystems WindowsNT und die organisatorische strikte Begrenzung der Datenerfassung auf die Erforderlichkeit für die Abrechnung.

Unabdingbar für einen datenschutzgerechten Einsatz des Verfahrens wird die Abbildung der konzeptionell festgelegten Sicherheitsfeatures auf die entsprechende technische Konfiguration sein. Erst dann ist das Verfahren datenschutzrechtlich verwendbar.

Selbst bei Erfüllung der o. g. Voraussetzungen ist die Übergangslösung — trotz umfassender nachträglicher Einschränkungen eines multifunktionalen Standardsystems zur computerunterstützten Praxisführung — die datenschutzrechtlich schwächere Lösung.

Im Datenschutzausschuß vom 18. November 1997 hat das Ressort eine mit mir abgestimmte Vorlage der Rechtsverordnung bis zur Sommerpause 1998 zugesagt (vgl. den Ausschußbericht o. Ziff. 10.2.1.). Sobald sie in Kraft getreten ist, ist das Softwareprodukt hinsichtlich seiner Funktionalitäten anzupassen.

14.8 Werkstatt Bremen — Personalinformationssystem mit Mängeln

Anfang 1996 hat mich die Werkstatt Bremen über die geplante Einführung eines Personalinformationssystems unterrichtet. In diesem System werden Daten von zwei unterschiedlichen Personenkreisen verarbeitet: Grundlage für die Verarbeitung der Daten von Mitarbeitern ist das Bremische Datenschutzgesetz (§ 22 BrDSG). Die Datenverarbeitung der sog. „Beschäftigten" basiert auf Vorschriften des Sozialgesetzbuches und des Schwerbehindertengesetzes.

Bei einer durch den Hersteller in der Werkstatt Bremen mit meiner Beteiligung erfolgten Systemvorführung definierte ich eine Reihe datenschutztechnischer Anforderungen:

So erfordern die unterschiedlichen Rechtsgrundlagen für die Personaldatenverarbeitung die Vergabe von Zugriffsrechten auf definierbare Teile des Gesamtdatenbestandes (Mandantentrennung). Zur Gewährleistung der Zweckbindung sowie zur Vermeidung unzulässiger Leistungs- und Verhaltenskontrollen ist eine feste Definition der Inhalte der Freitextfelder oder eine Eingabesperre für diese Felder erforderlich. Auswertungen personenbezogener Daten sind im Datenschutzkonzept verbindlich zu definieren (Zweckbindung, Transparenz); dies betrifft insbesondere langfristige Erkrankungen, die Fehlzeitenliste und den Listgenerator. Sowohl für die Administration des Novell-Netzes (als Systemumgebung für das Fachverfahren) als auch für diejenige des Fachverfahrens sind Systemverwalter/-innen zu benennen. Sowohl die Tätigkeiten der Systemverwaltung als auch die der Anwendung sind zu protokollieren. Und schließlich: Da das System keine automatische Löschfunktion bietet, ist die Löschung der Daten organisatorisch zu regeln (Löschverfahren, Fristen, etc.).

Die Umsetzung der o. g. Maßnahmen wurde von der Werkstatt Bremen zugesagt und in ihrem daraufhin erstellten Datenschutzkonzept festgeschrieben. Bei meiner auf die Umsetzung dieser Maßnahmen abzielenden Datenschutzprüfung mußte ich jedoch feststellen, daß bis auf die Eingabesperre für Freitextfelder keine der Vorkehrungen realisiert worden war.

Die Werkstatt Bremen hat kurz vor Redaktionsschluß im Februar 1998 zu meinem Prüfbericht von November 1997 Stellung genommen. Die Stellungnahme enthält umfangreiche Maßnahmen, die zur Mängelbeseitigung geeignet erscheinen. Eine Bewertung dieser Maßnahmen konnte bis Redaktionsschluß noch nicht vorgenommen werden.

14.9 „Verbesserter Datenaustausch bei Sozialleistungen" heißt Abbau des Sozialdatenschutzes

14.9.1 Wichtige Stationen der Rechtsentwicklung

14.9.1.1 Ausgangspunkt Volkszählungsurteil

Als das Bundesverfassungsgericht in 1983 in seinem Volkszählungsurteil zum Schutz des Grundrechts des Einzelnen auf informationelle Selbstbestimmung

- den Gesetzgeber aufforderte, den Verwendungszweck von zwangsweise zum Verwaltungsvollzug erhobenen Daten bereichsspezifisch und präzise zu bestimmen,
- forderte, daß die Angaben für diesen Zweck geeignet und erforderlich zu sein hätten,
- die Verwendung der Daten auf den gesetzlich bestimmten Schutz begrenzt sehen wollte und
- einen amtshilfefesten Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote forderte,

erklärte es zugleich, daß die seinerzeit geltenden Regelungen zum Schutz des Sozialgeheimnisses in die verfassungsrechtlich gebotene Richtung wiesen. Inzwischen ist die Entwicklung des Rechts der Datenverarbeitung durch Sozialleistungsträger jedoch in eine Richtung gegangen, die mit der erklärten Zielsetzung des höchsten Verfassungsgerichts zunehmend weniger zu vereinbaren ist.

14.9.1.2 Sozialgesetzbuch X

Bereits die seinerzeit umstrittene Neufassung der Vorschriften zum Schutz des Sozialgeheimnisses durch das 2. SGB-Änderungsgesetz in 1993 (vgl. dazu mein 16. JB, Ziff. 8.2) eröffnete der Verwendung einmal zu einem bestimmten Zweck erhobener Sozialdaten zu anderen Zwecken sowohl durch denselben als auch durch einen anderen Sozialleistungsträger Tür und Tor, stellte aber noch nicht die Prämisse in Frage, daß die jeweilige Verwendung im Einzelfall erforderlich sein müsse. Vor allem aber wurde mit § 67 a SGB X ein abgestuftes Datenerhebungsinstrumentarium beereitgestellt, wonach in sinnvoller Ergänzung zu den Mitwirkungspflichten des Leistungsempfängers bzw. Antragstellers nach §§ 60-66 SGB I der Sozialleistungsträger zunächst gehalten ist, die für seine Aufgabenerfüllung erheblichen Daten unter Mitwirkung des Betroffenen zu erheben und ihn erst in zweiter Linie befugt, bei Vorliegen bestimmter Voraussetzungen im Einzelfall am Betroffenen vorbei andere Stellen um Auskunft anzugehen und sich hierbei ggf. auf deren gesetzliche Auskunftspflicht (etwa nach §§ 20 Abs. 4, 98, 99 SGB X, 116, 117 Abs. 3 BSHG) zu berufen.

14.9.1.3 Sozialhilferecht

Gleichfalls in 1993 schuf der Bundesgesetzgeber in § 117 BSHG die Grundlage für automatisierte Datenabgleiche von Sozialhilfeträgern untereinander und mit anderen Sozialleistungsträgern (vgl. hierzu 16. JB, Ziff. 8.1). Die für die Schaffung der organisatorischen und technischen Voraussetzungen erforderliche Rechtsverordnung ist inzwischen erlassen worden. Bei der zentralen Datenstelle der Rentenversicherungsträger können zwecks Abgleich Daten von Leistungsbeziehern aller deutschen Sozialämter, Arbeitsämter, Rentenversicherungsanstalten und Berufsgenossenschaften zusammenlaufen, vorübergehend gespeichert und abgeglichen werden. Das Ergebnis soll an die anfragenden Sozialhilfeträger zurückgemeldet werden.

Diese umfassenden Datenabgleiche sind nicht mehr auf begründete Einzelfälle bezogen, sondern werden routinemäßig durchgeführt. Ihr Ziel ist nicht eine bürgerfreundliche Verwaltungsvereinfachung, erfordern sie doch im Gegenteil einen erheblichen zusätzlichen Aufwand, sondern erklärtes Ziel ist ausschließlich die Bekämpfung mißbräuchlicher Inanspruchnahme von Sozialhilfe. Immerhin wurde von Datenschutzseite aus durchgesetzt, daß sowohl die gesetzliche Regelung als

auch die Verordnung Beschränkungen der Datenmenge, Nutzungsbeschränkungen und Löschungsgebote vorsehen. Deren Beachtung in der Praxis der Datenabgleiche zu kontrollieren, wird eine wichtige Aufgabe der Datenschutzbeauftragten sein.

Im Jahr 1996 wurde durch eine Ergänzung des § 117 Abs. 3 BSHG, der bis dahin nur Anfragen im Einzelfall legitimierte (vgl. 16. JB, Ziff. 8.1.2, 2. Absatz), auch der automatisierte Datenabgleich der Sozialämter mit anderen kommunalen Stellen wie z. B. der Kfz-Zulassungsstelle und den Stadtwerken legalisiert.

14.9.1.4 Recht der Arbeitsförderung

Zum 1. Januar 1998 ist mit dem Arbeitsförderungs-Reformgesetz das SGB III in Kraft getreten (BGBl. 1997 S. 590). § 315 SGB III legt u. a. eine allgemeine Auskunftspflicht gegenüber den Arbeitsämtern für die Stellen fest, die für einen Leistungsbezieher ein Guthaben führen. Damit werden über die bislang geltenden Vorschriften über Auskunftspflichten von Unterhaltspflichtigen, Arbeitgebern, Finanzämtern und kommunalen Stellen nach §§ 20 Abs. 4, 98, 99 SGB X, nach § 116 BSHG (bzw. anderen Leistungsgesetzen) und nach § 117 Abs. 3 BSHG hinaus erstmals auch die Kreditinstitute unter Aufhebung des Bankgeheimnisses auskunftspflichtig. Damit geht einher die zunehmende Tendenz, entgegen der geltenden Rechtslage (§§ 60-66 SGB I und § 67 a SGB X) aus dem Bestehen einer Auskunftspflicht zu schließen, der Sozialleistungsträger brauche dann von vornherein nicht zu versuchen, die Angaben vom Betroffenen selbst zu erfragen oder bei ihm die Zustimmung zur Auskunftseinholung beim Auskunftspflichtigen einzuholen. Die Gesetzessystematik dagegen unterscheidet eindeutig zwischen der Befugnis des Leistungsträgers zur Datenerhebung ohne Mitwirkung des Betroffenen und Auskunftspflichten Dritter.

14.9.2 Die Initiative der Arbeits- und Sozialministerkonferenz

In 1996 und 1997 erarbeitete im Auftrag der Arbeits- und Sozialministerkonferenz (ASMK) eine Arbeitsgruppe unter Federführung des Bayerischen Arbeits- und Sozialministeriums den Bericht „Verbesserter Datenaustausch bei Sozialleistungen". Im Oktober 1997 legte diese Arbeitsgruppe den Bericht der ASMK vor mit einer Fülle von Vorschlägen für über den bisherigen gesetzlichen Rahmen hinausgehende Auskunftspflichten Dritter, verknüpft mit Befugnissen der Sozialleistungsträger zur Erhebung von Sozialdaten ohne Mitwirkung der Betroffenen.

Nach diesen Überlegungen sollen die Informationen, sei es bei anderen Sozialleistungsträgern, sei es bei anderen öffentlichen oder privaten Stellen, i. d. R. ohne Mitwirkung, sogar ohne Wissen des Betroffenen und anlaßunabhängig per automatisiertem Datenabgleich, d. h. nicht nur in begründeten Einzelfällen beschafft werden.

14.9.3 Die Reaktionen der Datenschutzbeauftragten und der ASMK

Demgegenüber beharrten die Datenschutzbeauftragten darauf, das Sozialgeheimnis und das Gebot der Verhältnismäßigkeit staatlicher Eingriffe in Bürgerrechte verlangten von Sozialämtern und Sozialversicherungsanstalten nach wie vor, daß ihre Verarbeitung von Sozialdaten gegenüber den Leistungsempfängern transparent bleibe und daß das derzeit ihnen vorgeschriebene differenzierte, grundrechtskonforme Verfahren der Datenerhebung

- beim Betroffenen selbst,
- bei Dritten nur unter Mitwirkung des Betroffenen sowie
- bei Dritten ohne dessen Mitwirkung nur aus konkretem Anlaß

beibehalten werde.

Datenerhebungen, insbesondere automatisierte Datenabgleiche, bei Dritten (z. B. bei anderen Sozialleistungsträgern, Finanzämtern, Banken) dürften nur auf gesetzlicher Grundlage nach sorgfältiger Prüfung eingeführt werden, ob sie zur Mißbrauchsbekämpfung erforderlich, angemessen und geeignet sind.

Nachdem die Datenschutzbeauftragten von Bund und Ländern mit einer gemeinsamen Entschließung (vgl. u. Ziff. 22.9.) in diesem Sinne interveniert hatten, machte sich die ASMK die Vorschläge ihrer Arbeitsgruppe nicht im einzelnen zu eigen, sondern leitete sie der Bundesregierung zu mit der Bitte, unter Einbe-

ziehung der Vorschläge der Arbeitsgruppe und der Entschließung der Datenschutzbeauftragten die erforderlichen Schritte zur Realisierung eines verbesserten Datenaustausches in die Wege zu leiten. Dabei solle auch das Gesprächsangebot der Datenschutzbeauftragten aufgenommen werden.

Zugleich wurde erklärt, man sei sich bewußt, daß im Einzelfall schwierige Güterabwägungen zwischen den Interessen der Solidargemeinschaft als ganzer an einem zielgenauen Ressourceneinsatz und den Interessen der einzelnen Leistungsempfänger bzw. Antragsteller an der Wahrung ihres Rechts auf informationelle Selbstbestimmung zu treffen seien.

Der Senator für Arbeit hatte mich — ebenso wie einige andere Sozialministerien meine jeweils zuständigen Kolleginnen und Kollegen — über die Ergebnisse der Arbeitsgruppe der ASMK so rechtzeitig unterrichtet, daß die Datenschutzbeauftragten insgesamt sich rechtzeitig vor der Sitzung der ASMK im Oktober 1997 zu Wort melden konnten. Die Bundesregierung ist m. W. bislang noch nicht an den Bundesbeauftragten für den Datenschutz zwecks Abstimmung über die Umsetzung von Vorschlägen der ASMK-Arbeitsgruppe herangetreten.

15. Bildung, Wissenschaft und Kunst

15.1 Organisationsuntersuchung zum Lehrereinsatz — Anforderungen an Beratungsfirma

Im Zusammenhang mit der Entwicklung eines Konzeptes zur Optimierung des Lehrereinsatzes beauftragte der Senator für Bildung, Wissenschaft, Kunst und Sport die Fa. Kienbaum Unternehmensberatung GmbH mit einer Untersuchung, die Datenerhebungen sowohl in der Behörde des Senators als auch an zahlreichen Schulen vorsah. Erhoben und ausgewertet werden sollten von der Auftragnehmerin z. B. Daten aus Organigrammen, Geschäftsverteilungsplänen und Stellenplänen der Schulen und Informationen über Krankheiten und Beurlaubungen von Lehrkräften. Es sollten nicht nur aggregierte oder statistische Ausgangszahlen, sondern gerade auch Einzelfälle betreffende personenbezogene oder zumindest personenbeziehbare Daten in die Erhebungen einbezogen werden.

Ich wies in meiner ausführlichen Stellungnahme darauf hin, daß bei der Zulässigkeit der Verarbeitung der Lehrerdaten danach zu unterscheiden ist, ob die Erhebung aus Datenbeständen im Bereich der nach dem Schulverwaltungsgesetz dem Land zugewiesenen Aufgaben erfolgt oder Angaben aus dem Bereich der den beiden Stadtgemeinden gesetzlich zugeordneten Aufgaben zusammengetragen werden.

Da in dem mit der Fa. Kienbaum abgeschlossenen Vertrag auch der Inhalt der für die Erhebung vorgesehenen Erhebungsunterlagen, der Kreis der von der Befragung Betroffenen und die Art der Auswertungen des erhobenen Datenmaterials festgelegt waren, war auf die Geltung der Vorschriften über die Datenverarbeitung im Auftrag (§ 9 BrDSG) hinzuweisen. Sie verpflichten zu einer ausdrücklichen Vertragsklausel, daß vom Auftragnehmer bestimmte näher bezeichnete technische und organisatorische Sicherungsmaßnahmen zu ergreifen, sowie dazu, daß etwaige Unterauftragsverhältnisse schriftlich festgelegt werden müssen. Da beide Punkte im Vereinbarungstext fehlten, schlug ich entsprechende Ergänzungen vor.

Als weitere Anforderungen definierte ich das Gebot der frühzeitigen Anonymisierung der auf einzelne Lehrer beziehbaren Angaben und die Notwendigkeit, daß der Abschlußbericht der Beratungsfirma oder sonstige dem Auftraggeber abzuliefernde Untersuchungsergebnisse keinen Personenbezug mehr aufweisen dürfen.

Der Senator für Bildung erklärte sich bereit, meinen Vorschlägen zu entsprechen bzw. für deren Beachtung durch das beauftragte Unternehmen zu sorgen. Der Vertragstext wurde allerdings nicht mehr ergänzt, wie ich es eigentlich für notwendig gehalten hätte. Die Auftragnehmerin gab aber jedenfalls gegenüber dem Bildungssenator noch einmal eine ausdrückliche Erklärung zur Einhaltung des Bremischen Datenschutzgesetzes ab.

Da mittlerweile zahlreiche Organisationsuntersuchungen in der bremischen Verwaltung durchgeführt wurden oder beabsichtigt sind, hat die Senatskommission für das Personalwesen im Juni 1997 eine entsprechende Arbeitshilfe herausgegeben, die auch Hinweise für den Umgang mit personenbezogenen Daten bei derartigen Vorhaben enthält (vgl. dazu o. Ziff. 11.3.).

16. Arbeit

16.1 Schatten der NS-Vergangenheit mit Datenschutzrelevanz

Mehr als ein halbes Jahrhundert nach dem Ende des NS-Unrechtsregimes müssen sich bremische Dienststellen noch immer mit dessen Folgen beschäftigen. Da es durchweg um menschliches Handeln und/oder menschliches Leiden geht, also personenbezogene Daten verarbeitet werden, ergibt sich zwangsläufig die datenschutzrechtliche Relevanz der staatlichen Aufarbeitung der NS-Vergangenheit.

16.1.1 Renten an „Kriegsverbrecher" im Ausland — Gefahr des Pauschalverdachts

Zu Beginn des Berichtsjahres berichteten die Medien darüber, daß immer noch Kriegsbeschädigtenrenten an ehemalige Mitglieder der Waffen-SS gezahlt würden. Vor allem zwei Fälle von in den USA lebenden Versorgungsempfängern wurden aufgedeckt; die Zahlung der Bezüge wurde eingestellt. Da das Versorgungsamt Bremen zentral für auf dem amerikanischen Kontinent lebende Versorgungsberechtigte zuständig ist, war es der öffentlichen Kritik besonders ausgesetzt.

Das Land Bremen reagierte hierauf zum einen damit, daß es im Bundesrat einen Entwurf zur Änderung des Bundesversorgungsgesetzes einbrachte, wonach demjenigen die Kriegsopferversorgung zu versagen bzw. zu entziehen ist, der gegen die Grundsätze der Menschlichkeit oder Rechtsstaatlichkeit verstoßen hat. Die Initiative hatte Erfolg: Inzwischen ist ein Gesetz dieses Inhalts verabschiedet worden und am 21. Januar 1998 in Kraft getreten (BGBl. I 1998, S. 66).

Zum anderen kam der Senator für Arbeit umgehend und offensichtlich ohne nähere Prüfung der Rechtslage der Aufforderung des Bundesministeriums für Arbeit und Sozialordnung (BMA) nach, ihm eine Liste der Empfänger von Versorgungsleistungen im Ausland zuzuleiten, die dieser zwecks Abgleich mit dortigen Unterlagen über Kriegsverbrechen an die Justizbehörden der Wohnsitzstaaten weiterleiten wollte. Andere gleichlautend angeschriebene Länderministerien reagierten ablehnend, z. T. auf Anraten des von ihnen eingeschalteten Landesdatenschutzbeauftragten. Da den Anstoß für die Aktion die Medienberichterstattung über in den USA lebende Versorgungsempfänger gegeben hatte, ist zu vermuten, daß die bremische Liste, die ja die Namen der Versorgungsempfänger in Nord- und Südamerika enthielt, im Mittelpunkt stand.

Ich äußerte in Übereinstimmung mit anderen Landesdatenschutzbeauftragten Bedenken dagegen, daß ohne Vorprüfung mehrere Tausend Namen von Versorgungsempfängern ausländischen Behörden mit dem Zweck der Prüfung wegen einer möglichen Verwicklung in NS-Verbrechen genannt werden sollten. Dies könne auch unbescholtene Betroffene in erhebliche Schwierigkeiten bringen. Zumindest bedürfe es vor einer Weiterleitung an ausländische Stellen der Prüfung, ob diese überhaupt Unterlagen haben, mit denen die Daten der Versorgungsempfänger abgeglichen werden könnten, und ob der jeweilige Staat die Einhaltung der Zweckbindung und Vertraulichkeit der Listen zu gewährleisten willens und imstande sei. Der Vorschlag, das Bundesministerium möge doch die Staaten, die über aufschlußreiches Datenmaterial zu verfügen glauben, bitten, dieses ihrerseits zwecks Abgleich durch die zuständige Landesversorgungsverwaltung zur Verfügung zu stellen, wurde bislang nicht aufgegriffen. Das Bundesministerium erklärte, dies sei keine gangbare Alternative. Es versicherte, es werde Listen nur weiterleiten, wenn das Verfahren im Empfängerstaat rechtsstaatlich sei und die Daten vertraulich für die Abgleichszwecke genutzt würden. Bislang haben nach meinem Informationsstand bremische Stellen keine Kenntnis davon, wie der Bund mit der Namensaufstellung aus Bremen umgegangen ist. Auch ist eine Rückmeldung über einen mit ihrer Hilfe aufgespürten NS-Täter bislang ausgeblieben. Nach Presseberichten von Anfang März 1998 soll das BMA die Überprüfung der Kriegsopferrenten inzwischen eingeleitet haben und beabsichtigen, dazu u. a. das Berlin Document Center und das Simon Wiesenthal Center in Israel einzuschalten.

Trotz der rechtspolitisch unstreitig lauteren Zielsetzung dieser Aktion war für mich wichtig, daß auch bei solchen Vorhaben der rechtsstaatlich gebotene Datenschutzstandard beachtet wird. Medienkritik sollte nicht zu übereilten Reaktionen führen, bei denen zu wenig Zeit aufgebracht wird für die Prüfung der Effektivität sowie der Verhältnismäßigkeit des Eingriffs in die Persönlichkeitsrechte der Betroffenen.

16.1.2 Auskünfte aus Entschädigungsakten an Versicherungen — nicht an den Opfern vorbei

Ganz anders war die Konfliktlage im zweiten „Fall": Der Datenschutz sieht sich hier vor der Aufgabe, Rechte von Opfern (oder deren Rechtsnachfolgern) des NS-Regimes zu wahren. Einige deutsche Versicherungsunternehmen sind in den USA von Holocaust-Opfern oder deren Nachkommen aus Lebensversicherungen in Anspruch genommen worden, die in den 20er und 30er Jahren abgeschlossen worden waren. Da das NS-Regime die Versicherungen von Deportierten konfisziert hatte, hatten später die geschädigten NS-Opfer die Möglichkeit, einen Anspruch auf Entschädigung gegen die Bundesrepublik geltend zu machen. Für Prozeßzwecke versuchen jetzt die verklagten Versicherungen, von den Entschädigungsbehörden der Länder Auskunft darüber zu erhalten, ob derartige Entschädigungen gezahlt worden sind. Die Angelegenheit ist auch wegen der erheblichen publizistischen Resonanz — vor allem in den USA — brisant.

Ich hatte Gelegenheit, der Konferenz der Entschädigungsreferenten der Länder die Datenschutzrechtslage zu erläutern. Grundlage für die Entscheidung, ob die Entschädigungsbehörden die gewünschten Auskünfte erteilen dürfen, sind die Regelungen der Landesdatenschutzgesetze zur Übermittlung personenbezogener Daten durch öffentliche an nicht-öffentliche Stellen, d. h. im Lande Bremen § 17 BrDSG. Nach dessen Absatz 1 Nr. 3 ist die Auskunftserteilung nur dann zulässig, wenn 1.) der Empfänger ein rechtliches Interesse an der Kenntnis der erfragten Daten glaubhaft macht, 2.) er diese Kenntnis nicht auf ihm zumutbare andere Weise erhalten kann und 3.) schutzwürdige Belange des Betroffenen nicht entgegenstehen. Mag die erste Voraussetzung gegeben sein, so ist doch anzuzweifeln, ob dies auch für die zweite gilt: Der Versicherung wird es zuzumuten sein, den ihr bekannten Anspruchsteller selbst um die Auskunft oder um seine Einwilligung in die Einholung der Auskunft zu bitten und dies bei Verweigerung dem Gericht gegenüber vorzutragen. Die Anforderung zu 3.) schließlich setzt zumindest voraus, daß vor Erteilung der Auskunft der Betroffene angehört wird.

Die Landesentschädigungsbehörden müssen — ggf. nach Beteiligung des jeweiligen Datenschutzbeauftragten — auf der Grundlage der jeweils in ihrem Bundesland geltenden, inhaltlich nicht völlig übereinstimmenden Landesdatenschutzgesetze entscheiden. Liegen die gesetzlichen Voraussetzungen für eine Übermittlungsbefugnis vor, so sind sie nicht schon deshalb zur Auskunft an die Versicherungen verpflichtet, sondern müssen nach pflichtgemäßem Ermessen entscheiden.

Bislang hat das Ausgleichsamt Bremen noch keine Anfragen von Versicherungsgesellschaften erhalten, ob mit oder ohne Einwilligung der Betroffenen. Jedenfalls sind für den Fall einer Anfrage die datenschutzrechtlichen Entscheidungskriterien geklärt.

16.2 AOK-Projekt Versichertenbetreuer

In meinem 17. Jahresbericht hatte ich unter Ziff. 13.1.2 berichtet, daß ich mich strittig mit der AOK Bremen/Bremerhaven darüber auseinanderzusetzen hatte, daß sie begonnen hatte, über den Rahmen der gesetzlich vorgesehenen Prüfverfahren hinaus die ihr für Abrechnungszwecke übermittelten Rezeptdaten ihrer Versicherten auf Dauer versichertenbeziehbar zu speichern, um sie bei Auffälligkeiten ggf. den Ärzten vorhalten und später auch versichertenbezogen auswerten zu können. Dem Senator für Arbeit und mir gelang es, die AOK dazu zu bewegen, von diesem Verfahren Abstand zu nehmen und die hierfür gespeicherten Daten vollständig zu löschen (vgl. 18. JB, Ziff. 15.2.4.).

Sorgfältig in Zusammenarbeit mit mir vorbereitet wurde dagegen das „Arzt-AOK-Versichertenbetreuungsprogramm", mit dessen Umsetzung die AOK auf der Grundlage eines abgestimmten Datenverarbeitungkonzepts begonnen hat, das folgende Schritte vorsieht: Aus den — jeweils auch die Diagnosen aufführenden — Arbeitsunfähigkeitsbescheinigungen bzw. Abrechnungsdaten der Krankenhäuser werden per EDV Versicherte mit bestimmten schwerwiegenden Krankheitsarten herausgefiltert. Eigens hiermit beauftragte Versichertenbetreuer wenden sich an diese Versicherten und bieten ihnen Beratung und Unterstützung an. Nach deren jeweils schriftlich erklärtem Einverständnis spricht der Versichertenbetreuer Ärzte und andere Beteiligte mit dem Ziel der Optimierung der gesundheitlichen und sozialen Versorgung an. Die in diesem Zusammenhang separiert

gespeicherten Daten des Versicherten werden nur für Zwecke des Programms genutzt und nach Beendigung gelöscht. Ist der Versicherte, z. B. mangels Einwilligung, nicht in das Programm aufgenommen worden, werden seine für Zwecke des Programms separiert gespeicherten Daten unverzüglich gelöscht.

Aus Sicht des Datenschutzes zeichnet dieses Projekt seine Transparenz gegenüber den einbezogenen Versicherten aus. Hinzukommt, daß inzwischen §§ 63-66 SGB V es den gesetzlichen Krankenkassen erlauben, zur Verbesserung der Qualität und der Wirtschaftlichkeit der gesundheitlichen Versorgung ihrer Versicherten Modellvorhaben durchzuführen. Die AOK Bremen/Bremerhaven will ihr Projekt zur Versichertenbetreuung in ihre Satzung aufnehmen. Es ist befristet und soll nach wissenschaftlichen Maßstäben ausgewertet werden.

16.3 Datenbanken der Krankenkassen — Sicherung der Zweckbindung

16.3.1 Bundesweite Initiative

Die Krankenkassen erhalten zu administrativen Zwecken eine Fülle von Gesundheitsdaten ihrer Versicherten, etwa auf Arbeitsunfähigkeitsbescheinigungen und in Unterlagen zur Abrechnung oder zu Wirtschaftlichkeitsprüfungen, neuerdings auch im Rahmen gesetzlich erlaubter Modellvorhaben. Über kurz oder lang werden diese Unterlagen nicht mehr in kaum auswertbaren Papierbergen bei den Kassen lagern, sondern in Datenbanken jederzeit digital, d. h. frei auswertbar, gespeichert sein.

Die Datenschutzbeauftragten von Bund und Ländern sind sich darin einig, daß § 78 a SGB X die Krankenkassen verpflichtet, technische und organisatorische Vorkehrungen dafür zu treffen, daß sie diese Datenmengen, und insbesondere die medizinischen Daten, nur im Rahmen der zugelassenen Zwecke und für die jeweils zugelassene Dauer nutzen können. In einem Datenschutzkonzept ist festzulegen, daß

- auf die gespeicherten Versichertendaten nur die jeweils zugriffsberechtigten Mitarbeiter im Rahmen der gesetzlichen Zweckbegrenzungen zugreifen,
- versichertenbezogene Daten zu löschen sind, sobald die gesetzlichen Fristen für ihre Speicherung abgelaufen sind.

Die Einhaltung dieser Vorgaben muß sowohl durch den Datenschutzbeauftragten der Krankenkassen als auch durch den jeweils zuständigen Bundes- oder Landesdatenschutzbeauftragten kontrolliert werden können.

Soweit es nicht die einzelne Krankenkasse ist, die je ein eigenes Datenverarbeitungskonzept erarbeitet, sondern dies ihr von ihrem Spitzenverband zur Verfügung gestellt wird, liegt es auch an diesem, das daraus resultierende Datenschutzkonzept bereitzustellen. Nachdem die AOK Bremen/Bremerhaven, mit der ich die Problematik zunächst erörtert hatte, dies eingewandt hatte, verständigten sich die Datenschutzbeauftragten von Bund und Ländern auf meinen Vorschlag hin, daß der Bundesbeauftragte für den Datenschutz an die Spitzenverbände der gesetzlichen Krankenversicherung mit der Forderung nach zentralen Vorgaben für Datenschutzkonzepte herantritt und daß die jeweils zuständigen Datenschutzbeauftragten ggf. anschließend dies gegenüber den einzelnen Krankenkassen unterstützen und die Umsetzung der Konzepte erörtern bzw. prüfen.

16.3.2 Trend zur Automation der Gesundheits-DV — Leitprinzipien der Beurteilung

Die geschilderte Entwicklung ist einzuordnen in den Gesamtkontext der zunehmenden Automatisierung der Verarbeitung medizinischer Daten durch Krankenkassen, Krankenhäuser und Gesundheitsämter, den ich im 18. Jahresbericht ausführlich dargestellt habe (vgl. 18. JB, Ziff. 15.1). Leitprinzipien datenschutzrechtlicher Beurteilung sind dabei für mich vor allem

- die Erhaltung des Freiraums für den Patienten/Versicherten, in Kooperation mit dem Arzt seines Vertrauens eigenverantwortlich über den Umgang mit seiner Gesundheit bzw. Krankheit zu bestimmen,
- die Ablehnung einer umfassenden Kontrolle des gesundheitlichen Verhaltens des Einzelnen per Datenauswertung durch anonyme administrative Systeme, sowie
- die Einhaltung gesetzlich vorgegebener Zweckbindungen und Löschungsfristen bei der Verarbeitung von Patienten- bzw. Versichertendaten.

Die Entwicklung der letzten zwei Jahre hat gezeigt, daß die Technik sich so rasant entwickelt, daß die Gefahren für die Persönlichkeitsrechte wachsen, daß aber zugleich sowohl die Einsicht in die Notwendigkeit regulierender Vorkehrungen wächst als auch die technischen Schutzinstrumente bereitgestellt werden können. Neue Risiken beinhalten auch die Überlegungen zur „Aufrüstung" von Chipkarten mit medizinischen Angaben bis hin zu einer umfassenden Vernetzung der an der gesundheitlichen Versorgung Beteiligten. Ich werde diese Entwicklung weiter aufmerksam beobachten.

17. Bau

17.1 Automatisiertes Liegenschaftsregister — verschlüsselte Datenübertragung

Unter den Voraussetzungen des § 10 Vermessungs- und Katastergesetz darf die Katasterbehörde anderen Behörden Daten aus dem Liegenschaftskataster übermitteln. Wegen des zunehmenden Technikeinsatzes in der bremischen Verwaltung wurde der Wunsch an die Behörde herangetragen, die zu übermittelnden Daten auf Datenträgern zur Verfügung zu stellen. Da es sich hierbei um die Übertragung im ASCII-Format gespeicherter und damit durch Standard-Software lesbare, personenbezogene Angaben handelt, und daher das Risiko bestand, daß die Daten auf den Datenträgern durch Unbefugte gelesen, verändert oder gelöscht werden könnten, habe ich die Katasterbehörde auf die Notwendigkeit einer Verschlüsselung hingewiesen.

Die Behörde erklärte sich daraufhin bereit, bis zur Benennung bzw. Freigabe eines geeigneten Verschlüsselungsprogramms durch die Senatskommission für das Personalwesen (SKP) auf die Datenübermittlung mittels Datenträger zu verzichten. Inzwischen wird aber die Verschlüsselungs-Software PGP (Pretty Good Privacy; s. o. Ziff. 9.1.2.) eingesetzt, was in der bremischen Verwaltung noch viel zu selten geschieht. Anzuerkennen ist m. a. W., daß die Katasterverwaltung bei der Gewährleistung sicherer Datenübertragung eine Art Vorreiterrolle einnimmt. Hinzu kommt, daß sie mit den Datenempfängern spezielle Nutzungsvereinbarungen trifft, die sicherstellen sollen, daß diese die erhaltenen Angaben nicht unbefugt verarbeiten.

17.2 Entwurf eines Wohnungsbaugesetzbuches

Der Senator für Bau, Verkehr und Stadtentwicklung hat mir im Sommer 1997 den Entwurf eines Gesetzes zur Reform des Wohnungsbaurechts der Bundesregierung mit der Bitte um Stellungnahme vorgelegt. Der Entwurf enthält an verschiedenen Stellen lediglich einzelne allgemeine Regelungen, die die Verarbeitung personenbezogener Daten über Bauherren, Eigentümer, Vermieter, Mieter und Mitbewohner voraussetzen. Ich halte es jedoch für erforderlich, systematisch gegliederte Vorschriften zu schaffen, die normenklar regeln, welche personenbezogenen Daten zu welchen Zwecken erhoben, gespeichert und ggf. an welche Stellen übermittelt werden dürfen und wann die Angaben zu löschen sind.

Hierbei ist unerheblich, ob die notwendigen Datenverarbeitungsvorschrifen in dieses Gesetz aufgenommen oder von den Ländern geschaffen werden, zumal § 22 des Entwurfs vorsieht, daß die Länder das Verwaltungsverfahren festlegen sollen. Im zweiten Fall sollte § 22 des Entwurfs ausdrücklich vorsehen, daß die Länder durch landesrechtliche Vorschriften (auch) die Verarbeitung personenbezogener Daten zur Durchführung dieses Gesetzes bestimmen.

Für den Fall, daß der Bund selbst diese Regelungen schafft, halte ich es für erforderlich, im Wohnungsbaugesetzbuch darüber hinaus festzulegen, welche Nachweise für welche Zwecke der Betroffene zu erbringen hat.

Außerdem sollte bestimmt werden, daß der Betroffene darauf hinzuweisen ist, daß er die in den Nachweisen enthaltenen Daten, die z. B. für die Ermittlung des Einkommens nach §§ 48 bis 52 des Entwurfs nicht erforderlich sind, unkenntlich machen darf (vgl. dazu o. Ziff. 17.3.).

Die senatorische Behörde hat meine Stellungnahme an das Bundesministerium für Raumordnung, Bauwesen und Städtebau weitergeleitet, allerdings im zuständigen Bundesrats-Ausschuß keine entsprechenden Anträge gestellt. Die erste Lesung des Entwurfs im Bundestag hat am 13. November 1997 stattgefunden. Das Gesetzgebungsverfahren ist noch nicht abgeschlossen.

17.3 Wohngeld — Einkommensnachweis mit Schwärzungsmöglichkeit

Nach § 11 Abs. 2 Satz 2 Wohngeldgesetz (WoGG) können bei Antragstellern, die zur Einkommensteuer veranlagt werden, die Einkünfte berücksichtigt werden, die sich z. B. aus dem letzten Einkommensteuerbescheid oder der letzten Einkommensteuererklärung ergeben. Das gleiche gilt für Anträge auf Erteilung von Wohnberechtigungsscheinen nach § 5 Wohnungsbindungsgesetz (WoBindG). Nach Angaben des Senators für Bau, Verkehr und Stadtentwicklung wird die Vorlage eines solchen Bescheides in der Regel von selbständigen bzw. gewerbetreibenden Antragstellern und in sonstigen Einzelfällen dann als Nachweis verlangt, wenn bestimmte Angaben nicht aus anderen Unterlagen ersichtlich sind. Diese Praxis hatte ich bereits im 17. Jahresbericht unter Ziff. 16.1 problematisiert.

Auf Anfrage hat die senatorische Behörde behauptet, es sei gängige Praxis bei den Wohngeldstellen, daß Antragsteller wohngeldrechtlich nicht relevante Daten auf den eingereichten Unterlagen oder den entsprechenden Kopien unkenntlich machen können. Meine Nachfrage, ob denn die Betroffenen generell auf diese Möglichkeit hingewiesen werden, hat der Bausenator zum Anlaß genommen, eine entsprechende allgemeine Information über die Schwärzungsmöglichkeit in die Antragsformulare und Erläuterungen aufzunehmen.

Inzwischen hat der Senator für Frauen, Gesundheit, Jugend, Soziales und Umweltschutz im Parallefall der Einkommensanrechnung bei den KTH-Beiträgen ein Mitteilungsblatt herausgegeben, aus dem für die Betroffenen klar erkennbar ist, welche Einkommensdaten im einzelnen erforderlich sind, so daß sie eine klare Entscheidungsgrundlage dafür haben, welche Daten sie unkenntlich machen können (vgl. o. Ziff. 14.4.1.2.).

Ich habe daraufhin den Senator für Bau, Verkehr und Stadtentwicklung am 2. Februar 1998 gebeten, für das Verfahren zur Einkommensermittlung bei Anträgen auf Wohngeld, Wohnberechtigung und Wohnungsbauförderung genauso detailliert und bürgerfreundlich zu verfahren und die entsprechenden notwendigen bzw. verzichtbaren Angaben in die einschlägigen Richtlinien sowie in die Erläuterungen zu den jeweiligen Anträgen aufzunehmen.

18. Finanzen

18.1 Eigenheimzulage — Finanzierungsnachweis nur im Einzelfall

Ein Eingeber hat sich an mich gewandt, weil ihm vom Finanzamt Bremerhaven schon bei der Ausgabe des Antragsformulars mitgeteilt worden war, daß er im Rahmen der Beantragung der Eigenheimzulage auch die Art der Finanzierung seines Hauses nachweisen müsse.

Mir wurde von der Oberfinanzdirektion Bremen, die vom zuständigen Finanzamt eingeschaltet worden war, bestätigt, daß Art und Zusammensetzung der Finanzierung der selbstgenutzten Wohnung im allgemeinen nicht für die Gewährung der Eigenheimzulage relevant sind. Allerdings seien die Finanzämter gemäß § 85 i. V. m. § 88 Abgabenordnung gehalten, bei steuerlich erheblichen Sachverhalten — wie z. B. größeren privaten Investitionen — aufzuklären, ob diese Aufwendungen mit den Steuererklärungen im Einklang stünden. Bei der Anwendung dieser Vorschriften habe das bearbeitende Finanzamt einen Spielraum, immer vorausgesetzt, daß es um die Prüfung eines konkreten Einzelfalls geht. Eine Praxis, bei der von vornherein alle Antragsteller zum Nachweis aufgefordert werden, ist jedenfalls mit dieser steuerrechtlichen Vorgabe nicht vereinbar.

18.2 Fahrtenbücher versus Arztgeheimnis

Das Bundesministerium der Finanzen hat in einem neuen Erlaß verfügt, daß ab 1. Januar 1998 Ärzte verpflichtet sind, im Fahrtenbuch, das der steuerrechtlichen Abgrenzung der privaten Fahrten von der geschäftlichen Nutzung dient, neben dem Fahrziel, den Kilometerständen etc. auch den Namen des aufgesuchten Patienten anzugeben.

Zu dieser Verfügung vertrete ich ebenso wie der Bundesbeauftragte für den Datenschutz und meine Kollegen in den Ländern, soweit sie sich bisher zur Thematik geäußert haben, folgende Auffassung:

Das Auskunftsverweigerungsrecht des Arztes nach § 102 Abs. 1 Nr. 3 Buchst. c AO gegenüber dem Finanzamt umfaßt alle Tatsachen, die ihm in seiner beruflichen Eigenschaft anvertraut oder bekannt geworden sind.

Einbezogen ist auch die Tatsache, daß ein bestimmter Patient von einem bestimmten Arzt behandelt wird und mithin auch dessen Name.

Unterstützt wird diese Auffassung durch eine Entscheidung des Bundesgerichtshofs zur Parallelsituation des Zeugnisverweigerungsrechts des Arztes im Strafverfahren (§ 53 Abs. 1 Nr. 3 StPO; BGHSt 33, 148, 151). Der BGH erstreckt dort die Schweigebefugnis ebenfalls auf die Identität des Patienten und die Tatsache seiner Behandlung.

Die neu eingeführte Verpflichtung der generellen Aufdeckung der Identität besuchter Patienten erscheint aber für die Aufgabenerfüllung der Finanzbehörden auch nicht erforderlich und damit nicht verhältnismäßig, weil diese die Aufzeichnungen der Ärzte nicht „flächendeckend", sondern in der Regel nur im Rahmen von Betriebsprüfungen oder sonstigen Stichprobenkontrollen überprüfen (können).

Mein Bonner Kollege hat mit Schreiben vom 21. November 1997 das Bundesfinanzministerium gebeten, den entsprechenden Erlaß und evtl. weitere Regelungen, die die Eintragung des Namens der Patienten in Fahrtenbüchern betreffen, aufzuheben. Eine Antwort ist mir noch nicht zugegangen.

Ich habe meine Auffassung sowohl der bremischen Ärztekammer ausführlich dargelegt als auch die Oberfinanzdirektion um Stellungnahme bzw. Änderung der Handhabung gebeten. Die Oberfinanzdirektion hat in ihrer Antwort auf die Begründung im Erlaß des Bundesfinanzministeriums verwiesen und im übrigen mein Schreiben zur weiteren Beratung an den Senator für Finanzen weitergeleitet. Eine Reaktion ist von dort bisher nicht erfolgt.

19. Magistrat Bremerhaven

19.1 Beanstandung: Krankheitsdaten an Arbeitgeber gefaxt

Schwerbehinderte genießen besonderen gesetzlichen Schutz. So muß der Arbeitgeber, will er einem schwerbehinderten Arbeitnehmer kündigen, behördliche Zustimmung einholen, in Bremerhaven beim Amt für Schwerbehinderte. Selbstverständlich soll das Amt ihn auf Anfrage darüber informieren, ob ein gekündigter Arbeitnehmer, der sich ihm gegenüber auf diesen Kündigungsschutz beruft, dies zu recht tut. In der Regel wird der Nachweis durch Vorlage des Schwerbehindertenausweises erbracht. Der Kündigungsschutz greift aber auch bereits, wenn noch vor der Kündigung die Anerkennung als Schwerbehinderter beantragt worden war.

Ein davon betroffener Arbeitnehmer wandte sich an mich. Er legte mir die Kopie eines Telefaxes des Amtes an den Arbeitgeber vor, das seinen Antrag auf Anerkennung als Schwerbehinderter beim hierfür zuständigen Versorgungsamt enthielt. Diesen hatte sich das Amt für Schwerbehinderte seinerseits vom Versorgungsamt faxen lassen, um seiner Beratungspflicht dem Arbeitgeber gegenüber nachkommen zu können. Das Amt für Schwerbehinderte wiederum hatte den ihm gefaxten Antrag an den Arbeitgeber weitergefaxt. Dieser konnte seinerseits dem Fax den Eingangsstempel des Amtes entnehmen und daraus schließen, ob er dessen Zustimmung einholen mußte oder nicht. Insoweit wäre aus datenschutzrechtlicher Sicht gegen den Vorgang nichts einzuwenden gewesen.

Der Arbeitgeber erfuhr aus der Fernkopie aber auch, auf welche Krankheiten sich der Arbeitnehmer in seinem Antrag auf Anerkennung als Schwerbehinderter berufen und welche Ärzte er als Auskunftsquellen benannt hatte. Diese Daten aber erfährt der Arbeitgeber selbst dann nicht, wenn einer seiner Arbeitnehmer als Schwerbehinderter anerkannt worden ist. Der Schwerbehindertenausweis jedenfalls enthält sie nicht; und dies mit gutem Grund.

Das Amt für Schwerbehinderte hätte sich auf Anfrage des Arbeitgebers auf die Auskunft beschränken müssen, ob und wenn ja, wann beim Versorgungsamt ein Antrag des Arbeitnehmers auf Anerkennung als Schwerbehinderter eingegangen war. Insoweit war das Amt zur Auskunftserteilung in Erfüllung seiner Beratungspflicht dem Arbeitgeber gegenüber nach § 69 Abs. 1 Nr. 1 SGB X befugt. Dagegen hat das Amt durch die Übermittlung der darüber hinausgehenden Daten seine aufgrund des § 35 SGB I dem Arbeitnehmer gegenüber bestehende Verpflichtung verletzt, dessen Sozialgeheimnis zu wahren.

Nach einem erfolglosen Schriftwechsel, im Rahmen dessen die Leitung des Amtes für Schwerbehinderte ohne nähere Begründung darauf beharrte, es sei bei der Absendung des Faxes korrekt verfahren, habe ich dem Magistrat der Seestadt Bremerhaven gegenüber eine Beanstandung nach § 29 BrDSG ausgesprochen. Der

Magistrat hat die Berechtigung der Beanstandung anerkannt, die Verletzung des Sozialgeheimnisses bedauert und angeordnet, daß die Mitarbeiter des Amtes für Schwerbehinderte nochmals eingehend auf die Einhaltung der Datenschutzbestimmungen hinzuweisen sind (vgl. o. Ziff. 3.2.3.).

19.2 PROSOZ/S Bremerhaven mit neuem Datenschutzkonzept

Das Sozialamt Bremerhaven hat mit der Einführung des Dialogsystems PROSOZ/S des Prosoz-Institutes Herten sein altes Stapelverfahren, das im wesentlichen zur Zahlbarmachung und Berechnung der laufenden Sozialhilfe eingesetzt wurde und neuen inhaltlichen und technischen Anforderungen nicht mehr gewachsen war, abgelöst. Das neue Dialogsystem ermöglicht die Bearbeitung allgemeiner Sozialhilfe, Heimhilfe und Leistungen an Asylbewerber/-innen (Erhebung persönlicher Daten von Hilfesuchenden, Berechnung des Hilfeanspruchs sowie Erstellung der Bescheide für Hilfeempfänger/-innen) direkt an computerunterstützten Sachbearbeiter/-innenplätzen. Das Fachverfahren wird im Rahmen einer sozialamtseigenen, d. h. internen Vernetzung unter Novell 4.11 betrieben.

Bei der Verarbeitung der sensiblen Daten von Sozialhilfeempfängern ist das Sozialgeheimnis der Betroffenen (§ 35 SGB I) durch die entsprechende Konfiguration der technischen Systeme zu gewährleisten (§ 78a SGB X). Dies gilt für alle Systemebenen.

Hierzu wurden in enger Abstimmung mit mir umfangreiche technische und organisatorische Maßnahmen in das mir zur Stellungnahme zur Verfügung gestellte Datenschutzkonzept aufgenommen, die ich insgesamt als angemessen im Verhältnis zum Schutzzweck bewertet habe.

Ich gehe davon aus, daß sowohl die Beantwortung einiger noch offen gebliebener Detailfragen als auch die Umsetzung weitergehender von mir vorgeschlagener Datenschutzmaßnahmen im Verlauf der Verfahrenserprobung erfolgen wird.

Der Magistrat plant inzwischen ein Intranet zur ämterübergreifenden Informationsaufbereitung und -darstellung sowie zur Bereitstellung genereller Applikationen. Hierfür liegen mir noch keine aussagefähigen Planungsunterlagen incl. Datenschutzkonzept vor. Arbeitskontakte mit dem zuständigen Amt 16 bestehen; erste Papiere für Projektplanungen habe ich erhalten.

Geplante Verbindungen zu diesem Netz sollen nach Vorstellung des Sozialamtes über gegenseitige Benutzereinrichtungen mit expliziter Rechtevergabe (Trusteezuordnungen zu den jeweiligen Verzeichnissen) im Rahmen der vorhandenen NDS-Struktur beim Sozialamt erfolgen.

Als Prinzip jedenfalls gilt, daß ein auf die vorherige datenschutzgerechte Netzplanung aufzubauendes Intranetdesign so zu entwickeln ist, daß das Risiko unerwünschter und fehlgeleiteter (d. h. gesetzlich unzulässiger) Zugriffe ausgeschlossen wird.

Eine Koppelung des Netzes des Sozialamtes Bremerhaven mit dem Magistratsnetz darf m. a. W. grundsätzlich nur erfolgen, wenn technische und organisatorische Maßnahmen ergriffen werden, die geeignet sind, den Schutz des Sozialgeheimnisses zu gewährleisten.

19.3 Stadtteilkonferenzen — Datenerhebungen über das Wohnumfeld

Zur stärkeren Beteiligung der Einwohner an der Gestaltung ihres unmittelbaren Wohnumfeldes haben sich in mehreren Bremerhavener Stadtteilen sog. Stadtteilkonferenzen gebildet. Auf freiwilliger Grundlage befassen sich dort interessierte Bürger und Bürgerinnen mit Fragen und Problemfeldern ihres Quartiers. Diese Gremien führen gelegentlich auch Befragungen durch, um die Situation in ihrem Stadtteil besser kennenzulernen. Von Interesse dabei sind u. a. Angaben über Wohnsituation, Lebensgewohnheiten, Einstellungen und Wünsche der befragten Einwohner.

Bei einer der Befragungsaktionen sollten z. B. Jugendliche auf freiwilliger Grundlage unter Angabe ihres Alters, ihres Geschlechts, ihrer Nationalität und ihrer finanziellen Lage, aber ohne Nennung ihres Namens und ihrer genauen Anschrift, nach ihrem Freizeitverhalten befragt werden. Die Erhebung sollte an einer im Stadtteil gelegenen Schule durchgeführt werden.

Dazu empfahl ich wegen der besonderen datenschutzrechtlichen Situation der Schulen, aber auch um die Anonymität der Befragung zu stärken, diese nicht direkt schulbezogene Umfrage aus der Schule möglichst herauszuhalten. Außer-

dem regte ich u. a. an, die Fragebögen um einen deutlichen Hinweis auf die Freiwilligkeit der Beantwortung zu ergänzen, die Auswertung ausschließlich für das konkrete Projekt vorzunehmen (Zweckbindung) sowie angemessene Löschungsfristen festzulegen.

Diese und weitere Vorgaben für die datenschutzgerechte Durchführung von Umfragen konnte ich auch einer unter Leitung der Dezernentin für Frauen, Bürgerbeteiligung und Ausländer des Magistrats zusammengekommenen Gesprächsrunde der Sprecher und Sprecherinnen der Stadtteilkonferenzen vortragen und dabei mein Merkblatt mit den wichtigsten dabei zu beachtenden Punkten verteilen. Die Teilnehmer reagierten kooperativ und nahmen mein Angebot zur Beratung bei der Vorbereitung von Einwohnerbefragungen an.

19.4 Telefonanlage des Magistrats — Gesprächsaufzeichnung nur bei Anlaß

In meinem letzten Jahresbericht hatte ich unter Ziff. 17.1 darüber berichtet, daß der Magistrat in seiner neuen zentralen Telefonvermittlung alle Gespräche anrufender Bürgerinnen und Bürger innerhalb eines Endlosbandes für zwölf Minuten aufzeichnen wollte. Nachdem ich unter Hinweis auf das Verbot der Aufzeichnung des nicht öffentlich gesprochenen Wortes in § 201 Strafgesetzbuch (StGB) meine Bedenken dagegen geltend gemacht und mehrere Gespräche hierzu, darunter eines auch mit dem Oberbürgermeister, geführt hatte, ist der Magistrat — meinem Vorschlag folgend — von seinem ursprünglichen Plan abgerückt und hat eine „Knopfdruck"-Vorrichtung installieren lassen. Diese gewährleistet, daß eine Gesprächsaufzeichnung nicht lückenlos, sondern nur bei einer konkret bestehenden oder zu erwartenden Belästigung oder Bedrohung erfolgt.

Ich habe mich durch einen Besuch Ende Januar 1998 in der Telefonzentrale von dem Vorhandensein der Vorrichtung überzeugt.

Im übrigen hält auch das neue Bundesamt für Post und Telekommunikation eine generelle Registrierung aller bei Telefonzentralen eingehenden Anrufinhalte für unzulässig. Eine Rechtfertigung im Sinne einer Notwehr- oder Notstandssituation könne nicht generell angenommen werden, sondern nur in begründeten Einzelfällen. Vergleichbar argumentiert auch das Bundesministerium der Justiz (Quelle: GDD-Mitteilungen 5/97, S. 5). Es hält eine rechtfertigende Einwilligung dann für möglich, wenn der Anrufer auf die Erfassung hingewiesen werde.

20. Datenschutz in der Privatwirtschaft

20.1 Umstrukturierung von Unternehmen — datenschutzrechtliche Konsequenzen

Bei der Umstrukturierung von Unternehmen oder Konzernen stellen sich für die Geschäftsleitungen auch datenschutzrechtliche Folgefragen. Aus diesem Grund hat mich im Berichtsjahr u. a. die Bremer Lagerhaus-Gesellschaft (BLG) um Beratung gebeten. Aus dem früheren Unternehmen wurden unter dem Dach einer Holding-Gesellschaft mehrere Tochterfirmen gebildet, darunter eine speziell für die Datenverarbeitung zuständige Gesellschaft.

Bei meiner Beratung ging es vor allem um die Problematik, wie der Konzernsachverhalt bei der Anwendung des Bundesdatenschutzgesetzes (BDSG) berücksichtigt werden kann. Das BDSG beinhaltet nämlich keine besonderen Regelungen für verbundene Unternehmen, sondern wendet sich ausschließlich an das Einzelunternehmen.

Besprochen habe ich mit der BLG u. a. die Frage, unter welchen Bedingungen der betriebliche Datenschutzbeauftragte nach § 36 BDSG für mehrere Tochtergesellschaften gleichzeitig bestellt werden kann. Dies ist unter bestimmten Rahmenbedingungen möglich. Allerdings habe ich davon abgeraten, daß Beauftragte der anderen Töchter zugleich als Beauftragte der Rechenzentrums-Gesellschaft fungieren: Auch unter einem Konzerndach bestehen Interessenkonflikte zwischen Auftraggeber und Auftragnehmer von Datenverarbeitungsaktivitäten und daher unterschiedliche Kontrollaufgaben der jeweiligen Beauftragten. Weitere Beratungsthemen waren die Meldepflicht der DV-Tochter zu dem bei mir nach § 32 BDSG geführten Register und die Anpassung der den Datenschutz betreffenden Vertragsklauseln in den Verträgen mit Kunden, Lieferanten und Beschäftigten an die neue Firmenstruktur.

Ich gehe davon aus, daß Beratungswünsche aus Anlaß gesellschaftsrechtlicher Umstrukturierungen in der Zukunft häufiger an mich gerichtet werden.

20.2 Kreditwirtschaft — Datenschutzprobleme im Überblick

Im Rahmen des sog. „Düsseldorfer Kreises", insbesondere in dessen „Arbeitsgruppe Kreditwirtschaft", haben die Datenschutzaufsichtsbehörden sich im Berichtsjahr mit mehreren Themenkreisen beschäftigt und ihre Auffassungen dazu abgestimmt. Im Rahmen dieses Berichts können nur Stichworte genannt werden wie

- die Klauselentwürfe des Zentralen Kreditausschusses (ZKA) für die Datenübermittlung im Konzern,
- die Übermittlung von Kundendaten durch Banken und Bausparkassen zur Durchführung von Kundenbefragungen und in anderen Fällen von Outsourcing,
- die Anforderungen an Regelungen der Kreditinstitute für Mitarbeitergeschäfte,
- die Beschränkung des geschäftsstellenübergreifenden Zugriffs auf Kontoinformationen,
- die Datenverarbeitung im Zusammenhang mit Videokamera-Überwachung in Schalterhallen, an Geldausgabeautomaten etc.

Zu meinem Bedauern konnte (noch) nicht zu allen Punkten mit den Vertretern der Kreditwirtschaft eine Einigung erzielt werden.

Besprochen zwischen der Bankenbranche und den Datenschutzbehörden wurden im Berichtsjahr auch die von der Kreditwirtschaft neu eingeführten Zahlungs- und Buchungssysteme. Das sogenannte Homebanking umfaßt die Abwicklung von Bankgeschäften sowohl über das Telefon als auch über den häuslichen PC. Waren online-Kontakte mit dem Kreditinstitut früher nur über das von der Telekom bereitgestellte System T-Online möglich, tritt mehr und mehr die interaktive Nutzung des Internet in den Vordergrund. Der dabei eingesetzte sogenannten HBCI-Standard (Homebanking Computer Interface) soll die Authentifizierbarkeit der Kommunikationspartner sowie die Vertraulichkeit der Kommunikation und die Integrität der übermittelten Daten gewährleisten.

Das technische Verfahren wurde durch einen Vertreter des Zentralen Kreditausschusses den Vertretern der Aufsichtsbehörden näher erläutert. Eine abschließende datenschutzrechtliche Bewertung dieses Verfahrens haben die Aufsichtsbehörden noch nicht vorgenommen.

Die datensicherungstechnische Evaluierung der sog. GeldKarte, ein u. a. auf den neuen Euroscheckkarten aufgebrachter aufladbarer Chip (vgl. dazu bereits 19. JB, Ziff. 18.1.), wurde im Berichtsjahr fortgesetzt. Mit ihr kann man bargeldlos auch kleinere Beträge bezahlen. Anders als beim Einsatz vor Bargeld entstehen bei Verwendung der GeldKarte „Datenspuren" des Kunden.

In einer Arbeitsgruppe der Datenschutz-Aufsichtsbehörden, die in Bremen tagte, haben Vertreter des Zentralen Kreditausschusses die Einzelheiten der verschiedenen, Datenverarbeitungsvorgänge und Datenströme, die bei der Aufladung wie auch beim Bezahlen mit der Karte im Hintergrund ablaufen, erläutert.

Als eines der Ergebnisse läßt sich festhalten, daß es erforderlich ist, daß die Kreditinstitute ihre Kunden so aufklären, daß diese wenigstens ansatzweise erkennen können, welche Datenflüsse stattfinden und an welchen Stellen über sie, wenn auch zum Teil verschlüsselt, Daten gespeichert und verarbeitet werden, z. B. in den sogenannten Schattenkonten. Die datenschutzrechtliche Einordnung der Verarbeitungsvorgänge bedarf ebenso weiterer Klärung wie die Zuordnung der Verantwortlichkeiten innerhalb des Verarbeitungssystems und die Verteilung der daran geknüpften Kontrollkompetenzen. Schließlich muß aus meiner Sicht durch ergänzende Regelungen bis hinunter zur Händlerebene sichergestellt werden, daß bei der Verwendung der GeldKarte nicht gegen oder ohne den Willen der Betroffenen Kunden- und Nutzungsprofile erstellt werden können.

Über die datenschutzfreundliche Ausgestaltung des GeldKarten-Verfahrens befinden sich die Aufsichtsbehörden mit der Kreditwirtschaft in weiteren Gesprächen.

20.3 Adressenbeschaffung durch „Verbraucherumfragen"

20.3.1 Bundesweite Befragungen

Im Berichtsjahr habe ich mich mehrfach mit dem Problem der Beschaffung und Vermarktung von Adreßdaten durch Verbraucherumfragen bzw. Hauhaltsbefragungen beschäftigt. Auch der Datenschutzausschuß hat sich mit der Thematik

befaßt. Mehrere derartige Umfragen bzw. Befragungsaktionen fanden im ganzen Bundesgebiet und damit auch im Bundesland Bremen statt, u. a. die Verbraucherumfrage der Infas Lifestyle AG, einem Unternehmen des Adreßhandelsunternehmens Schober-Gruppe in Ditzingen, und die Haushaltsumfrage der Claritas Deutschland Data + Services GmbH in Neu-Isenburg.

Bei diesen Umfragen wurden die befragten Personen entweder direkt angeschrieben und um Mithilfe gebeten (Infas Lifestyle) oder erhielten die Unterlagen per Postwurf zugestellt. Als Dankeschön für die Beteiligung an der Umfrage winkte den Betroffenen die Teilnahme an einer Verlosung. Die Erhebungsbögen enthielten eine Vielzahl sehr detaillierter Fragen (über 120), die sich u. a. mit dem Urlaub und dem Reiseverhalten, den Freizeitaktivitäten, der Gesundheit, der Wohnung, dem Auto, dem Kauf- und Konsumverhalten, der Schulbildung und beruflichen Tätigkeit und der finanziellen Situation beschäftigten. Um an der Verlosung teilzunehmen, mußte die genaue Adresse angegeben werden, außerdem weitere persönliche Daten wie z. B. der Familienstand und der Name des Ehepartners/Partners. Mit der Rückgabe eines ausgefüllten Erhebungsbogens erhielten die Betreiber der Umfragen also aktuellstes Adreßmaterial, das sich sehr gut nach unterschiedlichsten Kriterien, z. B. für genaue Verbraucherprofile, aufbereiten und für Direktwerbezwecke verwenden läßt (gezielte Ansprache).

20.3.2 Freiwilligkeit trotz Verwechslungsgefahr

Aus der Sicht des Datenschutzes ist zunächst anzumerken, daß trotz der mißverständlichen bzw. irreführenden Bezeichnungen, die eine Verwechslungsgefahr mit den Verbraucherbefragungen der amtlichen Statistik bzw. mit einer produktbezogenen Marktforschungsumfrage erzeugten, eine Pflicht zur Beantwortung der Fragen nicht bestand. Es handelte sich um absolut freiwillige Umfragen ohne jede Auskunftsverpflichtung. Wer etwas gegen die Nutzung seiner Daten für Marketing- und Werbezwecke hat, hat den Fragebogen vernünftigerweise erst gar nicht ausgefüllt bzw. zurückgeschickt, sondern gleich weggeworfen.

Außerdem war festzustellen, daß Firmennamen verwendet wurden, die vertrauenerweckende Assoziationen auslösen, z. B. im Fall Infas-Lifestyle mit dem u. a. aus der Wahlberichterstattung bekannten Meinungsforschungsinstut. Es handelte sich auch nicht — wie man auf den ersten Blick hätte vermuten können — um Erhebungen für eine konkrete produktbezogene Marktforschung. Bei Datenerhebungen für Zwecke der Markt- und Meinungsforschung müßten die erhobenen Daten umgehend anonymisiert werden und die Auswertungsergebnisse wären dann ohne Personenbezug. Bei diesen Umfragen war gerade dies nicht beabsichtigt. Vielmehr ging es eindeutig um die Beschaffung differenziert auswertbaren Adressmaterials für Direktwerbezwecke. Personen, die sich an derartigen Umfragen beteiligen, nehmen zwar an der ausgelobten Verlosung teil, müssen aber auch damit rechnen, verstärkt persönlich adressierte Werbepost zugeschickt zu bekommen

20.3.3 Einwilligung nur mit präziser Aufklärung

In den Anschreiben zu den beiden Umfragen wird die Art der Datenverwendung nur sehr knapp beschrieben. Infas Lifestyle hatte immerhin auf dem Fragebogen selbst eine Aufklärung zum Datenschutz aufgedruckt, in der allgemein auf die Verwendung der Daten für Marketingzwecke hingewiesen wird, und ließ sich durch Unterschrift das Einverständnis in diese Datenverarbeitung bestätigen. Bei der Claritas-Befragung wurde keine explizite Einwilligung in die Verarbeitung der Daten eingeholt, sondern vielmehr unterstellt, daß die vage Aufklärung im Anschreiben in Verbindung mit dem Ausfüllen und Rücksenden des Erhebungsbogens das Einwilligungserfordernis des Datenschutzrechts ausreichend erfüllt. Das Einverständnis für die Angaben zum Ehepartner/Partner wurde in keinem der beiden Fälle eingeholt.

Auf eine wirksame Zustimmung der Befragten kommt es aber entscheidend an. Denn: Eine gesetzliche Erlaubnis für eine Verarbeitung und Nutzung dieser Daten ohne Einwilligung sehe ich nicht; § 29 BDSG scheidet wegen der Vielzahl sensitiver Daten als Befugnisnorm für die Datenverarbeitung aus.

20.3.4 Reaktion der Aufsichtsbehörden

In den Gremien der Datenschutzaufsichtsbehörden wurden diese Umfragen bzw. Haushaltsbefragungen ebenfalls erörtert. Der Düsseldorfer Kreis, in dem die Datenschutzaufsichtsbehörden der Länder ihre Auffassung abstimmen, hat folgende Mindestanforderungen an derartige Datenerhebungen beschlossen:

— Es muß klar erkennbar sein, daß die Angaben nicht nur anonym, sondern auch personenbezogen ausgewertet werden.

— Es muß ferner erkennbar sein, für welche Zwecke die Angaben verwendet werden, z. B. für persönlich adressierte Werbung.

— Weiter muß eine unterschriebene Einwilligung auf dem Fragebogen erfolgen, und zwar von allen volljährigen bzw. einsichtsfähigen Betroffenen.

In den jüngsten BDSG-Hinweisen des Innenministeriums Baden-Württemberg, in dessen Zuständigkeit eine der genannten Firmen fällt, sind diese Mindestanforderungen weiter präzisiert worden. Beide o. a. Umfragen erfüllen diese Kriterien nicht.

20.3.5 Reaktionsmöglichkeiten der Betroffenen

Ich habe mich wegen vieler Bürger- und Medienanfragen zu diesen Haushaltsumfragen öffentlich, u. a. in einer Presseerklärung, geäußert. Viele Bürger wollten nicht nur wissen, wie sie sich verhalten sollten, sondern auch, wie sie ihre Beteiligung an diesen Datenerhebungen wieder rückgängig machen könnten. Ich habe sie über meine Einschätzung dieser Befragungsaktionen informiert und auf die Widerrufsmöglichkeit der Einwilligung und das Widerspruchsrecht aufmerksam gemacht.

Beim Widerruf der Einwilligung sollte darauf geachtet werden, daß dieser nachweisbar ist und schriftlich erfolgt und möglichst auch vom Betreiber der Umfrageaktion bestätigt wird. Das datenschutzrechtliche Widerspruchsrecht (§ 28 Abs. 3 BDSG) sieht vor, daß man als Betroffener entweder bei der speichernden Stelle, z. B. dem Betreiber der Umfrageaktionen, oder beim Empfänger der übermittelten Adreßdaten (der nur ausnahmsweise bekannt ist) der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung bzw. der Markt- und Meinungsforschung widersprechen kann. Die Daten dürfen dann nicht mehr für diese Zwecke verwendet werden; sie dürfen aber weiterhin gespeichert bleiben. In beiden Fällen, d. h. beim Widerruf der Einwilligung oder beim Widerspruch gegen die Datennutzung für Zwecke der Werbung bzw. der Markt- und Meinungsforschung, wäre die Verwendung der Daten für die genannten Zwecke unzulässig (Nutzungsverbot).

Als Aufsichtsbehörde kann ich Verstöße gegen ein solches Nutzungsverbot zwar überprüfen, sofern ich einen Datenverarbeiter feststellen kann, und meine Feststellungen einem Petenten mitteilen. Rechtlich dagegen vorgehen muß der Betroffene allerdings selbst, indem er z. B. einen Strafantrag stellt oder zivilrechtlich auf Unterlassung oder Schadensersatz klagt. Mir stehen nach der jetzigen Rechtslage — leider — keine Sanktions- und Anordnungsmöglichkeiten bei rechtswidriger Datenverarbeitung zu. Bei der Anpassung des BDSG an die EU-Richtlinie muß der Bundesgesetzgeber an dieser Stelle nachbessern und den Datenschutzaufsichtsbehörden auch Befugnisse bei unzulässigen Datenverarbeitungsvorgängen geben.

20.4 Wirtschafts- und Handelsauskunfteien — ausgewählte Beschwerdefälle

In der Bundesrepublik sind zahlreiche Wirtschafts- und Handelsauskunfteien tätig. Zu den bekanntesten gehören Creditreform, Bürgel, Dun & Bradstreet — ehemals Schimmelpfeng, Kreditschutzverein für Industrie, Handel und Dienstleistungen — IKD, und Infodata.

20.4.1 Unzureichende Benachrichtigung der Betroffenen

Immer wieder Probleme gibt es mit der Benachrichtigung der Betroffenen durch einzelne Handels- und Wirtschaftsauskunfteien. Nach dem Gesetz (§ 33 BDSG) haben die Betroffenen einen Anspruch darauf, bei erstmaliger Übermittlung ihrer Daten von dieser Datenübermittlung und der Art der übermittelten Daten benachrichtigt zu werden. Ein im Gesetz genannter Befreiungkatalog von dieser Verpflichtung kommt in diesen Fällen nicht zum Tragen. Die Benachrichtigung muß unverzüglich erfolgen, wobei die Form nicht vorgeschrieben ist. Zumeist wird schriftlich benachrichtigt. Dabei ist anzumerken, daß nur bei erstmaliger Datenübermittlung eine Benachrichtigungspflicht besteht; spätere Datenübermittlungen lösen keine Benachrichtigungspflicht mehr aus.

Ich erhalte häufig Eingaben oder Anfragen nach einer derartigen Benachrichtigung. Bei Überprüfungen mußte ich in der Vergangenheit immer wieder feststellen, daß die verwendeten Benachrichtigungsschreiben nicht den Anforderungen des BDSG entsprachen: Sie informierten nicht korrekt über die erstmalige Datenübermittlung und auch nicht über die Art der übermittelten Daten.

Vor Jahren schon hatte ich deshalb die Gremien der obersten Datenschutzaufsichtsbehörden mit dieser Sache befaßt (vgl. 18. JB, Ziff. 19.3.1). Inzwischen (Ende 1997!) haben die sehr zäh verlaufenen Gespräche zwischen den obersten Datenschutzaufsichtsbehörden und dem Verband der Handelsauskunfteien ein Muster-Benachrichtigungsschreiben erbracht, das die Intentionen des Gesetzgebers nach meinem Dafürhalten zwar immer noch nicht voll abdeckt, das aber wesentlich näher an diesen Intentionen liegt als die bisherigen ungenormten Schreiben. Die Verbandsvertreter haben zugesagt, dieses Muster künftig den Benachrichtigungschreiben der Mitgliedsunternehmen zugrunde zu legen. Es ist zu hoffen, daß zumindest die Beanstandungen wegen unzureichender Benachrichtigung der Betroffenen in dieser Branche weniger werden. Ich werde die Beachtung dieser Zusage in Bremen überprüfen.

20.4.2 Ehe als „Datengemeinschaft"?

Immer wieder erhalte ich auch Beschwerden darüber, daß in der Auskunft einer Handels- und Wirtschaftsauskunftei über einen Betroffenen Daten über dessen Ehegatten mitgeteilt werden, obwohl zu diesem nicht angefragt und kein berechtigtes Anfrageinteresse dargelegt wurde. Nach meiner Auffassung, die von den anderen Datenschutzaufsichtsbehörden geteilt wird, stellt eine Ehe keine „Datengemeinschaft" dar, was zur Folge hat, daß die Ehepartner grundsätzlich als Einzelpersonen zu betrachten und zu „beauskunften" sind; insoweit besteht kein Unterschied zu anderen Partnerschaften und Lebensgemeinschaften. Auskunftsersuchen mit der Darlegung eines berechtigten Interesses müssen sich also auf jeden einzelnen Partner beziehen. Nur in wenigen Ausnahmefällen kann von diesem Grundsatz abgewichen werden.

Gestützt wird diese Auffassung von einem Urteil des OLG Hamm (vom 4. April 1995, NJW 1996,131), in dem die Übermittlung von Informationen über die wirtschaftlichen Verhältnisse des Ehegatten einer angefragten Person nur in eng begrenzten Ausnahmefällen als zulässig angesehen wurde. Als Ausnahmefall für eine zulässige Ehegatten-Datenübermittlung wurde anerkannt, wenn der Ehegatte tatsächlich maßgeblichen Einfluß auf die Vermögensverwaltung des anderen Ehegatten nehmen und die nachgefragte Person deshalb als „Strohmann" für die eigenen Geschäfte seines Ehegatten angesehen werden kann.

Seit Jahren diskutieren die obersten Datenschutzaufsichtsbehörden dieses Problem mit dem Verband der Wirtschafts- und Handelsauskunfteien — bisher leider ohne befriedigendes Ergebnis. Im Herbst letzten Jahres wurde zwar ein Diskussionsergebnis erreicht; dieses ist aber immer noch nicht endgültig abgestimmt und erfüllt nach meiner Auffassung auch noch nicht alle oben genannten Anforderungen. Nach diesem Ergebnis soll die Übermittlung von Ehegattendaten in einer Auskunft zu einem Betroffenen in einem eingeschränkten Katalog von Fällen zulässig sein, u. a. in der o. a. „Strohmann"-Situation oder wenn der Ehepartner Funktionsträger (z. B. Prokurist) in der Firma der angefragten Person ist.

Außerdem soll, wenn das berechtigte Interesse des Auskunftsempfängers an den Ehepartnerdaten nicht zweifelsfrei erkennbar ist, die Auskunft auf die Firma und den oder die Funktionsträger beschränkt werden bzw. es darf allenfalls ein Hinweis auf die Möglichkeit der Anforderung einer separaten Auskunft gegeben werden.

Auch hier gilt wie bei den Verbraucherumfragen (vgl. o. Ziff. 20.3.): Die Datenschutzaufsichtsbehörden können nach dem BDSG bei Verstößen gegen die Zulässigkeit einer personenbezogenen Datenverarbeitung keine Anordnungen o. dgl. erlassen, sondern nur den Betroffenen ihre datenschutzrechtliche Auffassung mitteilen. Die Betroffenen müssen dann selbst entscheiden und ihre Rechte geltend machen oder u. U. Strafantrag stellen. Dieser Kompetenzmangel ist auch der Grund dafür, warum die obersten Datenschutzaufsichtsbehörden — von einzelnen Ordnungswidrigkeiten-Verfahren abgesehen — darauf beschränkt sind, z. T. über Jahre mit den Verbandsvertretern einen Kompromiß suchen zu müssen. Die Anpassung des BDSG an die EU-Richtlinie wird hier — so ist zu hoffen — Verbesserungen im Sinne einer effektiveren Kontrolle bringen.

20.4.3 Vortäuschen des „berechtigten Interesses" bei Anfragen

Immer wieder erhalte ich Eingaben von Bürgern, die sich bei mir darüber beklagen, daß von einer Auskunftei über sie Daten übermittelt worden seien, obwohl das für die Übermittlung nach § 29 Abs. 2 BDSG erforderliche berechtigte Interesse beim Empfänger der Daten nicht vorgelegen habe.

In einem Fall dieser Art, zu dem ich im vergangenen Jahr eine Eingabe erhielt, waren von einer in Bremen ansässigen Handelsauskunftei an ein Architekturunternehmen Daten über zwei Bürger übermittelt worden, obwohl das Unternehmen und die beiden Betroffenen in keinerlei Kontakt zueinander standen, der das gegenüber der Auskunftei angegebene berechtigte Interesse — Bonitätsprüfung im Hinblick auf die Anbahnung einer geschäftlichen Beziehung — hätte begründen können. Wie meine Prüfung ergab, hatte das Architekturunternehmen das Informationssystem der Auskunftei nur in Anspruch genommen, um sich ein Bild über die wirtschaftlichen Verhältnisse der ihm durch seine Tätigkeit in einem der Wohnung der Betroffenen benachbarten Haus bekannt gewordenen Personen zu machen.

In einem anderen Fall hatte die gleiche Handelsauskunftei an eine Rechtsanwaltskanzlei ebenfalls Daten mit der Zweckbegründung Bonitätsprüfung übermittelt. Bei der Überprüfung dieser Datenübermittlung begründete die Anwaltskanzlei ihre Anfrage dann jedoch mit einer Geschäftsbeziehung eines ihrer Mandanten mit dem Betroffenen und nicht, wie für das Vorliegen des berechtigten Interesses erforderlich, mit einer eigenen Geschäftsbeziehung.

In beiden Fällen hatte die Auskunftei also Daten übermittelt, obwohl das ihr mitgeteilte berechtigte Interesse für die Datenübermittlung nicht vorlag. Die Auskunftei hatte sich jeweils ohne Prüfung des Einzelfalls auf die ihr gegenüber behaupteten Angaben als „glaubhaft dargelegt" verlassen.

Die beiden vorstehenden Fälle machen wieder einmal die Gefahr deutlich, die sich im Hinblick auf das Vortäuschen des berechtigten Interesses an einer Übermittlung daraus ergibt, daß das berechtigte Interesse von den Auskunfteien wegen der hohen Fallzahl im Anfragegeschäft nur stichprobenweise, d. h. in ein bis zwei Promille aller Auskunftsfälle, bei den Auskunftsuchenden überprüft wird (vgl. hierzu auch 17. JB, Ziff. 17.2.6.).

Meine jeweiligen Prüfungsergebnisse samt datenschutzrechtlicher Beurteilung teilte ich sowohl den Betroffenen als auch der Handelsauskunftei mit. Zugleich machte ich die Betroffenen darauf aufmerksam, daß sie nunmehr selbst ihr Recht suchen müßten, indem sie z. B. Strafantrag stellen oder Schadensersatz geltend machen.

20.5 Schufa

20.5.1 Abfrage trotz Barzahlungsvereinbarung

Auch in einem die Schufa betreffenden Fall befaßte ich mich im vergangenen Jahr mit der Frage, ob für eine Datenübermittlung dieser Auskunftei beim Auskunftsempfänger das „berechtigte Interesse" als Voraussetzung für eine zulässige Anfrage bei der Schufa vorlag. Eine Bürgerin beklagte sich bei mir darüber, daß eine Mineralölhandlung, bei der sie Heizöl bestellt und mit der sie eine Bargeldzahlung zum Zeitpunkt der Lieferung des Öls vereinbart hatte, wegen ihrer Bestellung Auskünfte von der Schufa eingeholt habe. Grundsätzlich können auch Mineralölhandelsunternehmen, soweit sie an Konsumenten Warenkredite geben, Vertragspartner der Schufa werden und von dieser Auskünfte über den Betroffenen belastende Eintragungen erhalten.

Bei meiner Prüfung anläßlich der Eingabe begründete die Ölhandlung ihr Auskunftsersuchen an die Schufa damit, daß dieses erforderlich gewesen sei, um meine Petentin künftig auf Rechnung beliefern zu können. Gegenüber der Schufa hatte die Ölhandlung deshalb als berechtigtes Interesse die mögliche Gewährung eines Warenkredits geltend gemacht. Die Schufa ergänzte die Ausführungen der Ölhandlung noch dahingehend, daß ein Warenkredit, der das Vorliegen des berechtigten Interesses an einer Schufa-Auskunft begründet, im Mineralölhandel im Gegensatz zu den meisten anderen Handelszweigen bereits schon dann erteilt werde, wenn die Ölhandlung unmittelbar nach ihrer Lieferung den Kaufpreis kassiert. Der Grund hierfür sei, daß, wenn das Öl bei der Lieferung in die Tanks des Kunden eingepumpt worden sei, besondere technische Schwierigkeiten die Wiederherausgabe des eingepumpten Öls durch den Kunden bei Nichtbezahlung kaum noch zulassen würden.

Hierzu vertrat ich die Auffassung, daß bei einer Barzahlungsvereinbarung, wie sie zwischen meiner Petentin und dem Mineralölhandelsunternehmen abgeschlossen worden war, keinesfalls die Einholung einer Schufa-Auskunft gerechtfertigt werden könne. Im vorstehenden Fall hätte der Ölhändler den Preis für die verein-

barte Lieferung bereits vor dem Einpumpen des Öls in die Tanks erheben können. Die Einholung der Schufa-Auskunft war zumindest aus diesem Grund nicht erforderlich. Da auch keine Einwilligung der Betroffenen für eine Datenübermittlung durch die Schufa vorlag, war die erteilte Auskunft datenschutzrechtlich nicht zulässig. Dies teilte ich der Petentin mit.

20.5.2 Fehlende Nachmeldung berichtigter Daten

Bereits mehrmals habe ich kritisch über das Nachmelde-/Nachtragsverfahren der Auskunfteien berichtet (vgl. 17. JB, Ziff. 17.2.3.; 18. JB, Ziff. 19.3.2.).

Ein Bürger beklagte sich im vergangenen Jahr bei mir u. a. darüber, daß einer auswärtigen Bank, bei der er Kunde sei, von der Schufa ihn belastende sog. Negativmerkmale (Kündigung eines Kontos, Mahnbescheidsantrag) mitgeteilt worden seien, eine Berichtigungsmitteilung nach § 35 Abs. 6 BDSG über die Löschung dieser Merkmale wegen fehlerhafter Speicherung von der Auskunftei aber offenbar nicht vorgenommen worden sei. Durch die Nichtmitteilung der Datenlöschung sei ihm ein erheblicher Schaden entstanden. Aus dem Eingabeschreiben des Petenten war zu schließen, daß die Mitteilung der Negativmerkmale offenbar im Rahmen des Nachmeldeverfahrens der Schufa erfolgte.

Gem. § 35 Abs. 6 BDSG sind nicht-öffentliche Stellen, so auch Auskunfteien, verpflichtet, die Stellen, an die im Rahmen einer regelmäßigen Übermittlung Daten zur Speicherung weitergegeben werden, über die Berichtigung, auch Löschung unrichtiger Daten zu unterrichten, wenn dies zur Wahrung schutzwürdiger Interessen des Betroffenen erforderlich ist. Ein besonderes Gewicht hat § 35 Abs. 6 BDSG im Hinblick auf die Durchführung von Übermittlungen im Rahmen eines Nachmelde-/Nachtragsverfahrens, weil es sich hierbei stets um regelmäßige Übermittlungen zu einem Einzelfall handelt. Wenn in einem solchen Verfahren belastende Informationen über einen Betroffenen übermittelt werden und sich die Speicherung und damit auch Übermittlung dieser Informationen durch die Auskunftei im nachhinein als falsch und damit unzulässig erweisen, bedarf es nach der gesetzlichen Anforderung einer entsprechenden Mitteilung an die Empfänger derartiger Nachmeldungen bzw. Nachträge, zu denen im Fall der Schufa in erster Linie Banken und Sparkassen zählen.

Ich bat die Schufa um eine Stellungnahme zu ihrem Vorgehen. Da der Betroffene in der Zwischenzeit Klage auf Schadensersatz erhoben hatte, erklärte sich die Schufa hierzu mit dem Hinweis auf das schwebende Verfahren nicht bereit.

20.6 Mietenkataster — nur mit Einverständnis der Mieter

Nach § 2 Abs. 1 des Gesetzes über die Miethöhe (MHG) kann der Vermieter die Erhöhung der Miete bis zur Höhe der ortsüblichen Vergleichsmiete verlangen und zur Begründung auf Mietspiegel, Sachverständigengutachten oder Vergleichswohnungen Bezug nehmen. Nach Auskunft des Senators für Bau, Verkehr und Stadtenwicklung hat eine Bund-Länder-Arbeitsgruppe zur Reform des Mietrechts darüber diskutiert, zur Verstärkung der Akzeptanz von Mietspiegeln diesen bei Erhöhungsbegehren des Vermieters einen Begründungsvorrang einzuräumen. Er hat mir den Zwischenbericht dieser Arbeitsgruppe (Stand: 22. 10. 1997) zur Stellungnahme vorgelegt, da die Einführung eines Mietspiegels oder einer Mietdatenbank für die Stadtgemeinde Bremen vorgesehen ist.

In meiner ausführlichen Stellungnahme habe ich Verfahren zur Erstellung und Führung von Mietspiegeln und Mietdatenbanken vorgeschlagen, in denen die Verarbeitung personenbezogener Mieterdaten ohne Einwilligung der Betroffenen nicht erforderlich wäre. Die senatorische Behörde hat meine Stellungnahme an das Bundesministerium der Justiz sowie wegen der für Bremen erwogenen Aufstellung eines Mietspiegels oder einer Mietdatenbank an die zuständigen Stellen gesandt.

Inzwischen hat mich der Mieterverein Bremen darüber unterrichtet, daß Verhandlungen zwischen den Verbänden der Mieterschaft und der Vermieterschaft, der Wohnungswirtschaft und der Stadtgemeinde Bremen über die gemeinsame Gründung eines Vereins geführt werden, der Mieten für nicht preisgebundenen Wohnraum sammeln, auswerten sowie hierüber Auskunft erteilen soll. Es sei beabsichtigt, daß der Verein auf besondere Anfrage auch Auskunft über identifizierbare Vergleichswohnungen erteilen soll. Weil nach Angaben des Mietervereins die Sammlung dieser Daten sowie die Auskunftserteilung hierüber nur

auf freiwilliger Basis, nämlich nur mit ausdrücklicher Zustimmung sowohl des jeweiligen Vermieters als auch des Mieters erfolgen soll, besteht die Vorstellung, in die jeweiligen Formularmietverträge eine entsprechende Einverständnisklausel beider Parteien aufzunehmen.

Ich habe datenschutzrechtliche Bedenken sowohl generell gegen die standardisierte Form der Einwilligungserklärung als auch gegen die mir vorgelegte Textfassung geäußert. Sie beziehen sich zum einen auf die Voraussetzung der Freiwilligkeit angesichts der Abhängigkeit des Mieters, der auf eine Wohnung als wesentliche Existenzgrundlage angewiesen ist, zum anderen auf die mangelnde Genauigkeit der Beschreibung der Verarbeitungsvorgänge, denen zugestimmt werden soll, und der Datenempfänger.

Die Einwilligungserklärung des Mieters gegenüber dem Vermieter zur Weitergabe auf seine identifizierbare Wohnung bezogener Angaben muß m. a. W. präzise formuliert sein und gilt nur für den jeweiligen einzelnen Übermittlungsfall.

Der Mieterverein teilt meine Auffassung und hat erklärt, daß vor der Gründung des Vereins „Mietenkataster Bremen e. V." alle hiermit zusammenhängenden datenschutzrechtlichen Probleme geklärt werden müßten. Ende Januar 1998 hat ein erstes Gespräch einiger der an diesem Projekt Beteiligten stattgefunden. Ergebnis dieses Gesprächs war, daß zunächst das Amt für Wohnung und Städtebauförderung eine Einwilligungserklarung formulieren soll, die den datenschutzrechtlichen Anforderungen entspricht.

20.7 Archivierung von Beschäftigtendaten bei Konkurs

20.7.1 Rechtslage

Der damalige Betriebsrat der Bremer Vulkan Werft GmbH i. K. hat mich im Juli 1997 um Beratung gebeten, welche Anforderungen beachtlich sind, um die Arbeitsschutz- und Gesundheitsdaten der ehemaligen Beschäftigten über die Betriebsstillegung hinaus zu sichern, die sowohl der Arbeitgeber als auch der Arbeitssicherheitsausschuß des Betriebsrats gespeichert haben. Die Daten sind u. a. in Unfallanzeigen und -aufnahmen, Berufskrankheiten- sowie Asbestmeldungen, Unterlagen über Schulungen der Mitarbeiter, Listen der Ersthelfer und Sicherheitsbeauftragten und in genauen Analysen bemerkenswerter Unfälle enthalten.

Nach Beendigung der Tätigkeit des Bremer Vulkan endeten die Arbeitsverhältnisse der Beschäftigten mit dem Unternehmen, so daß die Verarbeitung der Arbeitnehmerdaten nach § 28 Abs. 1 Satz 1 Nr. 1 Bundesdatenschutzgesetz (BDSG) für die Durchführung der Arbeitsverträge nicht mehr erforderlich ist. Daraus könnte man schließen, daß der Konkursverwalter, der nach § 6 Abs. 2 Konkursordnung (KO) das Verwaltungs- und Verfügungsrecht über die Konkursmasse ausübt, die Daten nach § 35 Abs. 2 Nr. 3 BDSG zu löschen hat. Allerdings tritt nach Abs. 3 dieser Vorschrift an die Stelle der Löschung eine Sperrung der Daten, soweit Grund zu der Annahme besteht, daß durch eine Löschung schutzwürdige Interessen der Betroffenen beeinträchtigt werden, oder soweit gesetzliche Aufbewahrungsfristen entgegenstehen. Gesperrte Daten dürfen ohne Einwilligung nur unter engen Voraussetzungen (§ 35 Ab. 7 BDSG) übermittelt oder genutzt werden.

Die Sperrungsvoraussetzungen liegen hinsichtlich der Arbeitsschutz- und Gesundheitsdaten vor. Schutzwürdige Interessen der Mitarbeiter an der weiteren Aufbewahrung bestehen, weil diese Daten u. a. Aufschluß darüber geben können, ob spätere Erkrankungen betriebsbedingt sein können, und insoweit gewährleistet sein muß, daß die Beschäftigten evtl. Rechtsansprüche z. B. gegen die Berufsgenossenschaft geltend machen können.

Des weiteren sind bereichsspezifische Regelungen beachtlich. So sind z. B. nach § 34 Abs. 3 Satz 2 Gefahrstoffverordnung (GefStoffV) bei Vorsorgeuntersuchungen dem Arbeitnehmer der ihn betreffende Auszug aus der Vorsorgekartei und die ärztlichen Bescheinigungen auszuhändigen. Hierzu hat mir der Konkursverwalter erklärt, diese Unterlagen seien teilweise den Betroffenen ausgehändigt worden und würden teilweise zu den Personalakten genommen.

Außerdem sind die personenbezogenen Daten beim Arbeitsmediziner nach der Berufsordung für Ärzte im Lande Bremen zehn Jahre aufzubewahren. Dies gilt auch nach Beendigung der Tätigkeit.

20.7.2 Empfehlungen und weitere Schritte

Soweit die nicht ausgehändigten Unterlagen archiviert werden sollen, habe ich angeregt, daß die beteiligten Stellen (z. B. Konkursverwalter, ehemalige Betriebsratsangehörige, Senator für Arbeit, Arbeitsamt) festlegen

- die Zweckbindung, d. h. Zweck der Archivierung ist ausschließlich die Sicherung der Datenbestände, um schutzwürdige Interessen der Betroffenen zu wahren,
- die frühzeitige Unterrichtung der Betroffenen über Verantwortliche und Konzept der Archivierung und über ihre Einsichts-, Auskunfts- und sonstigen Nutzungsrechte,
- die Beendigung der Archivierung.

Inzwischen hat der Konkursverwalter mitgeteilt, es sei beabsichtigt, die arbeitsmedizinischen Untersuchungsergebnisse bzw. Krankenakten sowie die Personalakten einer treuhänderischen Stelle zur Aufbewahrung und ggf. Bescheinigungserstellung zu übergeben.

Zugleich streben die Vereine „Arbeit und Zukunft" und „Wir Vulkanesen" — beides Zusammenschlüsse von Betroffenen und engagierten Mitbürgern zur Bewältigung der sozialen Folgen des Vulkan-Konkurses -, die IG Metall, die Bremische Evangelische Kirche und das Zentrum für Sozialpolitik der Universität Bremen an, die Unterlagen zu archivieren und sie im Interesse der einzelnen Betroffenen (Beratung, Verfolgung von Rechtsansprüchen) bzw. für die Forschung (gesundheitliche Folgen von Schadstoffbelastungen am Arbeitsplatz und von Arbeitslosigkeit) zur Verfügung zu halten. Träger des Archivs soll „Arbeit und Zukunft" sein.

Ich habe den Beteiligten empfohlen, unverzüglich Kontakt mit dem Konkursverwalter aufzunehmen, ihnen die datenschutzrechtlichen Rahmenbedingungen für ihr Vorhaben erläutert und erklärt, ich sei bereit, sie weiterhin zu beraten und das Vorhaben zu begleiten.

21. Meldepflichtige Stellen: Statistische Übersicht und Prüfergebnisse

21.1 Statistische Übersicht

Die Zahl der Stellen, die mir zum Register nach § 32 BDSG gemeldet sind, hat sich im Berichtszeitraum wiederum leicht erhöht. Insgesamt weist das Register Anfang Januar 1998 124 Stellen gegenüber 122 Stellen im Vorjahr aus. Davon befinden sich 105 Stellen in Bremen und 19 Stellen in Bremerhaven. Der regionale Schwerpunkt liegt also eindeutig in Bremen. Die Mehrzahl der angemeldeten Stellen ist dem Bereich der Servicebetriebe zuzuordnen, insbesondere den DV- und Telekommunikations-Dienstleistungsanbietern.

Das Register nach § 32 BDSG ist kein Selbstzweck. Ursprünglich gedacht zur Information der Betroffenen, ist es heute Grundlage und wesentliche Orientierung für meine Prüftätigkeit nach § 38 Abs. 2 BDSG. Die Entwicklung im Bereich der Informations- und Kommunikationstechnik, die Dezentralisierung der Datenverarbeitung, die Auslagerung von DV-Aktivitäten sowie neuartige DV- und TK-Dienstleistungen führen zu häufigen Änderungen im Register. Änderungen ergeben sich auch dadurch, daß ich — ohne gesetzlich dazu verpflichtet zu sein — Datenverarbeiter, bei denen ich aufgrund von Handelsregistereintragungen oder von Branchenzuordnungen eine Meldepflicht vermute, anschreibe und um Prüfung ihrer Meldepflicht (die ja bußgeldbewehrt ist) bitte. Bei einigen der angeschriebenen Firmen ergibt sich dann jeweils, daß tatsächlich meldepflichtige Tätigkeiten ausgeübt werden, die dann zu einer Registereintragung führen.

Einzelheiten zum Stand des Registers zeigt die nachfolgende Übersicht:

Art der Tätigkeit	insgesamt	Bremen	Bremerhaven
1. Speicherung personenbezogener Daten zum Zwecke der Übermittlung (insgesamt)	**7**	**5**	**2**
— Auskunfteien	5	4	1
— Adreßverlage/Adreßhändler	2	1	1
2. Speicherung personenbezogener Daten zum Zwecke der anonymisierten Übermittlung (insgesamt)	**3**	**3**	
— Markt- u. Meinungsforschung	3	3	
3. Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (insgesamt)	**114**	**95**	**19**
— Datenerfassung	7	7	
— Dienstleistung/Rechenzentren	87	72	15
— Mikroverfilmer	4	4	
— Mailboxdienste	9	5	4
— Datenlöschung/Datenträgervernichtung	7	7	
Gesamt	**124**	**105**	**19**

21.2 Prüfergebnisse

Ich habe im Berichtszeitraum bei insgesamt 14 meldepflichtigen Stellen einfache Registerprüfungen durchgeführt; eine dieser Stellen bestand dabei aus mehreren rechtlich selbständigen, personell, organisatorisch und finanziell jedoch verflochtenen Gesellschaften. Zusätzlich habe ich bei zwei großen Service-Rechenzentren die im Vorjahr begonnenen und im wesentlichen auch durchgeführten umfassenderen Datenschutzprüfungen abgeschlossen.

Bei den einfachen Registerprüfungen überprüfe ich lediglich das Bestehen einer Meldepflicht nach § 32 BDSG sowie den Inhalt der Meldung, die Bestellung und Tätigkeit des betrieblichen Datenschutzbeauftragten nach den §§ 36/37 BDSG, die Verpflichtung der Mitarbeiter auf das Datengeheimnis gemäß § 5 BDSG und die Beachtung der Regelungen zur Auftragsdatenverarbeitung nach § 11 BDSG. Technisch-organisatorische Sicherungsmaßnahmen sowie die Zulässigkeit der personenbezogenen Datenverarbeitung werden hierbei nicht geprüft; sie bleiben gesonderten Prüfungen vorbehalten. Dabei ist darauf hinzuweisen, daß die Zulässigkeit der personenbezogenen Datenverarbeitung, die bei den gemeldeten Auftragsdatenverarbeitern stattfindet, von den jeweiligen Auftraggebern datenschutzrechtlich zu verantworten ist und daß die anlaßbezogenen Einzelfallprüfungen nach § 38 Abs.1 BDSG meist Zulässigkeitsfragen der Datenverarbeitung zum Gegenstand haben.

Bei meinen Überprüfungen habe ich auch dieses Jahr wieder Mängel feststellen müssen; in einem Fall habe ich ein Ordnungswidrigkeiten-Verfahren eingeleitet. Die wesentlichen Mängel lagen wiederum im Bereich der Registermeldungen (z. B. Aktualität der Meldung, fehlende Abmeldung, fehlende Ergänzungsmeldung), beim betrieblichen Datenschutzbeauftragten (z. B. fehlende schriftliche Bestellung, Bündelung von Funktionen) und bei den Verpflichtungen der Mitarbeiter auf das Datengeheimnis. Bei zwei Stellen (Adreßverlag sowie Firmenkonglomerat zur Adreßsammlung/Auskunftei) stellte sich heraus, daß es sich ganz offensichtlich um unseriöse Firmen handelte (vor denen z. B. Verbraucherschutzverbände, Kammern bzw. der Bundesanzeiger warnten). Datenschutzbestimmungen z. B. zur Zulässigkeit der Datenverarbeitung waren in einem dieser Fälle gänzlich unbekannt, im anderen Fall zwar bekannt, im praktischen Vollzug jedoch ohne Beachtung.

22. Die Entschließungen der Datenschutzkonferenz im Jahr 1997

22.1 Beratungen zum StVÄG 1996

Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Entwicklung, im Gesetzgebungsverfahren zu einem Strafverfah-

rensänderungsgesetz 1996 die Gewährleistung der informationellen Selbstbestimmung im Strafverfahren nicht nur nicht zu verbessern, sondern vielmehr bestehende Rechte sogar noch zu beschränken. Dies gilt insbesondere für den Beschluß des Bundesrates, der gravierende datenschutzrechtliche Verschlechterungen vorsieht.

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

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

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

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

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

Beispiele hierfür sind:

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

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

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

22.2 Genetische Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke

Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997

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

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

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

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

Dieser Gefährdung kann dadurch begegnet werden, daß bei Bekanntwerden von Überschußinformationen durch die bisherigen Untersuchungsmethoden andere Untersuchungmethoden (Analyse eines anderen Genomabschnitts) verwendet werden, die keine Informationen über die genetische Disposition liefern. Derartige Ausweichstrategien können jedoch zur Folge haben, daß die mit anderen Methoden erlangten Untersuchungsergebnisse nicht mit bereits vorliegenden vergleichbar sind. Datenspeicherungen über verformelte Untersuchungsergebnisse könnten daher dazu führen, daß einmal verwendete Untersuchungsformen im Interesse der Vergleichbarkeit beibehalten werden, obwohl sie sich als problematisch herausgestellt haben und unproblematische Alternativen zur Verfügung stehen, z. B. durch Verschlüsselung problematischer Informationen.

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

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

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

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

   — Nicht jede DNA-Analyse, die zum Zweck der Aufklärung einer konkreten Straftat erfolgt ist, darf in diese Datei aufgenommen werden. Die Speicherung von Verformelungen der DNA-Struktur in eine Datenbank darf nur dann erfolgen, wenn tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte künftig strafrechtlich in Erscheinung treten wird und daß die Speicherung aufgrund einer Prognose unter Zugrundelegung des bisherigen Täterverhaltens die künftige Strafverfolgung fördern kann.

   — Eine Speicherung kommt insbesondere dann nicht in Betracht, wenn der Tatverdacht gegen den Beschuldigten ausgeräumt wurde. Bereits erfolgte Speicherungen sind zu löschen. Gleiches gilt für den Fall, daß die Anordnung der DNA-Untersuchung oder die Art und Weise ihrer Durchführung unzulässig war.

   — Die Aufbewahrungsdauer von Verformelungen der DNA-Struktur ist konkret festzulegen (z. B. gestaffelt nach der Schwere des Tatvorwurfs).

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

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

22.3 Geplante Verpflichtung von Teledienstеanbietern, Kundendaten an Sicherheitsbehörden zu übermitteln

Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997

Der Entwurf der Bundesregierung für ein Teledienstedatenschutzgesetz (Artikel 2 [§ 5 Absatz 3] des Informations- und Kommunikationsdienste-Gesetzes vom 20. Dezember 1996 — BR-Drs. 966/96) sieht vor, daß die Anbieter von Telediensten (z. B. Home-Banking, Home-Shopping) dazu verpflichtet werden sollen, insbesondere der Polizei und den Nachrichtendiensten Auskunft über Daten zur Begründung, inhaltlichen Ausgestaltung oder Änderung der Vertragsverhältnisse mit ihren Kunden (sog. Bestandsdaten) zu erteilen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Aufnahme einer solchen Übermittlungsvorschrift in das Teledienstedatenschutzgesetz des Bundes. Eine Folge dieser Vorschrift wäre, daß Anbieter von elektronischen Informationsdiensten (z. B. Diskussionsforen) offenlegen müßten, welche ihrer Kunden welche Dienste z. B. mit einer bestimmten politischen Tendenz in Anspruch nehmen. Darin läge ein massiver Eingriff nicht nur in das Recht auf informationelle Selbstbestimmung, sondern auch in die Informations- und Meinungsfreiheit des Einzelnen. Das geltende Recht, insbesondere die Strafprozeßordnung und das Polizeirecht, enthalten hinreichende Möglichkeiten, um strafbaren und gefährlichen Handlungen auch im Bereich der Teledienste zu begegnen. Über die bisherige Rechtslage hinaus würde bei Verabschiedung der geplanten Regelung zudem den Nachrichtendiensten ein nichtöffentlicher Datenbestand offenstehen. In keinem anderen Wirtschaftsbereich sind vergleichbare Übermittlungspflichten der Anbieter von Gütern und Dienstleistungen hinsichtlich ihrer Kunden bekannt.

Mit guten Gründen haben deshalb die Länder davon abgesehen, in den inzwischen von den Ministerpräsidenten unterzeichneten Staatsvertrag über Mediendienste eine vergleichbare Vorschrift aufzunehmen. In der Praxis werden sich aber für Bürger und Online-Dienstanbieter schwierige Fragen der Abgrenzung zwischen

den Geltungsbereichen des Mediendienstestaatsvertrags und des Teledienstedatenschutzgesetzes ergeben. Auch aus diesem Grund halten die Datenschutzbeauftragten eine Streichung der Vorschrift des § 5 Absatz 3 aus dem Entwurf für ein Teledienstedatenschutzgesetz für geboten.

22.4 Achtung der Menschenrechte in der Europäischen Union

Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997

Die DSB-Konferenz ist gemeinsam der Überzeugung, daß hinsichtlich nicht Verdächtiger und hinsichtlich nicht kriminalitätsbezogener Daten die Forderung des Europäischen Parlaments vom 17. September 1996 zu den Dateien von Europol unterstützt werden soll.

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

22.5 Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen

Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997

Die Datenschutzbeauftragten des Bundes und der Länder halten es für sehr problematisch, daß in Folge technischer und gesellschaftlicher Veränderungen in einer zunehmenden Anzahl von Konstellationen personenbezogene medizinische Patientendaten außerhalb des ärztlichen Bereiches verarbeitet werden. Sie fordern, daß zunehmend die Möglichkeiten einer anonymen oder pseudonymen Datenverarbeitung mit Verschlüsselung genutzt werden. Soweit dennoch Patientendaten personenbezogen weitergegeben werden, ist ein wesentliches Problem, daß außerhalb des ärztlichen Gewahrsams der von der Strafprozeßordnung vorgesehene Schutz personenbezogener Patientendaten vor Inanspruchnahme als Beweismittel durch Zeugeneinvernahme oder Beschlagnahme nicht mehr zweifelsfrei sichergestellt ist bzw. überhaupt nicht existiert.

Die folgenden Beispiele machen dies deutlich:

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

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

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

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

Die zunehmende Verlagerung personenbezogener Patientendaten aus dem Schutzbereich des Arztgeheimnisses nach außen verstößt nach Ansicht der Datenschutzbeauftragten massiv gegen Interessen der betroffenen Patienten, solange nicht ein gleichwertiger Schutz gewährleistet ist.

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

22.6 Novellierung des Bundesdatenschutzgesetzes und Modernisierung des Datenschutzrechts

Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997

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

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

Für die Entwicklung des Datenschutzes ist diese Lage höchst nachteilig:

— Verbesserungen des Datenschutzes der Bürger, z. B. durch genauere Information über die Verarbeitung ihrer Daten, verzögern sich;

— dem Datenschutzrecht droht Zersplitterung, weil den Ländern eine Orientierung für die Anpassung der Landesdatenschutzgesetze fehlt.

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

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

— weitgehende Gleichbehandlung des öffentlichen und des privaten Bereichs bei gleichzeitiger Verbesserung der Datenschutzkontrolle, insbesondere durch generell anlaßunabhängige Kontrolle und durch die ausdrückliche Festlegung der völligen Unabhängigkeit der Aufsichtsbehörden und die Erweiterung ihrer Eingriffsbefugnisse;

— Bestellung weisungsfreier Datenschutzbeauftragter auch bei öffentlichen Stellen mit dem Recht, sich jederzeit an den Bundes- oder Landesbeauftragten für den Datenschutz zu wenden;

— Bürgerfreundlichkeit durch einfache und verständliche Formulierung des BDSG, z. B. durch einen einheitlichen Begriff der Verarbeitung personenbezogener Daten entsprechend der Richtlinie;

— Gewährleistung eines einheitlichen, hohen Datenschutzniveaus durch Beibehaltung der Funktion des BDSG und der Landesdatenschutzgesetze als Querschnittsgesetze sowie durch Vermeidung eines Gefälles zwischen den Bereichen, die der EG-Datenschutzrichtlinie unterfallen, und den übrigen Gebieten, deren Datenschutzregelungen nicht verschlechtert werden dürfen;

— Sonderregelungen für Presse und Rundfunk nur, soweit zur Sicherung der Meinungsfreiheit notwendig.

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

— Verbindliche Grundsätze für die datenschutzfreundliche Gestaltung von Informationssystemen und -techniken, so zur Datensparsamkeit, zur Anonymisierung und Pseudonymisierung, zur Verschlüsselung und zur Risikoanalyse;

— mehr Transparenz für die Verbraucher und mehr Eigenständigkeit für die Anbieter durch Einführung eines Datenschutzaudits;

— Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen, Regelung der Video-Überwachung;

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

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

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

Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997

Überlegungen des Gesetzgebers und eine beginnende öffentliche Diskussion, moderne Dokumentationstechnik der Wahrheitsfindung und dem Zeugenschutz in gerichtlichen Verfahren nutzbar zu machen, liegen auch im Interesse des Datenschutzes. Dabei ist allerdings zu beachten, daß Bild-Ton-Aufzeichnungen von Vernehmungen im Strafverfahren einen erheblichen Eingriff in das Persönlichkeitsrecht darstellen. Sie spiegeln die unmittelbare Betroffenheit der Beschuldigten oder Zeugen in Mimik und Gestik umfassend wider. Zweck und Erforderlichkeit dieses Eingriffs bedürfen einer sorgfältigen Begründung durch den Gesetzgeber. Sie bildet den Maßstab, der über Möglichkeiten, Grenzen und Verfahren der Videotechnologie im Strafprozeß entscheidet. Erkennbar und nachvollziehbar sollte sein, daß der Gesetzgeber die Risiken des Einsatzes dieser Technologie, insbesondere die Verfügbarkeit der Aufzeichnungen nach den allgemeinen Vorschriften über die Beweisaufnahme, bedacht und bewertet hat. Ferner sollte erkennbar und nachvollziehbar sein, daß Alternativen zur Videotechnologie, namentlich die Verwendung von Tonaufzeichnungen, in die Erwägungen des Gesetzgebers aufgenommen wurden.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sollten die vorliegenden Gesetzentwürfe des Bundesrates (BT-Drs. 13/4983 vom 19. Juni 1996) sowie der Fraktionen der CDU/CSU und F.D.P. (BT-Drs. 13/7165 vom 11. März 1997) in einem umfassenderen Bedeutungs- und Funktionszusammenhang diskutiert werden. Zunehmend tritt das Anliegen der Praxis hervor, Bild-Ton-Aufzeichnungen auch mit anderer Zielsetzung zu verwerten:

Bild-Ton-Aufzeichnungen ermöglichen eine vollständige und authentische Dokumentation nicht nur des Inhalts, sondern auch der Entstehung und Begleitumstände einer Aussage. Die Beurteilung ihres Beweiswerts wird dadurch deutlich verbessert. Zugleich dient eine nur einmalige Vernehmung, die möglichst zeitnah zum Tatgeschehen durchgeführt und aufgezeichnet wird, der Wahrheitsfindung und erhöht die Qualität der gerichtsverwertbaren Daten („Vermeidung kognitiver Dissonanzen"). Ausgehend von diesen Überlegungen, hat der Gesetzgeber unter Einbeziehung von Erkenntnissen der Vernehmungspsychologie zu prüfen, ob und

inwieweit eine wortgetreue Abfassung von Vernehmungsniederschriften ausreicht und eine Aufzeichnung der Aussage nur im Wort auf Tonband für die Zwecke des Strafverfahrens in ihrer Beweisqualität der Videotechnologie sogar überlegen ist.

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

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

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

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

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

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

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

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

22.8. Erforderlichkeit datenschutzfreundlicher Technologien

Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997

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

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

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

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

Vom Gesetzgeber erwarten die Datenschutzbeauftragten des Bundes und der Länder, daß er die Verwendung datenschutzfreundlicher Technologien durch Schaffung rechtlicher Rahmenbedingungen forciert. Sie begrüßen, daß sowohl der Mediendienstestaatsvertrag der Länder als auch das Teledienstedatenschutzgesetz des Bundes bereits den Grundsatz der Datenvermeidung normieren. Der in den Datenschutzgesetzen des Bundes und der Länder festgeschriebene Grundsatz der Erforderlichkeit läßt sich in Zukunft insbesondere durch Berücksichtigung des Prinzips der Datensparsamkeit und der Verpflichtung zur Bereitstellung anonymer Nutzungsformen verwirklichen. Die Datenschutzbeauftragten des Bundes und der Länder bitten darüber hinaus die Bundesregierung, sich im europäischen Bereich dafür einzusetzen, daß die Förderung datenschutzfreundlicher Technologien entsprechend dem Vorschlag der Kommission in das 5. Rahmenprogramm „Forschung und Entwicklung" aufgenommen wird.

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

22.9 „Verbesserter Datenaustausch bei Sozialleistungen"

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 20. Oktober 1997 zu den Vorschlägen der Arbeitsgruppe der ASMK

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

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

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

Diese Verfahren der Datenerhebung sind mit jeweils unterschiedlich schwerwiegenden Eingriffen in das Persönlichkeitsrecht der Betroffenen verbunden. So weiß z. B. bei einer Datenerhebung beim Betroffenen dieser, wer wann welche Daten zu welchem Zweck über ihn erhebt, und Dritte erhalten keine Kenntnis von diesen Datenerhebungen.

Im Gegensatz dazu wird bei einer Datenerhebung bei Dritten ohne Mitwirkung des Betroffenen dieser darüber im unklaren gelassen, wer wann welche Daten zu welchem Zweck über ihn erhebt, und Dritten werden Daten über den Betroffenen zur Kenntnis gegeben (z. B. der Bank die Tatsache, daß der Betroffene Sozialhilfeempfänger ist).

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

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

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

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

Bezugnehmend auf die bisherigen Äußerungen des BfD und von LfDs bestehen gegen folgende Vorschläge im Bericht gravierende Bedenken:

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

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

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

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

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

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

Die Datenschutzbeauftragten teilen nicht die Auffassung, daß Stichproben nach der geltenden Rechtslage zu § 21 Abs. 4 SGB X möglich sind. 21 Abs. 4 SGB X

ist eine Auskunftsvorschrift für die Finanzbehörden, die über die Datenerhebungsbefugnis der Sozialleistungsträger nichts aussagt. Die Leistungsträger dürfen diese Auskünfte bei den Finanzbehörden als Dritten nur nach Maßgabe des § 67 a SGB X einholen, soweit das erforderlich ist: Diese Erforderlichkeit setzt Anhaltspunkte für Leistungsmißbrauch im Einzelfall voraus.

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

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

Die Annahme in der Begründung des Vorschlags, ohne eine derartige Auskunftspflicht bestünden keine sachgerechten Ermittlungsmöglichkeiten, trifft nicht zu. Der Betroffene ist verpflichtet, Nachweise zu erbringen; dazu können auch Bankauskünfte gehören. Allerdings ist dem Betroffenen vorrangig Gelegenheit zu geben, solche Auskünfte selbst und ohne Angabe ihres Verwendungszwecks beizubringen. Nur soweit dennoch erforderlich, ist der Betroffene im Rahmen seiner Mitwirkungspflicht gehalten, sein Einverständnis in die Erteilung von Bankauskünften zu geben.

Die vorgeschlagene pauschale Auskunftsverpflichtung birgt deshalb die Gefahr in sich, daß dann generell ohne Mitwirkung des Betroffenen und ohne sein Einverständnis sofort an die Bank/Lebensversicherung herangetreten wird mit der Wirkung, daß der Betroffene desavouiert wird.

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

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

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

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

23. Informationen zum Datenschutz

Die nachfolgende Übersicht erhebt nicht den Anspruch auf Vollständigkeit, bietet aber doch viele nützliche Adressen für Abrufe aus dem Internet zum Thema Datenschutz. Eine Gewähr für die Richtigkeit der Angaben kann nicht übernommen werden.

23.1. WWW-Adressen

Allgemeine Informationen und Verweise finden sich unter:

http://www.datenschutz.de

Tätigkeitsberichte einiger Datenschutzbeauftragter

http://www.itsoft.de/html/berichte.html

Der direkte Zugriff auf meine letzten Jahresberichte jeweils als gepacktes Window-Dokument findet sich unter:

http://www.itsoft.de/download/bremen96.zip (19. Jahresbericht)

http://www.itsoft.de/download/bremen95.zip (18. Jahresbericht)

http://www.itsoft.de/download/bremen94.zip (17. Jahresbericht)

http://www.itsoft.de/download/bremen93.zip (16. Jahresbericht)

Hamburger Datenschutzhefte — Datenschutz bei Multimedia und Telekommunikation

http://www.hamburg.de/Behoerden/HmbDSB/Material/hamdat.htm

Materialien des Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder:

— **Arbeitspapier Datenschutzfreundliche Technologien — Privacy Enhancing Technology PET**

http://www.datenschutz-berlin.de/to/datenfr.htm

— **Arbeitspapier Datenschutzfreundliche Technologien in der Telekommunikation:**

http://www.datenschutz-berlin.de/to/tk/ds_123.htm

— **Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet:**

http://www.datenschutz-berlin.de/jahresbe/95/sonstige/inhinter.htm

Ergebnisse der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

http://www.datenschutz-berlin.de/sonstige/konferen/konf-de.htm

Die Adressen der Landesbeauftragten für den Datenschutz:

httm://www.datenschutz-berlin.de/sonstige/behoede/ldbauf.htm

Die Adressen der Aufsichtsbehörden für den Datenschutz

http://www.datenschutz-berlin.de/sonstige/behoerde/aufsicht.htm

Infomationen über den Datenschutz im Gesundheitswesen

http://ourworld.compuserve.com/homepages/gesundheitsdatenschutz

Gesetze und datenschutzrechtliche Regelungen auf Bundesebene:

http://datenschutz-berlin.de/gesetze/bund.htm

— **Telekommunikationsgesetz:**

http://www.datenschutz-berlin.de/gesetze/berlin/tkg/tkg.htm

— **Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG)** (Art. 1: Teledienstegesetz, Art. 2 Teledienstedatenschutzgesetz, Artikel 3 Signaturgesetz und weiter Artikel)

http://www.datenschutz-berlin.de/gesetze/medien/iukdg.htm

Mediendienstestaatsvertrag:

http://www.datenschutz-berlin.de/gesetze/berlin/medien/medsta.htm

23.2 Verfügbare Broschüren und Faltblätter

Folgende Publikationen können bei mir angefordert werden:

— Bremisches Datenschutzgesetz
— Der betriebliche Datenschutzbeauftragte
— Tips zum Adressenhandel und gegen die Werbepapierflut im Briefkasten
— Mobilfunk und Datenschutz
— Handels- und Wirtschaftsauskunfteien
— Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffenlichen Verwaltung an das Internet
— Handys — Komfort nicht ohne Risiko
— Bundesdatenschutzgesetz (BfD — Info 1)
— Der Bürger und seine Daten (BfD — Info 2)
— Schutz der Sozialdaten (BfD — Info 3)
— Der behördliche Datenschutzbeauftragte (BfD — Info 4)