FREIE HANSESTADT BREMEN

Landesbeauftragter für den Datenschutz

19. Jahresbericht

Vorgelegt zum 31. März 1997

BREMISCHE BÜRGERSCHAFT
Landtag
14. Wahlperiode

Drucksache 14/627
15.04.97

19. Jahresbericht des Landesbeauftragten für den Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats meinen 19. Bericht über das Ergebnis meiner Tätigkeit im Jahre 1996 zum 31. März 1997 (§ 33 Abs. 1 Bremisches Datenschutzgesetz — BrDSG).

Dr. Stefan Walz, Landesbeauftragter für den Datenschutz

Inhaltsübersicht

1. Vorwort

1.1 Datenschutz durch Technikgestaltung

In der aktuellen öffentlichen Diskussion über Ausgestaltung und Zukunft der Informationsgesellschaft dominieren die Grundsatzfragen nach Chancen und Gefahren einer tendenziell weltweiten Vernetzung und nach den Möglichkeiten, das Recht auf informationelle Selbstbestimmung auch in einer künftig völlig veränderten Techniklandschaft zu bewahren. Daß und wie Datenschutz als Kernelement einer verfassungs- und sozialverträglichen Technikgestaltung im Zeitalter von INTERNET und Multimedia konzipiert werden müßte, habe ich in der Einleitung zum 18. Jahresbericht zu skizzieren versucht (vgl. 18. JB., Ziff. 2). „Präventiver Datenschutz" durch frühzeitige Definition von Anforderungen an System- und Verfahrensplanungen und unter Einsatz datenschutzfreundlicher Informations- und Kommunikationstechnologien (Privacy Enhancing Technologies) wird zum zukunftsweisenden Konzept auch und gerade für die Datenschutzinstitutionen.

Die Konferenz der Datenschutzbeauftragten legt auf diesen Ansatz einen Schwerpunkt ihrer Arbeit. Konsequenterweise hat sie im Berichtsjahr mehrere Beschlüsse mit datenschutzfreundlichen Anforderungen an die Systemgestaltung gefaßt. So haben meine Kollegen und ich uns u. a. für anonyme Zugangsmöglichkeiten zu Mediendiensten und beim digitalen Fernsehen, für erhöhte Sicherheit bei der elektronischen Datenübertragung und gegen ein Verschlüsselungsverbot ausgesprochen (vgl. die Entschließungstexte Ziff. 20.4, 20.5 und 20.6).

Entsprechende Vorschläge der Datenschutzbeauftragten haben inzwischen Niederschlag gefunden in den von Bund und Ländern vorbereiteten und zur Zeit in den gesetzgebenden Körperschaften beratenen Regelwerken zum Multimediabereich. So verlangen z. B. die Entwürfe sowohl für den Mediendienstestaatsvertrag als auch für das Informations- und Kommunikationsdienste-Gesetze (IuKDG-E,BR-Drucks. 966/96 v. 20. Dezember 1996), daß die Anbieter registrierungsfreie Nutzung — oder plakativ formuliert anonyme „Auffahrten auf die Datenautobahn" — anbieten müssen, soweit dies technisch möglich und zumutbar ist. Der IuKDG-E ermöglicht es beispielsweise auch, am Netzverkehr unter Pseudonym teilzunehmen, um personenbezogene Nutzungsprofile zu vermeiden.

Sicher bleibt Kritik anzumelden an der einen oder anderen vorgesehenen Regelung des Multimediagesetz-Entwurfs, etwa an der pauschalen Auskunftspflicht der Teledienstunternehmen gegenüber Strafverfolgungsbehörden und Nachrichtendiensten über die sog. Bestandsdaten der Teilnehmer. Verstärkter Vertraulichkeitsschutz darf nicht durch intensivierte Kontrolle konterkariert werden. Ich habe diese Kritik auch gegenüber den zuständigen Bremer Ressorts geäußert. Der Bundesrat hat diese Bedenken leider nicht aufgegriffen.

Insgesamt aber ist die Entwicklung in der deutschen Gesetzgebung für den Multimedia-Sektor positiv zu bewerten. Die Regelungsvorschläge belegen, daß offensichtlich das Bewußtsein für die Risiken der modernen Informations- und Kommunikationstechnologien für die Privatsphäre des Individuums bei den politisch Verantwortlichen ebenso zunimmt wie die Bereitschaft, darauf normativ zu reagieren. Notwendig bleibt die Anstrengung, auch auf der EG-Ebene solche Standards durchzusetzen.

1.2 Die traditionellen Datenschutzthemen bleiben aktuell

Verfehlt wäre es allerdings, über den Themen der Zukunft die aktuelle Wirklichkeit des Datenschutzes in Dienststellen und Unternehmen, die täglichen Probleme des Bürgers gegenüber datenverarbeitenden Ämtern und Firmen zu vernachlässigen. Das belegen die Beiträge in diesem 19. Jahresbericht. Er bietet wie seine Vorgänger ein breites Spektrum von Stellungnahmen zu Gesetzen, Vorschlägen für den Einsatz von Informations- und Kommunikationstechnik, Ergebnissen von Kontrollen sowie Eingaben und Beschwerden von Bürgerinnen und Bürgern.

Dabei wird ganz deutlich: Die Konfliktlagen und Spannungsfelder zwischen dem Perönlichkeitsrecht des Einzelnen einerseits und den Verarbeitungsinteressen von Staat und Wirtschaft andererseits verändern sich kaum. Auch in diesem Bericht geht es wieder um die Themen Mißbrauchsbekämpfung gegen gesellschaftliche „Unschuldsvermutung", Kostenkontrolle zu Lasten der Vertraulichkeit der Patienten- oder Klientenbeziehung und Dateienabgleich aus Gründen der Verwaltungserleichterung anstelle gebotener Zweckbindung der beim Bürger erhobenen Angaben.

Auch wenn kritische Töne meiner Aufgabenstellung entsprechend überwiegen, weise ich in den Jahresberichten auch immer auf positive Beispiele engagierten Datenschutzes in Ämtern und Unternehmen hin. Ein Beispiel dafür ist in dieser Ausgabe das vorbildliche Konzept der Bremer Entsorgungsbetriebe (vgl. u. Ziff. 12.3).

In diesem Zusammenhang ist ein bemerkenswertes Phänomen zu beobachten: das wachsende Interesse an Datenschutzthemen in kulturindustriellem Kontext. In den Talkshows von Margarete Schreinemakers und Ilona Christen wurden in den vergangenen Monaten Datenschutzfragen ebenso behandelt wie z. B. in HÖR ZU oder der ADAC-Motorwelt. Unabhängig von der Qualität der Sendungen oder Presseerzeugnisse im übrigen bewerte ich es als positiv, wenn die gesellschaftliche Auseinandersetzung über den Datenschutz aus Insider- und Expertenzirkeln herauskommt und das breite Publikum erreicht.

1.3 Datenschutz als Informationsbarriere?

Nicht neu sind auch die Versuche der Verwaltungen, „den Datenschutz" als vermeintliche Informationsbarriere gegenüber Auskunftswünschen von Presse, Parlament oder Bürgern aufzubauen. Nicht selten handelt es sich dabei entweder um einen Deckmantel für bloße Bequemlichkeit der für die Auskunft zuständigen Behördenmitarbeiter oder um eine bewußte Arkanisierung von Verwaltungswissen. Der Datenschutzausschuß der Bremischen Bürgerschaft hat es sich zur Aufgabe gemacht, solchen Fällen im einzelnen nachzugehen und die Stichhaltigkeit der Berufung auf Datenschutzhindernisse zu überprüfen (vgl. u. Ziff. 7.1.2).

1.4 Nachruf auf Hans Schepp

Am 19. Mai 1996 ist Hans Schepp verstorben. Er war der erste Bremische Landesbeauftragte für den Datenschutz. Er hat die Dienststelle in Bremerhaven aufgebaut. In der im produktiven Sinne unruhigen Zeit der geplanten Volkszählung 1983 war er Vorsitzender der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Er hat die Entscheidungsbildung der Konferenz in dieser für die gesamte künftige Entwicklung des Datenschutzes in Deutschland zentralen Frage ebenso umsichtig geleitet wie in seiner eindeutig an der Wahrung der Bürgerrechte orientierten Position beeinflußt. Hans Schepp übte sein Amt bis zu diesem Jahr 1983 mit hohem Engagement aus und blieb auch als Pensionär lebhaft an Datenschutzfragen interessiert; so lehnte er auch in öffentlichen Versammlungen die Einführung des sog. Großen Lauschangriffs ab. Bremen hat Hans Schepp viel zu verdanken.

1.5 Redaktionelle Hinweise

Dieser neue Jahresbericht beschreibt in verschiedenen Kapiteln ausführlich technische Sachverhalte. Dies mag auf den Computerlaien ermüdend oder schwer verständlich wirken. Schwachstellenanalysen von DV-Systemen und -Programmen und Maßnahmenkatkaloge zur Beseitigung von Sicherheitsdefiziten — natürlich nur für die ganz überwiegend in der Bremischen Verwaltung eingesetzten Produkte — nehme ich aber ganz absichtlich so detailliert in den Berichtstext auf. Belegt wird damit zum einen die deutliche Aufgabenverschiebung für den Datenschutzbeauftragten von rechtlichen Fragestellungen bis hin zum technischen und dabei möglichst präventiven Datenschutz (s. o. Ziff. 1.1). Dieser Jahresbericht weist aus, daß meine Mitarbeiter trotz beschränkter Ressourcen ein umfangreiches Prüf- und Testprogramm absolviert haben.

Zum anderen zeigen die Reaktionen auf die früheren Jahresberichte erhebliches Interesse eines bestimmten Leserkreises, nämlich der DV-Organisatoren und -Anwender, an möglichst konkreten Vorgaben und Hinweisen für die datenschutzgerechte Einrichtung und Nutzung ihrer PC und Netze. Die zunehmende Nachfrage nach technischer Beratung stößt in meinem Amt allerdings rasch an Kapazitätsgrenzen. Soll ich meinen Aufgaben nach § 27 BrDSG auch weiterhin, jedenfalls im bisherigen Umfang, nachkommen können, brauche ich in den Haushaltsberatungen der kommenden Jahre die Unterstützung von Senat und Datenschutzausschuß.

Dieser Bericht soll nicht nur in Bürgerschaft, Senat und Öffentlichkeit informieren, sondern will auch zu Kritik und Stellungnahmen anregen. Reaktionen auf die Beiträge sind also auch außerhalb der förmlichen parlamentarischen Behandlung erwünscht; sie fördern die Motivation der Autoren.

2. Bürgerberatung, Eingaben, Beschwerden und Hinweise

2.1 Bilanz in Zahlen

2.1.1 Schriftliche Eingaben

Schon aus arbeitsökonomischen Gründen ist es nicht möglich, eine vollständige Statistik aller Arbeitskontakte des LfD und seiner Mitarbeiter mit Bürgerinnen und Bürgern zu führen. Daher registriere ich die Zahl der telefonischen Anfragen und Hinweise ebensowenig wie die vielen Einzelgespräche anläßlich von Tagungen oder Fortbildungsveranstaltungen. Gleiches gilt für die Bitten um Zusendung von Informationsmaterial. Erfaßt und nach Stichworten vermerkt sind lediglich die schriftlichen Eingaben. Zahl und Inhalt dieser Schreiben zeigen, worüber sich die Bürgerinnen und Bürger besonders ärgern, in welchem Bereich sie ihre Individualrechte einfordern und zu welchen Themen Informationsbedarf besteht. Es geht also nicht nur um Beschwerden oder Kritik; manchmal wird auch nur um eine Rechtsauskunft gebeten.

2.1.2 Öffentlicher Bereich (Verwaltung)

Im Berichtsjahr 1996 (bis einschl. Januar 1997) habe ich insgesamt 164 Eingaben erhalten, d. h. 25 mehr als im Vorjahr. 90 davon betrafen Stellen der öffentlichen Verwaltung. Schwerpunkte waren die Bereiche Jugend/Soziales (13), Gesundheit (12) sowie Staatsanwaltschaft (7) und Polizei (5). Die Senatskommission für das Personalwesen steht mit 5 Eingaben zu Buche. Im folgenden gebe ich zur Illustration einige wenige Stichworte zu den Themen.

Im Bereich Jugend/Soziales wurde z. B. moniert:

— die Datenerhebung ohne Mitwirkung des Betroffenen durch eine Anfrage beim Arbeitgeber,

— die Übermittlung von Sozialdaten an den Vermieter (Wohnungsgenossenschaft),

— die Weitergabe von Einkommensnachweisen durch das Sozialamt an das Arbeitsamt sowie

— die Erhebung von Sozialdaten am Betroffenen vorbei bei einer Bank.

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

— Vermerk „Verdacht auf HIV-positiv" in Patientenunterlagen,

— Anspruch des Patienten auf Einsicht in seine Krankenunterlagen und

— Befundweitergabe des Medizinischen Dienstes an eine Krankenkasse im Rahmen der Überprüfung der Arbeitsunfähigkeit.

2.1.3 Nicht-öffentlicher Bereich (Privatwirtschaft)

74 Schreiben hatten Datenschutzfragen in privaten Unternehmen zum Gegenstand; das sind 22 mehr als im Vorjahr. „Spitzenreiter" waren hier die Auskunfteien (17) und Kreditinstitute (9). Vier Eingaben betrafen Zeitungsverlage bzw. Presseveröffentlichungen. Eine kleine Auswahl dieser Fälle ist im Kapitel 18 dargestellt.

2.2 Bremen-Sprechstunde

In meiner Dienststelle in Bremerhaven stehen meine Mitarbeiter und ich jederzeit für persönliche Beratungen zur Verfügung. Seit dem 23. Mai 1996 biete ich jeden Donnerstag von 15.00 bis 18.00 Uhr zusätzlich in meinem Bremer Büro eine Sprechstunde an. Damit habe ich auf den immer wieder geäußerten Wunsch Bremer Bürgerinnen und Bürger reagiert, ihre Hinweise und Beschwerden persönlich und in Ruhe vortragen zu können, ohne jeweils im Einzelfall einen Termin vereinbaren oder ihre Angelegenheiten telefonisch — und zwar per Ferngespräch — mitteilen zu müssen. Ich habe mit Absicht auch den „kundenfreundlichen" Donnerstag mit seinen seit langem verlängerten Öffnungszeiten gewählt. Mehrere Dutzend Bremerinnen und Bremer haben von diesem Angebot Gebrauch gemacht. Auch gingen zahlreiche Anrufe ein, was belegt, daß auch die Gesprächsmöglichkeit zum Ortstarif eine wichtige Rolle spielt.

3. Fortbildung und Referate

3.1 Fortbildung

Meine Mitarbeiter und ich haben u. a. folgende Lehr- und Fortbildungsveranstaltungen abgehalten:

- Im Aus- und Fortbildungszentrum (AFZ) der SKP zwei zweitägige Grundseminare zum Bremischen Datenschutzgesetz,
- an der Hochschule Bremerhaven/Fachbereich Systemanalyse die Kurse Datenschutz und Datensicherung I und II,
- beim Arbeitgeberverband Bremerhaven eine Veranstaltung zum Datenschutz im Betrieb,
- an der Schule für Verfassungsschutz eine Veranstaltung zum Datenschutzrecht bei nachrichtendienstlicher Tätigkeit sowie
- an der Datenschutzakademie Schleswig-Holstein zum Sozialdatenschutz.

3.2 Referate

Weitere Referate von mir und meinen Mitarbeitern auf Foren, Kolloquien und Podiumsveranstaltungen hatten u. a. die folgenden Themen zum Gegenstand:

- „Telekommunikationsrecht im Wandel",
- „Datenschutz an Schulen",
- „Ist Privatheit im Multimedia-Zeitalter noch zu retten?",
- „Neue Medien und Datenschutz",
- „Datenschutz-Kontrolle in der Privatwirtschaft",
- „Harmonisierung des Grundrechtschutzes in der EU",
- „Data Protection in the private sector in Germany",
- „Lauschangriff contra Grundgesetz".

Diese Auflistung zeigt anschaulich die Spannbreite des von Kongreß- und Tagungsveranstaltern nachgefragten Themenspektrums. Insgesamt ist der Schwerpunkt im Themenfeld Multimedia und Informationsgesellschaft offensichtlich. Die Vorträge wurden gehalten u. a. in der Universität, bei Bürgerrechtsvereinigungen und bei Fachinstituten wie dem Bundesamt für die Sicherheit in der Informationstechnik.

Das Engagement im Bereich Fortbildung und Vortragstätigkeit steht allerdings unter dem Vorbehalt der beschränkten Kapazitäten; zu meinem bedauern muß ich immer wieder Anfragen zu Veranstaltungen und Referaten ablehnen.

4. Presse- und Öffentlichkeitsarbeit

4.1 Pressemitteilungen und -konferenzen; Rundfunkinterviews

Die Darstellungen meiner Presse- und Rundfunkkontakte im Jahresbericht hat eine doppelte Funktion: Zum einen soll deutlich gemacht werden, wie wichtig die Unterstützung einer kritischen Medienöffentlichkeit für die Schaffung von Problembewußtsein in Politik, Verwaltung und Wirtschaft für die Belange des Datenschutzes ist. Zum anderen geben die von den Medien aufgegriffenen aktuellen Themen einen guten Überblick über die gerade aus der Sicht des Bürgers und damit des „Objekts" behördlicher oder geschäftlicher Datenverarbeitung besonders relevanten Fälle und Konflikte.

Meine Pressemitteilungen betrafen u. a. folgende aktuelle Themen:

31. 01. 96: „Telefonbuch-CD-ROM datenschutzrechtlich unzulässig" (vgl. dazu auch 18. JB, Ziff. 19.1);

19. 03. 96: „Datenschutzbeauftragte warnen vor Datenspeicherung auf Vorrat im Telefonnetz";

06. 07. 96: „TELEKOM-Widersprüche: Formularschreiben beim Datenschutzbeauftragten erhältlich";
Dieses Formschreiben wurde ca. 350mal angefordert.

21. 02. 97: „Kritik am Entwurf für ein Strafverfahrensänderungsgesetz".

In zwei Landespressekonferenzen habe ich mich geäußert

— zur Problematik der Medienberichterstattung aus Strafverfahren und

— zusammen mit der Frauen- und der Ausländerbeauftragten zur Unabhängigkeit und künftigen Zusammenarbeit der drei Beauftragten.

In meinen Hörfunk- und Fernsehauftritten ging es u. a. um Datenschutzprobleme der sog. ASYL-CARD, des Direktbanking, der Schufa und bei Multimedia.

4.2 Faltblatt Auskunfteien

Zusammen mit meinen Datenschutzkollegen in Berlin, Hamburg und Niedersachsen habe ich das Faltblatt „Handels- und Wirtschaftsauskunfteien" herausgegeben. Es soll die Bürgerinnen und Bürger informieren über die Arbeitsweise sowie die Zulässigkeit und den Umfang der Datenspeicherungen in dieser Branche sowie über ihre Rechte gegenüber den Unternehmen. Dieses Informationsblatt ist noch vorrätig und kann bei meiner Dienststelle angefordert werden.

5. EG-Datenschutzrichtlinie und Novellierung des BDSG

5.1 Umsetzung der Datenschutzrichtlinie

Die Frist für die Mitgliedstaaten zur Anpassung ihres einzelstaatlichen Datenschutzrechts an die Datenschutzrichtlinie 95/46/EWG läuft im Oktober 1998 ab (vgl. ausführl. 18. JB, Ziff. 5.1). Entgegen ersten Ankündigungen hat das Bundesinnenministerium bis zum Redaktionsschluß dieses Berichts noch keinen Referentenentwurf zur Novellierung des Bundesdatenschutzgesetzes (BDSG) vorgelegt. Lediglich ein erster Text ist Ende Februar 1997 den Bundesressorts zur Stellungnahme zugeleitet worden. Die Zeit drängt nicht zuletzt deshalb, weil auch für die Datenschutzgesetzgebung der Länder Änderungen notwendig werden, um diese in Übereinstimmung mit den Vorgaben der Direktive zu bringen. Die Datenschutzbeauftragten haben die aus ihrer Sicht wichtigsten Regelungsziele und -vorschläge für eine Modernisierung und europäische Harmonisierung des deutschen Datenschutzrechts bereits auf ihrer 51. Konferenz im März 1996 formuliert (vgl. die Entschließung u. Ziff. 20.3).

Der Senat hat in seiner Stellungnahme zum 18. Jahresbericht meine Auffassung unterstützt, daß die Reform des BDSG sich nicht auf eine Minimalanpassung an die Bedingungen der Richtlinie beschränken darf, es vielmehr notwendig ist, daß die Datenschutzgesetzgebung jetzt flexibel auf die neueren Entwicklungen der Informations- und Kommunikationstechnik reagiert (Bürgerschafts-Drucks. 14/499, S. 1). Dieser Haltung des Senats haben sich zunächst der Datenschutzausschuß mit seinem Antrag zum 18. Jahresbericht (Drucks. 14/564, S. 1) und schließlich auch die Bürgerschaft mit ihrer Zustimmung zu diesem Antrag am 20. Februar 1997 angeschlossen.

5.2 Gruppe nach Art. 29 der Richtlinie

Die Gruppe nach Art. 29 der Richtlinie (vgl. dazu 18. JB, Ziff. 5.1.4) 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.

Aufgaben und Tätigkeit der Gruppe nach Art. 29 werden in dem Maße an Bedeutung zunehmen, in dem die Dynamik des informationellen Großraums Europäische Union zwangsläufig stark zunehmende grenzüberschreitende Datenflüsse und gemeinschaftsweit regelungsbedürftige Sachverhalte mit sich bringen wird. Schwerpunkt der Arbeit in den vier Sitzungen dieses Berichtsjahrs war die Auslegung der Art. 25 und 26, d. h. die zukünftige Verfahrensweise bei der Datenübermittlung in Drittstaaten, die über keinen — wie die Richtlinie fordert — „adäquaten" Schutzstandard verfügen. Weitere Beratungsthemen waren u. a. die

Sonderstellung der Medien aufgrund der ihnen zukommenden Meinungs- und Pressefreiheit (Art. 9, vgl. auch § 41 BDSG) sowie das in der Direktive angelegte System der Pflicht zur Meldung von Datenverarbeitungen bei der Datenschutzbehörde (Art. 18 ff.).

Die Diskussionen in der Gruppe werden zumeist vorstrukturiert durch rechtsvergleichende Übersichten, die das Sekretariat auf der Basis der Informationen der Gruppenmitglieder über ihre nationale Rechtssituation erstellt. Zu allen genannten Beratungspunkten wird die Meinungsbildung der Datenschutzgruppe im Jahr 1997 intensiv fortgesetzt.

6. Datenschutz durch Technikgestaltung und -bewertung

6.1 bremen.online — auf dem Weg zum interaktiven Bürgerinformationssystem

Das bereits im 17. Jahresbericht (vgl. dort Ziff. 5.1.4) angesprochene Bürgerinformationssystem soll in den nächsten Jahren schrittweise zu einem interaktiven Stadtinformationssystem ausgebaut werden. Das Vorhaben dient u. a. der Evaluation der Anwendungs- und Nutzungsmöglichkeiten von Onlinediensten und insbesondere des INTERNET für verschiedene Institutionen und gesellschaftliche Gruppen (Wirtschaft, Tourismus, Verwaltung sowie Vereine, Initiativen und gemeinnützige Organisationen). bremen.online enthält Informationsangebote über die Landesverwaltung (u. a. einen Behördenwegweiser) sowie über zahlreiche sonstige Einrichtungen, Angebote und Veranstaltungen in Bremen.

Während auf die Daten des „alten" Bürgerinformationssystems nur über einige wenige „Infosäulen" zugegriffen werden konnte, sind die Informationen von bremen.online auch über das INTERNET im World Wide Web (WWW) weltweit abrufbar (http://www.bremen.de).

Die zukünftige interaktive Funktion von bremen.online soll darin bestehen, den Bürgerinnen und Bürgern direkte elektronische Kontaktmöglichkeiten zu den Ämtern, z. B. für die Antragstellung oder Informationsanfragen, zu eröffnen. Die Zielvision hat die SKP mit dem Schlagwort „online-Verwaltung 2005" beschrieben.

Die Einführung dieser neuen Infrastruktur für die Telekommunikation, sowohl zwischen Bürger und Verwaltung als auch nach außen in die globalen Netze hinein, stellt große neue Anforderungen an Datenschutzrecht und technische Datensicherheit. Die Begleitung von bremen.online mit dem Ziel, die interne wie externe Vernetzung datenschutzgerecht und sozialverträglich zu gestalten, wird eines der Schwerpunktvorhaben meines Amtes werden (vgl. o. Ziff. 1.1).

Erste Etappe wird die Ausarbeitung eines Sicherheitskonzepts für das Stadtinformationssystem zusammen mit der SKP sein. Die Bürgerschaft hat mich mit der Annahme des Ausschußberichts zu meinem 18. Jahresbericht gebeten, dazu bis zur Sommerpause 1997 einen Sachstandsbericht zu geben (vgl. u. Ziff. 7.1.1).

6.2 Windows-Software: Schutzlücken und Schutzmaßnahmen

6.2.1 Windows 95 und NT 3.51

Schon bald nachdem Windows 95 auf den Markt kam, wurde klar, daß dieses Betriebssystem ohne zusätzliche Schutzsoftware die Standards jedenfalls des Bremischen Datenschutzgesetzes für die Verarbeitung personenbezogener Daten nicht erfüllt. Insbesondere stellte sich heraus, daß die in Bremen eingesetzte Sicherungssoftware (SAFEGuard) zu Windows 95 nicht kompatibel ist. Es wurde daher Einigkeit mit der Senatskommission für das Personalwesen (SKP) erzielt, daß in den Bereichen, in denen der Einsatz von SAFEGuard bisher erforderlich war, die Kombination DOS 6.x, Windows 3.x und SAFEGuard vorerst weiterhin eingesetzt werden solle.

Das TuI-Referat der SKP hat überlegt, diese Kombination durch Einsatz von Windows-NT-Client in Verbindung mit einer Verschlüsselungssoftware zu ersetzen (vgl. bereits 18. JB, Ziff. 9.1). Daher habe ich Windows-NT 3.51 in meiner Dienststelle genauer „getestet", und zwar folgende Varianten:

— Windows-NT 3.51 Client als Betriebsystem auf einem stand-alone-PC,

— Windows-NT 3.51 Client als Betriebssystem auf einem vernetzten PC und

— Windows.NT 3.51 Server als Netzbetriebssystem.

6.2.2 Windows-NT 3.51 Client auf Einzelplatz-PC

Mit dem Einsatz von Windows-NT 3.51 Client (WNT-Client) auf einem stand-alone-PC soll die bisher eingesetzte Kombination von MS-DOS 6.x und Windows 3.x bzw. Windows for Workgroups (Version 3.11) in Verbindung mit der Sicherheitssoftware SAFEGuard abgelöst werden. Beim Vergleich beider Lösungen habe ich u. a. folgendes festgestellt:

SAFEGuard bietet durch den Einbau einer SAFEGuard-Karte hardwareseitig die Möglichkeit, Daten auf der Festplatte bzw. auf beweglichen Datenträgern zu verschlüsseln. WNT-Client sieht die Verschlüsselung von Daten nicht vor.

WNT-Client ermöglicht es, den Zugang zum PC durch ein sogenanntes Bootpaßwort zu beschränken, bietet aber keine Prüfung der Systemdateien auf Veränderung (Virenschutz). Eine systemseitige Realisierung des „Vier-Augen-Prinzips" ist nicht vorgesehen.

WNT-Client erlaubt eine differenzierte Vergabe von Rechten: So können System-, Objekt-, Verzeichnis- und Dateirechte vergeben werden, die zudem noch auf Unterverzeichnisse „vererbt" werden können. Dadurch kann die unter SAFEGuard mögliche Anmeldung von mehreren Personen mit jeweils eigenen Paßwörtern auf einen PC ersetzt werden. Vorausgesetzt sind allerdings umfangreiche Kenntnisse bei der Systemverwaltung und den Anwendern.

Die Sperre von seriellen Schnittstellen, die unter SAFEGuard möglich ist, sieht WNT-Client nicht vor, so daß über diese Schnittstellen ein unkontrollierter Datentransfer möglich wäre.

Soll der Einsatz von WNT-Client die bisherigen Softwareprodukte ersetzen, so ist sicherzustellen, daß

— die gesamte Festplatte mit dem NTFS-Dateisystem konfiguriert wird,

— im BIOS-Setup das Booten von Diskette unterbunden wird,

— der Zugriff auf das BIOS-Setup paßwortgeschützt wird, wobei dafür Sorge zu tragen ist, daß das Paßwort nur dem PC-Koordinator bekannt ist.

Sollte die Sensibilität der gespeicherten Daten eine Verschlüsselung der Daten auf der Festplatte erfordern, ist eine Verschlüsselungssoftware erforderlich.

Eine allgemeingülige Aussage über die Ersetzbarkeit der bisher eingesetzten Produkte durch WNT-Client kann nicht getroffen werden, da im Einzelfall die Sensibilität der zu verarbeitenden Daten, die vorgesehene Anzahl der Benutzer sowie die zusätzlich getroffenen organisatorischen Maßnahmen berücksichtigt werden müssen. Wegen der Komplexität des Programms sollte die Administration nur von den PC-Koordinatoren der Dienststelle vorgenommen werden.

6.2.3 WNT-Client auf einem vernetzten PC

Grundsätzlich gelten für den Einsatz von WNT-Client auf vernetzten PC die unter Ziffer 6.2.2 getroffenen Aussagen. Eine zusätzliche Sicherheit im Netzwerk ist durch den Verzicht auf Diskettenlaufwerke zu erreichen. Eine abschließende Bewertung kann nur einzelfallorientiert unter Berücksichtigung des gesamten Netzkonzeptes erfolgen.

6.2.4 WNT-Server als Netzbetriebssystem

Ich habe Windows-NT 3.51 Server (WNT-Server) auf einem stand-alone-PC getestet und die nachfolgende Beschreibung meiner Ergebnisse etwas ausführlicher gehalten, da dieses Netzbetriebssystem in Verbindung mit WNT-Client in der bremischen Verwaltung in großem Umfang eingesetzt werden wird und in den Behörden für die für den TuI-Einsatz Verantwortlichen ein hoher Schulungs- und Beratungsbedarf zu erwarten ist. Für diese Einsatzform liegt im übrigen eine Zertifizierung nach dem C2-Standard der NSA (National Security Agency) nach den Richtlinien des US-Department of Defense „TCSEC" (Trusted Computer System Evaluation Criteria) vor.

Die Serverversion von WNT 3.51 macht deutlich, daß die Sicherheit des Systems entscheidend von den Kenntnissen und Fähigkeiten der Systemverwaltung abhängt. So greifen z. B. die Sicherheitsfeatures nur, wenn das Produkt mit bestimmten Einstellungen, wie z. B. dem Dateisystem NTFS, eingesetzt wird.

6.2.4.1 Physikalische Sicherheit

Für den physikalischen Schutz des Netzes sollte der Server in einem abgeschlossenen Raum aufgestellt werden, zu dem nur ein fest definierter Personenkreis zutrittsberechtigt ist. Bei der Verarbeitung von Personaldaten sollte das Netz als „Insellösung", d. h. ohne jegliche Verbindung mit anderen Netzen, betrieben werden.

6.2.4.2 Logische Sicherheit — Zugangsschutz

Dafür sollten möglichst alle als Arbeitsstation eingesetzten PC ohne Diskettenlaufwerk und mit WNT-Client ausgestattet sein. Die Festplatten der angeschlossenen PC sollten mit dem Dateisystem NTFS konfiguriert werden, da dieses von den angebotenen Dateisystemen den größtmöglichen Schutz bietet. Allerdings ist dieser Schutz nur begrenzt, da im INTERNET bereits Software zur Umgehung dieses Dateisystems abgerufen werden kann.

Als weitere Schutzmaßnahme sollte die Anzahl der Arbeitsstationen, von denen aus eine Anmeldung als Systemverwaltung möglich ist, begrenzt werden, um die Möglichkeiten, das Systemverwalterpaßwort zu „knacken" und somit freien Zugang zum System zu erlangen, einzuschränken.

Die Anmeldezeiten für die Nutzer sollten i. d. R. auf die dienststellenübliche Arbeitszeit begrenzt werden. Ist abzusehen, daß ein Anwender für längere Zeit abwesend ist, sollte sein Benutzerkonto gesperrt werden.

Für die Einrichtung von Benutzerkonten sollte die Mindestlänge des Paßwortes genau vorgegeben werden. Die Anzahl der maximal möglichen Login-Versuche sollte auf drei beschränkt werden. Die Entsperrung sollte durch die Systemverwaltung vorgenommen und dokumentiert werden. Angaben zu Paßwortalter und Paßwortzyklus sollten ebenso vorgesehen werden wie die Sperrung von Trivialpaßworten. Die Einrichtung eines Benutzerkontos ohne die Verpflichtung zur Paßworteingabe ist nicht zu akzeptieren.

Wie bereits in anderen Systemen ist auch beim Einsatz von WNT-Server die Systemverwaltung eine besondere Schwachstelle, da der Zugriff nach dem „Vier-Augen-Prinzip" vom System nicht unterstützt wird. Der Systemverwalter kann jedem Nutzer die vollen Rechte zuteilen. Die Aktivitäten der Systemverwaltung werden zwar protokolliert, aber nicht revisionssicher, da die Systemverwaltung auf diese Protokolldaten zugreifen und sie damit ändern kann.

Möglich ist die Zuordnung von Benutzern zu einer von sechs Gruppen mit bereits systemseitig vorgesehenen Standardrechten, ohne die Rechte dieser Gruppe im Detail zu kennen. Einschränkungen von Rechten für einzelne Anwender müssen explizit festgelegt werden.

Die für die Datensicherheit äußerst wichtige Ausgestaltung der Vergabe von Rechten ist bei diesem Netzbetriebssystem eine sehr komplexe Angelegenheit, die in diesem Bericht nicht im Detail dargestellt werden kann. Dies gilt auch für die bei WNT-Server vorgesehenen umfangreichen Protokollierungen und deren Schwachstellen.

Die abschließende datenschutzrechtliche Bewertung des Einsatzes von WNT-Server kann ebenfalls nur im Einzelfall unter Einbeziehung des Netzkonzeptes erfolgen.

6.2.5 Fazit

Die zentralen Anforderungen lauten zusammengefaßt: Neben einer adäquaten Qualifikation der Systemverwaltung ist eine durchdachte Rechtestruktur unbedingt erforderlich. Bei der Verarbeitung von sensiblen personenbezogenen Daten ist die Verschlüsselung der Daten auf Festplatte und beweglichen Datenträgern durch eine entsprechende zusätzliche Software sicherzustellen. Das „Vier-Augen-Prinzip" ist ebenso zu realisieren wie eine revisionssichere Protokollierung. Diese Kriterien werden auch der Bestandsaufnahme über den Stand der Datensicherheit zugrundeliegen, die vorzulegen der Datenschutzausschuß den Landesbeauftragten in Abstimmung mit der SKP — gebeten hat (vgl. u. Ziff. 7.1.1.2, zu 18. JB, Ziff. 9.1).

6.3 Antragsverfahren für Einzelplatz-PC vereinfacht

In der TuI-Ausschuß-Sitzung am 11. Juni 1996 habe ich bekanntgegeben, daß ich bei nichtvernetzten Einzelplatz-PC, die keine Datenfernübertragungs-Anbindung haben, grundsätzlich auf die zuvor übliche Vorlage des PC-Antrages bzw. der PC-Beschaffungsanzeige durch die jeweiligen Dienststellen verzichte. Dies hat vor allem Kapazitätsgründe. Ich will und muß die begrenzte Technikkapazität meines Amtes auf die potentiell risikoreicheren Netzprojekte konzentrieren. Allerdings habe ich mir vorbehalten, in Einzelfällen — insbesondere, wenn die Angaben im TuI-Gesamtplan des jeweiligen Ressorts unzureichend oder besonders sensible Daten betroffen sind — mir auch Beschaffungsvorhaben für isolierte Rechner zur Stellungnahme vorlegen zu lassen. Hilfreich wäre für mich, wenn in künftigen TuI-Gesamtplänen bei den einzelnen Beschaffungsvorhaben vermerkt wäre, ob eine Vernetzung und/oder eine DFÜ-Anbindung geplant ist. Auf Wunsch stehe ich natürlich weiterhin für Datenschutzfragen auch bei stand-alone-Rechnern zur Verfügung.

7. Bürgerschaft

7.1 Die Arbeit des Datenschutzausschusses

7.1.1 Beratung des 18. Jahresberichts

7.1.1.1 Der Ablauf der Beratung

Der Datenschutzausschuß hat meinen 18. Jahresbericht (Bürgerschafts-Drucks. 14/272) und die Stellungnahme des Senats (Drucks. 14/499) in seiner 13. Sitzung am 11. Dezember 1996 im Beisein der für die Tagesordnungspunkte jeweils zuständigen Ressortvertreter beraten. Wie immer wurden auch aus dem 18. Jahresbericht nur die aus der Sicht der Parlamentarier besonders wichtigen, insbesondere die zwischen dem Senat und mir strittigen Themen aufgegriffen. Zu kritisieren ist, daß in zwei Fällen senatorische Behörden Arbeitsaufträge der Bürgerschaft, die diese bereits in ihrem Beschluß zu meinem vorigen (17.) Jahresbericht erteilt hatte, nicht erfüllt hatten, so daß der Ausschuß deren Erledigung anmahnen mußte.

Bericht und Antrag des Ausschusses wurden am 21. Januar 1997 verabschiedet (Drucks. 14/564). In der Februar-Sitzung ist die Bürgerschaft den Bemerkungen des Ausschusses beigetreten. In dieser Plenarsitzung wurde mir erstmalig die Gelegenheit eingeräumt, in der Aussprache über den Jahresbericht diesen den Abgeordneten vorzustellen (vgl. § 33 Abs. 4 BrDSG).

7.1.1.2 Der Bericht des Ausschusses im Wortlaut

Im Wortlaut enthält der Ausschußbericht folgende Feststellungen, Empfehlungen und Aufforderungen an den Senat:

„Einleitend sei angemerkt, daß der Ausschuß die vom Datenschutzbeauftragten und vom Senat übereinstimmend aufgestellte Forderung nach einer Novellierung des Bundesdatenschutzgesetzes unterstützt. Der Ausschuß teilt die Auffassung, daß eine Neukonzeption des Datenschutzrechts sich nicht in einer Anpassung an die EU-Datenschutzrichtlinie erschöpfen darf, sondern insbesondere auch die durch die neuen Möglichkeiten der Informations- und Kommunikationstechnik veränderten Bedingungen der Datenerhebung und -verarbeitung berücksichtigen muß."

— Ausländerzentralregister (11.2 = Ziff. des 18. Jahresberichts)

Aufgrund von Prüfungen bei den Ausländerämtern Bremen und Bremerhaven hat der Landesbeauftragte für den Datenschutz festgestellt, daß im Widerspruch zu dem in dem Bundesgesetz über das Ausländerzentralregister vorgeschriebenen Datenverarbeitungsverfahren das Register weiterhin auf der Grundlage des vor Inkrafttreten dieses Gesetzes geltenden Verfahrens betrieben wird. Dies hat zum Beispiel zur Folge, daß die Protokollierung der Abrufe und Dateneingaben unzureichend ist, wodurch die Kontrollmöglichkeit des Datenschutzbeauftragten erschwert wird.

Der Senator für Inneres hat vor dem Ausschuß erklärt, er werde den Bundesminister des Innern auf die ordnungsgemäße Umsetzung der Protokollierungspflicht nach dem Gesetz über das Ausländerzentralregister hinweisen.

Der Ausschuß bittet den Landesbeauftragten für den Datenschutz nach Ablauf von sechs Monaten um einen Sachstandsbericht in dieser Angelegenheit.

— Verfassungsschutzüberprüfung bei Einbürgerung (8.2 = 17. Jahresbericht 9.2.5)

Der Datenschutzausschuß hatte bereits in seinem Bericht vom 6. Februar 1996 zum 17. Jahresbericht (Drucks. 14/214) die Auffassung vertreten, daß der Senat entsprechend der Praxis in der Mehrzahl der anderen Bundesländer bei Ermessenseinbürgerungen Rückfragen beim Verfassungsschutz nicht als Regel, sondern nur in den Fällen vornehmen solle, in denen Anhaltspunkte einer Einbürgerung entgegenstünden.

Der Senator für Inneres hat nunmehr gegenüber dem Ausschuß zugesagt, er werde in Zusammenarbeit mit dem Landesamt für Verfassungsschutz ein den Vorstellungen des Ausschusses entsprechendes Verfahren entwickeln.

— Wahlkampf mit Wählerdaten (8.2 = 17. Jahresbericht 9.4.1)

Der Senator für Inneres hat gegenüber dem Ausschuß angekündigt, daß er bereit sei, der vom Datenschutzausschuß bereits in seinem letztjährigen Bericht erhobenen Forderung nachzukommen, gegenüber den Meldebehörden im Lande Bremen klarzustellen, daß Wählerdaten nicht an Parteigliederungen außerhalb Bremens weitergegeben werden dürfen.

— Vorlage des Steuerbescheids statt Nachweis von Einzelangaben (8.2 = 17. Jahresbericht 16.1)

Die Bürgerschaft (Landtag) hatte entsprechend der Beschlußempfehlung des Datenschutzausschusses vom 6. Februar 1996 den Senat um einen Bericht insbesondere zu der Frage gebeten, welche Angaben im einzelnen bei der Gewährung öffentlicher Leistungen (zum Beispiel Wohngeld, Sozialhilfe, Kindergartenplätze) verlangt werden. Dieser Bericht liegt erst seit kurzem vor und konnte deshalb im Ausschuß noch nicht behandelt werden.

— Neue Software — inkompatibel mit bisherigem Zugriffsschutzprogramm (9.1)

Für die bisher in der bremischen Verwaltung verwendeten Betriebssysteme MS-DOS und Windows 3.1 wurde als einheitliches Sicherungssystem das Produkt „SAFEGuard" verwendet. Zwischenzeitlich werden neue Software-Entwicklungen eingesetzt, für die das bisherige Sicherheitsprodukt ungeeignet ist. Wirksame Sicherungssysteme befinden sich derzeit noch in der Entwicklung. Als Übergangslösung empfiehlt die Senatskommission für das Personalwesen die Software Windows NT.

Als Grundlage für die weitere Behandlung dieser Angelegenheit im Datenschutzausschuß ist es notwendig, eine Bestandsaufnahme darüber zu erhalten, ob der bisherige Standard der Datensicherheit durch Einsatz neuer Software gehalten oder verbessert worden ist. Der Ausschuß hat deshalb den Landesbeauftragten für den Datenschutz gebeten, in Absprache mit der Senatskommission für das Personalwesen zunächst eine entsprechende Umfrage bei den bremischen Dienststellen durchzuführen. Nach Vorliegen des Ergebnisses wird der Ausschuß seine Beratung fortsetzen.

— INTERNET: Orientierungshilfe zur Lösung von Datensicherungsproblemen (9.2)

In der öffentlichen Verwaltung besteht großes Interesse an einem Zugang zu weltweiten Netzen, insbesondere zu dem INTERNET. Die Netzanbindung soll sowohl zur Informationsgewinnung als auch zur Bereitstellung eigener Informationen für andere dienen.

Einer Umfrage der Senatskommission für das Personalwesen zufolge sind derzeit von den Dienststellen insgesamt 200 Anschlüsse geplant. Im Rahmen des Projekts Stadtinformationssystem (bremen.online) sind zur Zeit 36 Anschlüsse eingerichtet, und zwar als Einzelanschlüsse für Bürgerbeauftragte, Datenkoordinatoren und einige Ortsämter.

Der Ausschuß sieht ebenso wie Datenschutzbeauftragter und Senat bei Anschlüssen an das INTERNET erhebliche Risiken für den Datenschutz und die Datensicherheit, und er begrüßt deshalb das gemeinsame Vorhaben der Senatskommission für das Personalwesen und des Datenschutzbeauftragten zur Erstellung eines

Sicherheitskonzepts für diesen Bereich. Der Landesbeauftragte für den Datenschutz wird gebeten, bis zur Sommerpause 1997 insoweit einen Sachstandsbericht zu geben.

Um sich selbst ein Bild über die Gesamtproblematik machen zu können, wird sich der Ausschuß am 27. Januar 1997 (redakt. Hinweis: Terminverschiebung erfolgte auf 18. Februar 1997) vor Ort, das heißt im TuI-Referat der Senatskommission für das Personalwesen, informieren.

7.1.2 Aktuelle Themen

Neben dem Jahresbericht und dem Haushalt meiner Dienststelle behandelt der Datenschutzausschuß regelmäßig aktuelle Themen, die von den Abgeordneten oder mir eingebracht werden. Diese Tagesordnungspunkte nehmen nicht selten bezug auf Medienberichte oder beruhen auf Rückfragen von Parlamentskollegen.

Der Ausschuß hat sich weiterhin vorgenommen, ggf. unter Beiziehung der zuständigen Ressortvertreter Behauptungen der Verwaltung zu überprüfen, „der Datenschutz" behindere bestimmte organisatorische Maßnahmen bzw. Sachverhaltsfeststellungen oder erschwere die Beantwortung parlamentarischer Anfragen. Dies betraf u. a.

— eine Vorlage für die staatliche Deputation für Arbeit zu einer Verbleibsanalyse von Teilnehmern von Vorqualifizierungskursen und

— die Abrechnung von Müllgebühren nach der Personenzahl von Haushalten in Großwohnanlagen (vgl. u. Ziff. 12.2).

In beiden Fällen kam der Ausschuß zu dem Ergebnis, daß keine datenschutzrechtlichen Hinderungsgründe vorlagen. Ich begrüße diesen Arbeitsansatz des Datenschutzausschusses. Es erleichtert meine Arbeit, wenn Mißverständnisse und Fehlinterpretationen, die sich immer wieder auch in mir nicht zugänglichen Verwaltungsdokumenten befinden, im Ausschuß angesprochen und dann geklärt bzw. richtiggestellt werden.

Außerdem wurden im Berichtszeitraum u. a. folgende Themen beraten:

— Widerspruchsrechte von Telefonkunden gegen die Eintragung in gedruckte und elektronische Teilnehmerverzeichnisse,

— Rechtmäßigkeit der Fragebogenaktion des Bausenators bei den Kleingärtnern in der Waller Fleet (vgl. u. Ziff. 15.2),

— Speicherung von Anzeigeerstattern mit befürchteter Aufnahme in das polizeiliche Führungszeugnis (erfolgt nicht!),

— Datenschutzklausel in Versicherungsverträgen.

Über Konzeption und Struktur des geplanten Stadtinformationssystems und die dabei entstehenden datenschutzrechtlichen Fragen (vgl. o. Ziff. 6.1) informierte sich der Ausschuß bei einer von der Senatskommission für das Personalwesen organisierten Vorführung am 18. Februar 1997 (vgl. o. Ziff. 7.1.1.2).

7.2 Grundrecht auf Datenschutz — Reform der Landesverfassung (LV)

Der Beschluß der Bürgerschaft zur „Weiterführung der Verfassungs- und Parlamentsreform" sieht als einen der wesentlichen Beratungspunkte die „Aufnahme eines Grundrechts auf informationelle Selbstbestimmung" vor (vgl. 18. JB., Ziff. 1.2.1). Der Datenschutzausschuß hatte nach intensiver Debatte in mehreren Sitzungen dem nichtständigen Ausschuß zur Reform der Landesverfassung einen einvernehmlich verabschiedeten Textvorschlag vorgelegt. Der Reformausschuß hat ihn mit einer kleinen Änderung gebilligt und in den Entwurf des Abschlußberichts an die Bürgerschaft aufgenommen, der im Februar 1997 den Fraktionen vorgelegt wurde.

Danach soll durch eine Ergänzung von Art. 12 LV jedermann das Recht auf Schutz seiner personenbezogenen Daten garantiert bekommen. Auch das bereits einfachgesetzlich im BrDSG eingeräumte Auskunftsrecht über die eigenen Daten soll von Verfassungs wegen garantiert werden. Und: Bei Verlagerung von Aufgaben der öffentlichen Verwaltung auf Private soll den Staat die Pflicht treffen, auch bei diesen für die Sicherstellung des Datenschutzes zu sorgen.

Wenn das Recht auf informationelle Selbstbestimmung, das das Bundesverfassungsgericht in seinem Volkszählungsurteil aus den Artikeln 1 und 2 des Grundgesetzes abgeleitet hat, ausdrücklich in den Text der Landesverfassung aufgenommen wird, bedeutet dies keine überflüssige Redundanz. Vielmehr würde dadurch der Wille der bremischen Volksvertretung bekräftigt, die Entwicklung zur Informationsgesellschaft auch und gerade in diesem Bundesland nur zu akzeptieren, wenn die private Sphäre des Einzelnen hinreichend geschützt bleibt. Ich hoffe daher, daß sich die Bürgerschaft insgesamt bei der abschließenden Beratung der Verfassungsreform der Willensbildung der Ausschüsse anschließt.

7.3 Datenschutzordnung

Am 26. September 1996 hat die Bürgerschaft einen gemeinsamen Antrag aller Fraktionen verabschiedet. Darin wird der Datenschutzausschuß beauftragt, eine Datenschutzordnung für die Datenverarbeitung durch die Bremische Bürgerschaft (Landtag und Stadtbürgerschaft), ihre Gremien und Mitglieder zu erarbeiten und zur Beschlußfassung vorzulegen. Diese Datenschutzordnung soll sich außerdem auf die Fraktionen und Abgeordneten bzw. deren Mitarbeiter sowie — soweit sie zu parlamentarischen Zwecken tätig sind — die Bediensteten der Verwaltung erstrecken (Beschluß Nr. 14/378 zu Drucks. 14/408). Die verfassungsrechtlichen Vorgaben und die Erforderlichkeit einer solchen Regelung habe ich im letzten Jahresbericht dargestellt (vgl. 18. JB, Ziff. 7.1.1.4).

Vorausgegangen waren dieser Plenumsentscheidung eingehende Beratungen im Datenschutzausschuß. Herangezogen wurden dabei auch die parallelen Regelungen und Regelungsprojekte in anderen Landtagen. Die Bürgerschaftsverwaltung hatte mir daraufhin unter Berücksichtigung der Erörterungen im Ausschuß und auf der Grundlage des Musterentwurfs der Parlamentsdirektoren (vgl. dazu 18. JB, a.a.O.) einen ersten Entwurf zugeleitet, zu dem ich Mitte November 1996 Änderungen und Ergänzungen vorgeschlagen habe. Nach bilateralen Gesprächen konnte dem Datenschutzausschuß in der Februar-Sitzung eine zwischen der Bürgerschaftsverwaltung und mir abgestimmte Textfassung vorgelegt werden.

Da die Debatte über Datenschutzordnungen sowohl im Bundestag als auch in einer Reihe von Landtagen läuft, hat sich auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 1996 mit der Thematik befaßt. Die Rechtslage ist von Land zu Land allerdings insoweit abweichend, als die Regelungsdichte für einzelne parlamentarische Bereiche, etwa für den Datenumgang durch Untersuchungs- und Petitionsausschüsse, unterschiedlich ist. Soweit spezialgesetzliche Normen vorliegen, greifen bloße Geschäftsordnungsbestimmungen nicht bzw. nur ergänzend. Die Ergebnisse dieser Beratung mit meinen Kollegen habe ich in meine Stellungnahme gegenüber der Bürgerschaft (s.o.) einbezogen.

Der Datenschutzausschuß wird seine Beratungen im kommenden Berichtszeitraum fortsetzen.

8. Personalwesen

8.1 PuMa — Neues Datenschutzkonzept

8.1.1 Geändertes Datenschutzkonzept

Im Laufe des vergangenen Jahres wurde sukzessive mit der Installation des Verfahrens PuMa (Personalverwaltung und -management) in den senatorischen Dienststellen begonnen, wie z. B. beim Senator für Frauen, Gesundheit, Jugend, Soziales und Umweltschutz im Bereich Gesundheit, Jugend und Soziales.

Die von mir in meinem letzten Jahresbericht unter Ziff. 10.1.4 monierte fehlende Abschottung der Systemverwaltung gegenüber der Protokollierung unter Windows-NT sollte durch eine organisatorische Regelung kompensiert werden. Die Senatskommission für das Personalwesen (SKP) erklärte sich damals bereit, die Funktion der Datenbankadministration zentral für die einzelnen Dienststellen zu übernehmen.

Bereits im Laufe des Jahres stellte sich heraus, daß eine zentrale Datenbankadministration noch nicht erforderlich ist, da es keine bereichsspezifischen Programmänderungen geben wird, bevor nicht die PuMa-„Standardversion" in allen vorgesehenen Dienststellen implementiert ist.

Im Herbst wurde mir ein neues mit dem Gesamtpersonalrat abgestimmtes PuMa-Datenschutzkonzept zur Kenntnisnahme übersandt. Neben einigen redaktionellen Änderungen wurden insbesondere die Rollen der Systemadministration neu definiert.

Im alten Konzept waren zwei Funktionen für die Administration vorgesehen:

— Die Funktion „PuMa-Admin" sollte über uneingeschränkte Rechte verfügen, mit einem Zugriff nach dem „Vier-Augen-Prinzip" arbeiten und ein Jahr zentral durch Personal der SKP ausgeführt werden.

— Der „Verwalter" sollte ein sog. dezentraler Administrator mit fest definierten Aufgaben und allen Benutzerrechten sein, mit Ausnahme der Berechtigung, Protokolleinstellungen zu ändern oder auf Protokolldateien zuzugreifen.

8.1.2 Kombination zentraler/dezentraler Netzadministration

Die Neugliederung der Administrationsaufgaben sieht nun folgende Funktionen vor:

— Die „PuMa-Verwaltung" soll die Aufgaben der Datenbankadministration vor Ort wahrnehmen und hat Zugriff auf alle Daten in der Datei „PuMaDat". Alle Tätigkeiten werden in einem Tätigkeitsprotokoll festgehalten. Diese Rolle soll ein Jahr zentral durch die SKP wahrgenommen werden, sofern nicht einzelne Aufgaben (z. B. monatliches Update der SKP-Daten) durch fest programmierte Anwendungen, die einen Zugriff auf den PuMa-Datenbestand nicht gestatten, vor Ort durchgeführt werden können.

— Die „Verwaltung" soll für die dezentrale Administration (z. B. Einrichten von Benutzern) verantwortlich sein. Sie hat — wie nach dem alten Konzept der „Verwalter" (s. o.) — keine Möglichkeit, Protokolleinstellungen zu ändern oder auf Protokolldateien zuzugreifen, so daß das „Vier-Augen-Prinzip" nicht mehr notwendig ist.

— Für die uneingeschränkte Netzadministration mit allen Systemrechten ist die Funktion „Admin" vorgesehen. Sie wird bis auf weiteres durch die SKP zentral wahrgenommen.

— Die Mitglieder der Gruppe „PuMa-Verwaltung" arbeiten nach dem „Vier-Augen-Prinzip". Alle Aktivitäten sind in einem Tätigkeitsprotokoll festzuhalten. Sofern einzelne Aufgaben durch fest programmierte Anwendungen erledigt werden können, können sie dezentral wahrgenommen werden, ansonsten übernimmt die SKP diese Funktion zunächst für ein Jahr.

Die neue Verteilung der Administrationsaufgaben ermöglicht es, die Protokollierung der Aktivitäten von Mitgliedern der Administratorengruppe nicht mehr für alle Tätigkeiten, sondern nur noch bei Dateizugriffen auf die PuMa-Daten und Benutzerverzeichnisse auf dem Server vorzunehmen. Diese Neukonzeption gewährleistet den durch die Dienstvereinbarung erreichten Datenschutzstandard.

8.1.3 Verschlüsselung beim Datentransport

Ende letzten Jahres habe ich den PuMa-Einsatz beim Senator für Frauen, Gesundheit, Jugend, Soziales und Umweltschutz — Bereich Gesundheit, Jugend und Soziales — geprüft und dabei festgestellt, daß die Daten, die die SKP monatlich an die Behörde weitergibt, nicht verschlüsselt werden. Dies verstößt gegen die Regelung zur Transportkontrolle in Ziffer 5.5 des PuMa-Datenschutzkonzepts, das als Anlage A Bestandteil der Dienstvereinbarung (DV) PuMa ist (vgl. Ziffer 4.3 DV). Danach sind die Daten mit einem sicheren Verfahren zu verschlüsseln.

Da die SKP für die Beseitigung dieser Mängel verantwortlich ist, habe ich sie Ende Januar 1997 um Stellungnahme hierzu gebeten. Eine Antwort steht noch aus.

8.2 Arbeitszeiterfassung (AZE) — Neukonzeption und Umsetzungsdefizite

8.2.1 Zentralisierung der Verarbeitung geplant

Nach der Dienstvereinbarung (DV) über die Grundsätze der gleitenden Arbeitszeit war vorgesehen, in den Dienststellen der bremischen Verwaltung dezentrale AZE-Systeme zu installieren. Aufgrund der damit verbundenen erheblichen

Kosten hat die SKP mich Ende September 1996 stichpunktartig über eine neue Konzeption der elektronischen Arbeitszeiterfassung informiert und um eine erste kurze Bewertung gebeten.

Vorgesehen ist, nur noch einen Rechner für das gesamte Verfahren bei der Informations- und Datentechnik Bremen (ID Bremen) zu installieren. Geplant ist, daß die Übertragung der Arbeitszeitdaten durch die Dienststellen an die ID Bremen abends über die sonst tagsüber genutzte Telefonleitung erfolgen und der Beschäftigte sein Arbeitszeitkonto selbst verwalten soll.

Des weiteren ist beabsichtigt, für die Personalstellen der Dienststellen bei der ID Bremen monatliche Kontrollisten zu erstellen, die u. a. Überschreitungen der zulässigen Minus- und festzulegenden Pluszeiten und von den Beschäftigten eingegebene Tage für Abwesenheit durch Krankheit, Dienstreisen, Urlaub, Kur und Freizeitausgleich enthalten sollen.

Ich habe der SKP in einer ersten Stellungnahme mitgeteilt, daß die vorgesehene Nutzung der Telefonleitung für die Datenübertragung nur dann zulässig ist, wenn die Transportkontrolle gem. § 7 Abs. 2 Nr. 9 Bremisches Datenschutzgesetz (BrDSG) gesichert ist, d. h. wenn der Transport verschlüsselt erfolgt und vor jeder Datenübertragung eine Überprüfung zumindest der Rufnummer des zentralen ID-Bremen-Servers vorgenommen wird.

Die Grundsätze für die gleitende Arbeitszeit sehen vor, daß die Beschäftigten die Arbeitszeitkonten selbst verwalten. Deshalb habe ich die Notwendigkeit eines Online-Anschlusses und -Zugriffs der Personalstellen der Dienststellen in Frage gestellt, zumal eine Einsicht der Systemverantwortlichen nach Ziffer 20 Abs. 2 der DV ohnehin nur im „Vier-Augen-Prinzip" mit den Beschäftigten erfolgen darf.

Außerdem weicht die Erstellung monatlicher Kontrollisten von Ziffer 18 Abs. 3 DV ab, wonach der Vorgesetzte die Richtigkeit der Zeiterfassung nur stichprobenweise zu überprüfen hat. Die Notwendigkeit solcher Monatslisten für die Personalstellen ist bisher noch nicht hinreichend dargelegt worden.

Die SKP hat mir auf Anfrage mitgeteilt, meine endgültige Beteiligung werde erst dann erfolgen, wenn die Beratungen mit dem Gesamtpersonalrat abgeschlossen sind. Außerdem hat mir die SKP im Januar 1997 eine „Vorstudie Zeiterfassung" der ID Bremen zur Verfügung gestellt. Beabsichtigt ist, auf dieser Basis eine europaweite Ausschreibung für das Arbeitszeiterfassungssystem vorzunehmen.

8.2.2 SKP: Fehlende Unterlagen zur Arbeitszeiterfassung

Bereits in meinem 18. Jahresbericht (Ziff. 10.2) habe ich das bei der SKP eingeführte System zur Arbeitszeiterfassung problematisiert, da es entgegen Ziffer 19 Abs. 2 DV nicht als stand-alone-System, sondern zusammen mit der Zugangskontrolle zum Gebäude betrieben wird.

Die SKP hatte den Betrieb des Systems im Hinblick auf eine landesweite Ausschreibung der Bremer Kommunikationstechnik (BreKom) zunächst gestoppt. Sie führt die Arbeitszeiterfassung aber auf freiwilliger Basis mit etwa der Hälfte der Behördenmitarbeiter/-innen weiter; die Beschäftigten haben jederzeit die Möglichkeit, die Teilnahme an der Arbeitszeiterfassung aufzunehmen oder zu beenden. Bereits im 4. Quartal 1995 hatte ich wegen dieser Fortführung um Informationen über die technische Umsetzung gebeten und ein Revisionskonzept, die Dateibeschreibung und das Geräteverzeichnis angefordert. Meine Fragen und Informationswünsche sollen voraussichtlich Mitte März 1997 in einer Besprechung mit den zuständigen Mitarbeitern und dem Personalrat der SKP erörtert werden.

8.2.3 Bereich Gesundheit, Jugend und Soziales: Prüfungsergebnis

Bei dieser Behörde habe ich exemplarisch die Arbeitszeiterfassung vor Ort geprüft. Sobald das Mitbestimmungsverfahren für das Datenschutzkonzept abgeschlossen ist, soll das System im Echtbetrieb laufen. Nach meinen Feststellungen sind dort (nur) folgende Punkte korrekturbedürftig:

Die manuelle Eingabe von Daten aus den nach Ziffer 14 Abs. 1 DV vorgesehenen Arbeitszeitbelegen ist nach Ziffer 11 Abs. 1 DV durch den Beschäftigten selbst in das Arbeitszeitkonto vorzunehmen. Gleichwohl leistet das dort eingesetzte System die Selbsteingabe insoweit nicht. Aus diesem Grunde ist — sofern Korrekturen der Zeitbuchungen erforderlich werden — immer ein Arbeitszeit- bzw. Korrekturbeleg auszufüllen, der außerdem vom Vorgesetzten abzuzeichnen und dann

dem Systemverantwortlichen zu übergeben ist, damit dieser die Eingabe vornehmen kann. Diese Handhabung ist zu umständlich. Ich habe daher die Behörde gebeten, das Verfahren den Vorgaben der Dienstvereinbarung anzupassen.

Und: Die mit der Erfassung von Korrekturbelegen und Statusbuchungen betrauten Mitarbeiter/-innen haben auch allein Einblick in die Arbeitszeitkonten der Beschäftigten, obwohl Ziffer 20 Abs. 2 DV dies nur im „Vier-Augen-Prinzip" mit den Beschäftigten vorsieht. Ich habe daher eine Umgestaltung der Software vorgeschlagen, da es für die Datenerfassung ausreichend ist, eine Eingabemaske ohne Einsichtsmöglichkeit in die Arbeitszeitdaten des jeweiligen Monats zur Verfügung zu stellen.

Mein Schreiben habe ich im Januar 1997 an die Behörde gesandt und mit ihr zwischenzeitlich vereinbart, daß sie sich nach der Abstimmung mit ihrem Personalrat zu meinen Monita äußert.

8.3 Löschung der Untersuchungsdaten abgewiesener Polizeibewerber/-innen

In meinem letzten Jahresbericht hatte ich bemängelt, daß nach der bisherigen Praxis beim Polizeiärztlichen Dienst die Untersuchungsdaten abgewiesener Bewerber über einen Zeitraum von zehn Jahren aufbewahrt wurden (18. JB, Ziff. 10.5). Inzwischen hat der Leiter der Bereitschaftspolizei nach Klärung der endgültigen Sachlage mit der Gesundheitsbehörde den Polizeiärztlichen Dienst angewiesen, sich für die medizinischen Unterlagen dieses Personenkreises an § 22 Abs. 5 BrDSG zu halten. Danach sind personenbezogene Daten, die vor der Eingehung eines Dienstverhältnisses — also von Stellenbewerbern — erhoben wurden, unverzüglich zu löschen (zu vernichten), sobald feststeht, daß ein Dienstverhältnis nicht zustande kommt. Diese Vernichtung ist — so wurde mir auf Anfrage bestätigt — inzwischen geschehen.

8.4 Neue Personalakten-Richtlinien jetzt in Kraft

8.4.1 Die wichtigsten Regelungen

In meinem 17. Jahresbericht hatte ich unter Ziffer 8.4 auf den von der Senatskommission für das Personalwesen (SKP) vorgelegten Entwurf der Richtlinien über die Erhebung und Führung von Personalaktendaten hingewiesen und die aus meiner Sicht wichtigsten Punkte aus meiner Stellungnahme gegenüber der SKP dargestellt. Inzwischen sind die Richtlinien vom 25. Mai 1996 (Brem.Abl. S. 433) am 1. Juni 1996 in Kraft getreten. Die SKP hat zahlreiche meiner Anregungen aufgegriffen. Zentraler Regelungszweck war dabei für mich der Ersatz veralteter beamtenrechtlicher Vorstellungen durch die moderneren Prinzipien des Datenschutzrechts.

Die wichtigsten meiner Vorschläge sind wie folgt berücksichtigt bzw. nicht berücksichtigt worden:

Ziffer 6 Abs. 1 der Richtlinien legt nunmehr fest, daß der Datenfluß zwischen Grund- und Teilakten sowie Nebenakten zwar keine Datenübermittlung ist, jedoch für die jeweiligte Aufgabenerfüllung erforderlich sein muß.

Die im Entwurf vorgesehene Absicht, Gesundheitszeugnisse und ärztliche Untersuchungsergebnisse, die nicht allein dem Zweck der Eingehung eines Dienstverhältnisses dienen, zur Personalakte zu nehmen, ist in den Richtlinien so nicht mehr enthalten. Ziffer 11 Abs. 1 stellt fest, daß Unterlagen übern ärztliche und psychologische Untersuchungen sowie Vorgänge über ärztliche Behandlungen nicht Bestandteil der Personalakte, jedoch entsprechend den Personalaktendaten zu behandeln sind. Nur Gesundheitszeugnisse und Untersuchungsergebnisse für eine dienst- oder arbeitsrechtliche Entscheidung gehören nach Ziffer 10 Abs. 1 Nr. 10 zur Grundakte. Soweit ärztliche und andere vertrauliche Unterlagen zur Personalakte zu nehmen sind, erfolgt die Aufbewahrung nach Ziffer 7 Abs. 2 in einem verschlossenen Umschlag in der Personalakte.

Der schon lange überholte Grundsatz, daß die Personalakte ein möglichst vollständiges Bild über den beruflichen Werdegang und insoweit über die Persönlichkeit des Betroffenen geben soll, ist — entgegen dem seinerzeitigen Entwurf — nicht mehr in die Richlinien aufgenommen worden. Es gilt also das im § 93 Satz 1 Bremischen Beamtengesetz (BremBG) enthaltene Prinzip, daß nur die für das Dienstverhältnis erforderliche Angaben zu erheben sind.

Mein Vorschlag, Personenstandsurkunden und Familienstandsnachweise einschließlich des Urteilstenors von Scheidungsurteilen und für versorgungsrechtliche Entscheidungen die Regelungen über den Versorgungsausgleich nicht in die nicht selten benutzte Grundakten, sondern in die Zahlakte aufzunehmen, ist nicht übernommen worden (Ziffer 10 Abs. 1 Nr. 6). Somit ist nicht ausgeschlossen, daß z. B. Hinweise auf Scheidungen bei Auswahlverfahren, in dnene die Grundakte herangezogen wird, mißbräuchlich verwendet werden können.

8.4.2 Regelungsdefizit bei medizinischen und psychologischen Untersuchungen

Mit dem Inkrafttreten dieser Richlinien erfüllt die SKP nur zum Teil ihre Verpflichtung aus §§ 93 Satz 2, 93a Abs. 2 Satz 5 Bremisches Beamtengesetz (BremBG), wonach die oberste Dienstbehörde das Nähere über Inhalt und Umfang der Personaldatenerhebung, insbesondere auch hinsichtlich medizinischer und psychologischer Untersuchungen, regelt und Verwaltungsvorschriften über die Führung von Personalakten erläßt.

Es fehlen noch die Regelungen zur Datenerhebung bei medizinischen und psychologischen Untersuchungen. Hierzu hat die SKP im Juli 1996 erklärt, daß sich diese in Vorbereitung befänden. Auf meine Anfrage im Januar 1997 hat die senatorische Dienststelle dann mitgeteilt, die Arbeiten daran seien noch nicht abgeschlossen. Im Zusammenhang mit dem Gesetz zur Reform des öffentlichen Dienstrechts würden u. a. Maßnahmen zur Vermeidung der Versetzung in den Ruhestand wegen Dienstunfähigkeit erörtert. Hierzu zähle auch eine gesetzliche Regelung zum Umfang der Auskunftspflicht von Amtsärzten im Zurruhesetzungsverfahren. Erst nach Abschluß des Gesetzgebungsverfahrens könnten die Regelungen abschließend bearbeitet werden. Der Ende Januar erzielte Kompromiß im Vermittlungsausschuß zum dienstrechtlichen Reformgesetz enthält allerdings zu diesem Thema keine Bestimmungen (vgl. die Beschlußempfehlung vom 29. 1. 1997, BT-Drucks. 13/6825).

8.5 Regelanfrage beim Verfassungsschutz aufgehoben

Nach dem sog. „Radikalerlaß" vom 31. März 1977 (Brem.Abl. S. 87) war die Verfassungstreue regelmäßig vor den Neueinstellung aller Richter, Staatsanwälte, Polizei- und Strafvollzugsbediensteten sowie bei Lehrern, Sozialpädagogen, Erziehern und Sozialarbeitern durch Anfrage beim Landesamt für Verfassungsschutz zu überprüfen. Darüber hinaus galt dies auch bei anderen Bewerbern für den öffentlichen Dienst, wenn aufgrund von Tatsachen, die ohne besondere Ermittlungen bekannt waren, Zweifel an der Verfassungstreue bestanden. Aufgrund der öffentlichen Diskussion war diese Regelanfrage am 7. Februar 1983 zunächst lediglich bei Lehrern, Sozialpädagogen, Erziehern und Sozialarbeitern abgeschafft worden (Brem. Abl. S. 197).

Zehn Jahre später erfuhr ich anläßlich der Beratungen zu dem Antrag der CDU-Bürgeschaftsfraktion „Radikale im öffentlichen Dienst" in der Bremischen Bürgerschaft, daß entgegen der Praxis in anderen Bundesländern die Regelanfrage für den Justiz- und den Polizeibereich nach wie vor bestand (Protokoll der 28. Sitzung am 18. Februar 1993). Auf Anfrage der Presse habe ich diese Handhabung als schon aufgrund der historischen Entwicklung in Deutschland überholt und ohne ausreichende Rechtsgrundlage bewertet.

Der Senat hatte dann mit Beschluß vom 26. Oktober 1993 die Senatskommission für das Personalwesen gebeten, hierzu eine Senatsvorlage zu erstellen. Erst nachdem ich immer wieder vergeblich Sachstandsanfragen an die SKP gerichtet und dann im Juli 1995 den Justizsenator um Unterstützung gebeten hatte, kam wieder Bewegung in die Angelegenheit. Der Senat hat mit Beschluß vom 27. Februar 1996 (Brem.Abl. S. 130) die Regelanfrage auch für den verbliebenen Personenkreis aufgehoben. Unberührt bleibt die Möglichkeit, die Verfassungstreue bei Anhaltspunkten im Einzelfall zu überprüfen.

8.6 Unbeschränkte BZRG-Auskunft bei Stellenbewerbern aufgehoben

Die SKP hatte bisher — nach ihren Angaben aus Gründen der Einheitlichkeit — regelmäßig über alle Bewerber für den bremischen öffentlichen Dienst vor der Einstellung eine unbeschränkte Auskunft aus dem Bundeszentralregister (BZR) eingeholt, also eine Auskunft, die auch die aus Resozialisierungsgründen bereits

getilgten Eintragungen enthält. Nach meiner Auffassung entspricht eine solche undifferenzierte Praxis ohne Rücksicht auf Art und Bedeutung des Arbeitsplatzes bzw. Dienstpostens nicht dem Grundsatz der Verhältnismäßigkeit. Bezeichnenderweise hatte auf meine Anfrage hin der Senator für Inneres seinerzeit erklärt, ihm sei kein Fall bekannt, in dem eine unbeschränkte BZR-Auskunft zu einer Ablehnung der Einstellung geführt hätte.

Die SKP hat inzwischen ihre Praxis geändert und Anfang August 1996 mitgeteilt, künftig werde sie bei Neueinstellungen in der Regel auf die Anforderung einer unbeschränkten Auskunft verzichten. Im Gros der Fälle reicht es m. a. W. aus, wie auch in der Privatwirtschaft das sog. „Führungszeugnis" zu verlangen.

8.7 Fall: Vollständige statt Teil-Personalakte an den Amtsarzt

Ein Mitarbeiter einer Dienststelle aus dem Bereich des Senators für Frauen, Gesundheit, Jugend, Soziales und Umweltschutz hat sich darüber beschwert, daß zur Feststellung der Berufsunfähigkeit seine vollständige Personalakte an das Hauptgesundheitsamt (Amtsarzt) weitergeleitet worden ist.

Ich habe die Behörde darauf hingewiesen, daß die nach § 93 e Abs. 1 Satz 3 Bremischen Beamtengesetz (BremBG) zulässige Vorlage der Personalakte an den Amtsarzt gem. Abs. 3 dieser Vorschrift auf den jeweils erforderlichen Umfang zu beschränken ist. Die Akten waren also vor der Weiterleitung auf ihre Relevanz für die medizinische Untersuchung hin durchzusehen.

Die betroffene Behörde hat den Fehler anerkannt und mit der Überlastung des zuständigen Personals erklärt. Der Fall macht deutlich, daß eingefahrene Verhaltensweisen der Verwaltung gerade beim Umgang mit sensiblen Beschäftigtendaten korrekturbedürftig und an die zugunsten des Persönlichkeitsrechts der Mitarbeiter veränderte Rechtslage anzupassen sind.

8.8 Fall: Echt- statt Testdaten im Fortbildungskurs

Ein Teilnehmer an einem Fortbildungskurs des Aus- und Fortbildungszentrums der SKP hat moniert, daß im Rahmen von Übungen am PC Reisekostenfälle mit Echtdaten bearbeitet worden sind. Er konnte auf diese Weise die Einzelheiten von Dienstreisen seiner Kollegen zur Kenntnis nehmen.

Ich vertrete die Auffassung, daß die Nutzung von Echtdaten im allgemeinen, nicht am Arbeitsplatz stattfindenden Fortbildungsveranstaltungen nicht zulässig ist. Vielmehr darf nur mit fiktiven Testdatensätzen gearbeitet werden. Das Aus- und Fortbildungszentrum hat meine Auffassung bestätigt. Allerdings sei der Dozent nicht auf die Authentizität der von der die Kursteilnehmer entsendenden Behörde zur Verfügung gestellten Daten hingewiesen worden. In Zukunft werden in Fortbildungsveranstaltungen vergleichbarer Art darauf geachtet werden, daß keine personenbezogenen Daten verarbeitet werden.

9. Inneres

9.1 „Chaostage" im August 1996: Überprüfung der Speicherungen

9.1.1 Registrierung von (potentiellen) Teilnehmern

Nachdem im Sommer letzten Jahres in Hannover alle Veranstaltungen im Zusammenhang mit den sog. „Chaostagen" verboten worden waren bzw. das Verbot angekündigt war, ergab sich aus den der Polizei vorliegenden Erkenntnissen u. a. aus der „Punker-Szene", daß Bremen als „Ausweichort" dienen sollte. Am 3. und 4. August 1996 kam es in diesem Zusammenhang zu mehreren Hundert von sog. „Ingewahrsamnahmen" durch die Polizei. Die Einzelheiten des Ablaufs sind damals in einer Vielzahl von Presseartikeln geschildert worden. Das Thema wurde auch in der Bürgerschaft am 26. September 1996 behandelt.

Nicht zuletzt aufgrund von Beschwerden und Nachfragen Betroffener habe ich die Datenaufnahme, -registrierung und -verwendung im Zusammenhang mit den polizeilichen Aktionen überprüft. Dabei ging es mir in erster Linie um die Klärung der Verantwortlichkeit innerhalb der Bremer Polizei, die Abgrenzung der Datennutzung zu vollzugspolizeilichen und zu Strafverfolgungszwecken und um die Aufbewahrungsfristen.

Im Oktober 1996 erhielt ich die Auskunft, es seien ca. 310 Personen in Gewahrsam genommen worden. Von ihnen seien teilweise Polaroid-Aufnahmen gefertigt worden. Die Unterlagen über die registrierten Personen befänden sich noch verstreut bei verschiedenen Polizeidienststellen. Es müsse erst noch geprüft werden, wie bzw. wann die Unterlagen ausgewertet und weiterbearbeitet oder vernichtet würden.

Diese Sichtung erfolgte dann ab November 1996 zentral beim Kommissariat K 7, das auch für die Verfolgung von Staatsschutzdelikten zuständig ist. Dort habe ich u. a. Kurzberichte über Straftäter/Störer bei Ingewahrsamnahme, Formulare zur Durchführung der Ingewahrsamnahme, Kopien aus den Gewahrsamsbüchern über den Zeitpunkt der Aufnahme und Entlassung, alphabetisch geordnete Dokumente über ausgesprochene Platzverweise, Formulare über Personenüberprüfungen und Belegungslisten der Gefangenensammelstelle Vahr sowie Polaroid-Lichtbilder vorgefunden. Soweit Strafermittlungsverfahren eingeleitet wurden, z. B. wegen Verstoßes gegen §§ 125, 125 a StPO (Landfriedensbruch), waren die genannten Dokumente zu den Verfahrensakten genommen worden.

9.1.2 Unterschiedliche Verarbeitungszwecke und Löschung

Ich habe gegenüber dem Polizeipräsidium zunächst darauf hingewiesen, daß die gesammelten Unterlagen verschiedenen Zwecken dienen und dementsprechend unterschiedlich zu behandeln sind:

Soweit sie zur Durchführung von Strafermittlungsverfahren benötigt werden, erfolgt die Datenverarbeitung im Rahmen der Strafprozeßordnung (StPO). Insoweit sind die Dokumente auszusondern und den für die Verfolgung der jeweiligen Straftatenkategorie zuständigen Polizeidienststellen zur Verfügung zu stellen. Die weitere Speicherung bzw. die Aufbewahrungsfristen richten sich für diese Unterlagen u. a. nach den Regelungen der Richtlinien über kriminalpolizeiliche Sammlungen (KpS-Richtlinien). Nur soweit es sich um klassische Staatsschutzdelikte handelt, sind diese Vorgänge im Bereich des K 7 weiter zu bearbeiten. Verfahren aufgrund von Anzeigen gegen Polizeibeamte sollen, so wurde mir mitgeteilt, von der Innenrevision beim Polizeipräsidium weiterverfolgt werden. Deshalb sollen die einschlägigen Akten konsequenterweise auch dorthin abgegeben werden.

Der größte Teil der Unterlagen hat jedoch nichts mit dem Staatsschutz zu tun, sondern betrifft den vollzugspolizeilichen Bereich. Sie werden für (mögliche) Verwaltungsstreitverfahren wegen der Platzverweise, Ingewahrsamnahmen etc. benötigt. Diese Akten gehören daher nicht in das Staatsschutzkommissariat. Für die Datenverarbeitung ist materiell Polizei-, nicht Strafprozeßrecht anzuwenden. Aus §§ 11, 31 und 35 Bremisches Polizeigesetz (BremPolG) ergibt sich, daß die Unterlagen, soweit sie nicht im Einzelfall tatsächlich für Ermittlungszwecke oder ein anhängiges Verwaltungsverfahren benötigt werden, spätestens dann gelöscht werden müssen, wenn nicht mehr zu erwarten ist, daß Betroffene sich beschweren werden, spätestens aber nach Ablauf der Rechtsmittelfrist, die in den hier einschlägigen Fällen (Verwaltungsakt ohne Rechtsmittelbelehrung) ein Jahr beträgt.

Einen konkreten Termin für diese Löschung hat das Polizeipräsidium noch nicht verbindlich festgelegt. Nach den Erfahrungen anderer Polizeien in vergleichbaren Fällen sei auch nach einem längeren Zeitraum noch damit zu rechnen, daß beispielsweise Schadensersatzforderungen wegen evtl. Amtspflichtverletzungen geltend gemacht würden, nachdem zuvor Verwaltungsgerichte die Rechtswidrigkeit polizeilichen Handelns festgestellt hätten. Das Polizeipräsidium geht allerdings davon aus, daß die Jahresfrist eingehalten werden kann.

Ich habe die Aufbewahrung dieser Unterlagen unter der Prämisse akzeptiert, daß die Daten lediglich für die genannten Zwecke der Dokumentation polizeilichen Handelns bzw. des Nachweises für evtl. Schadensersatz- oder Amtshaftungsansprüche aufbewahrt werden. Im übrigen war eine Sperrung der Daten nach § 20 Abs. 2 Nr. 2 BrDSG vorzunehmen und ein entsprechender Sperrvermerk anzubringen. Abgesehen von den einer Straftat verdächtigten Personen werden diese Daten weder in die abrufbaren polizeilichen Informationssysteme noch in die erkennungsdienstlichen Dateien eingestellt.

Das Polizeipräsidium ist meinen Vorschlägen und Hinweisen weitgehend gefolgt. Die Aufbereitung der eingegangenen Unterlagen durch das K 7 ist — so das Polizeipräsidium — zwischenzeitlich abgeschlossen.

9.2 Prüfung: Telefonüberwachungs-Maßnahmen durch Polizei

Im Berichtsjahr habe ich die Durchführung von Telefonüberwachungs-Maßnahmen (TÜ-Maßnahmen) in vier Kommissariaten der Bremer und Bremerhavener Polizei mit unterschiedlichen Aufgabenbereichen geprüft. Diese führen alle Arbeitsschritte wie z. B. die Beantragung einer TÜ-Maßnahme bei der Staatsanwaltschaft oder die Erfassung und Auswertung der Aufzeichnungen selbst durch. In Bremen (Stadt) ist geplant, die Durchführung von TÜ-Maßnahmen in absehbarer Zeit bei einer neuzugründenden Organisationseinheit zu zentralisieren.

Meine Überprüfung hat einige Organisationsmängel ergeben, die sich zu Lasten der Betroffenen, d. h. aller abgehörten Telefonteilnehmer, auswirken können. So habe ich z. B. angeregt, daß beim Ausbau des polizeilichen Informationssystems ISA-D sichergestellt wird, daß die zuständigen Kommissariate über den Abschluß eines Verfahrens unterrichtet werden. Nur dann kann die umgehende Vernichtung der in den Kommissariaten noch vorhandenen TÜ-Unterlagen wie Handakten und Arbeitsbänder erfolgen. Oder: Ein Kommissariat übersandte den Gerichtsbeschluß per Fax an den Netzbetreiber. Bei aller Anerkennung der Eilbedürftigkeit muß aber bedacht werden, daß Fernkopieren insbesondere das Risiko enthält, daß auf dem Leitungsweg oder beim Empfänger Unbefugte Kenntnis erlangen. Ich habe daher zu einer verschlüsselten Übertragung geraten.

Drittes Beispiel: Zu dem Programm zur Erfassung und Auswertung der Gespräche habe ich Änderungen angeregt und ausführlich mit dem Polizeiführungsstab besprochen, um die nichtrelevanten Gespräche besser aus der weiteren Bearbeitung herausfiltern zu können.

Die gemeinsam vom Senator für Inneres und vom Senator für Justiz und Verfassung erlassenen „Richtlinien für das taktische Vorgehen anläßlich einer Überwachung des Fernmeldeverkehrs nach §§ 100 a und 100 b StPO vom 1. Juli 1990" waren in den geprüften Kommissariaten nicht bekannt. Ich habe den Senator für Inneres in einem Schreiben darauf hingewiesen und aufgrund meiner Prüfergebnisse eine Anpassung bzw. Ergänzung dieser Richtlinien vorgeschlagen. Präzisere Vorgaben sind u. a. notwendig für die Weitergabe, Aufbewahrung und Vernichtung der TÜ- Unterlagen, zur Behandlung von Verteidigergesprächen, zum Einsatz von Dolmetschern, zum Einblick in die TÜ-Protokolle und zur Gebäudesicherheit. Festlegungen sind auch für die technische Umsetzung, insbesondere die Datensicherheit der bei den eingesetzten PC gespeicherten Daten, vonnöten.

Mein Schreiben ging erst am Ende des Berichtszeitraumes dem Senator für Inneres zu. Eine Antwort steht noch aus. Gleiches gilt für die Ergebnisse der Prüfungen in den einzelnen Kommissariaten, die ich dem Polizeipräsidium Bremen und der Ortspolizeibehörde Bremerhaven schriftlich mitgeteilt habe.

9.3 Meldedaten — Risiken elektronischer Übermittlung

9.3.1 Melderegister ins INTERNET?

Aufgrund der Entwicklungen im Bereich der IuK-Technik gibt es derzeit bei vielen Meldebehörden im Bundesgebiet Überlegungen, Melderegisterauskünfte nicht mehr selbst zu erteilen, sondern durch Einstellung eines Auszugs aus dem Melderegister in Online-Abrufdienste wie z. B. den T-Online-Dienst der Telekom oder durch direkte Anbindung des Melderegisters an das INTERNET den öffentlichen und privaten Interessenten die gewünschten Melderegisterauskünfte zur eigenen Abfrage zur Verfügung zu stellen.

Das Melderegister ist nach seiner Entstehungsgeschichte, seiner Konzeption und der derzeitigen rechtlichen Gestaltung kein öffentliches Register, das jedermann ganz oder in reduzierter Form zur freien Verfügung zugänglich gemacht werden könnte. Es dient nach der melderechtlichen Zielsetzung ausschließlich der Erfüllung ganz bestimmter Aufgaben der Verwaltung und läßt unter bestimmten Voraussetzungen die Weitergabe an andere Behörden und in einem abgestuften System (Grund-, erweiterte Auskunft) auch an private Personen oder Stellen zu.

Alle Einwohner einer Kommune sind kraft Gesetzes unter Bußgeldandrohung verpflichtet, sich anzumelden und Änderungen ihrer Meldeverhältnisse, z. B. Umzüge, Eheschließungen, Geburten etc., mitzuteilen. Der Gesetzgeber hat bewußt auch aus verfassungsrechtlichen Gründen darauf verzichtet, ein bundesweites Einwohnerregister zu schaffen oder eine Verzahnung der vielen kommunalen Einwohnerregister zuzulassen. Die Einstellung der kommunalen Melderegister in ein zentrales, letztlich weltweit zugängliches Online-System oder die

Anbindung der örtlichen Melderegister an das INTERNET-System würde die verfassungsrechtlichen Schranken und gesetzgeberischen Absichten unterlaufen. Der Gesetzgeber hat zudem die Verwendung der regelmäßig übermittelten Meldedaten bestimmten Zweckbindungsregelungen unterworfen und an die Berücksichtigung schutzwürdiger Belange der Betroffenen gekoppelt. Dies bedeutet, daß auch die im Rahmen derartiger Online-Verfahren abgerufenen Meldedaten diesen Beschränkungen unterworfen sind, was aber nicht gewährleistet werden kann.

Diese Möglichkeit könnte allenfalls mit ausdrücklicher Zustimmung der Betroffenen zugelassen werden, wobei zudem noch Sonderregelungen für Minderjährige oder nicht voll Geschäftsfähige vorzusehen wären.

Meine Bedenken habe ich nach einer entsprechenden Anfrage dem Senator für Inneres vorgetragen. Rückäußerungen habe ich nicht erhalten.

9.3.2 Adreßbuchdaten auf CD-ROM

Nach § 33 Abs. 3 Bremisches Meldegesetz (BremMG) dürfen die Meldebehörden Adreßbuchverlagen Auskunft über Namen und Anschrift sämtlicher volljährigen Einwohner geben, wobei die Betroffenen das Recht haben, der Weitergabe ihrer Daten zu widersprechen. Auf das zeitlich nicht befristete Widerspruchsrecht muß die Meldestelle bei der Anmeldung und vor Herausgabe des Adreßbuches, d. h. vor der entsprechenden Datenübermittlung, durch öffentliche Bekanntmachung hinweisen.

In der bisherigen Praxis wurden sowohl in Bremen als auch in Bremerhaven aufgrund eines Vertrages der jeweiligen Verlage mit den Meldebehörden regelmäßig Adreßbücher herausgegeben, wobei in aller Regel in Form eines redaktionellen Zeitungshinweises und in Form einer amtlichen Bekanntmachung auf das Widerspruchsrecht aufmerksam gemacht wurde. Unabhängig von der Tatsache, daß derartige Bekanntmachungen meist überlesen werden und das Widerspruchsrecht selbst nicht sehr bekannt ist, funktioniert dieses Hinweisverfahren in vielen Fällen auch nicht. Bei volljährig werdenden Einwohnern wird ohne Nachfrage automatisch Zustimmung zur Datenübermittlung an Adreßbuchverlage unterstellt, was in vielen Fällen eben nicht angenommen werden kann, wie mir entsprechende Bürgereingaben zeigen. Auch die straßenweise Sortierung der Daten im Adreßbuch bereitet nach wie vor datenschutzrechtliches Unbehagen.

Neuerdings gibt es das Ansinnen, statt der gedruckten Adreßbücher die Adreßbuchdaten auf CD-ROM herauszugeben. Mit Hilfe eines solchen Datenträgers ist es sehr viel leichter möglich, die entsprechenden Meldedaten auf der eigenen Datenverarbeitungsanlage zu verarbeiten. Man kann sie z. B. mit anderen Anschriftenbeständen wie Adreßhandelsdaten oder Telefonkundenverzeichnissen verknüpfen oder in eigene Datenbestände wie etwa Kundendateien einstellen.

Die erhöhten Verknüpfungs- und Sortierungsrisiken der CD-ROM habe ich im letzten Jahresbericht im Zuammenhang mit elektronischen Telefonverzeichnissen thematisiert (vgl. 18. JB, Ziff. 19.1). Die neue Telekommunikationsdienstunternehmen-Datenschutzverordnung (vgl. 18. JB, Ziff. 6.2.6) sieht konsequenterweise ein selektives Widerspruchsrecht des Teilnehmers vor, wonach er der Aufnahme seiner Angaben im klassischen Telefonbuch zustimmen und gleichzeitig der Speicherung auf einer CD-ROM widersprechen kann.

Ich habe gegenüber dem Senator für Inneres und den Meldebehörden erhebliche Bedenken gegen derartige Pläne geäußert. § 33 Abs. 3 BremMG spricht von der Herausgabe eines Adreßbuches, also eines gedruckten Werks. Von CD-ROM oder anderen elektronischen Datenträgern ist in dieser Gesetzesbestimmung nicht die Rede. Zwar ist der Datenträger für die Übermittlung an die Adreßbuchverlage im Meldegesetz nicht vorgeschrieben, was bedeutet, daß die Meldebehörden die Daten auch auf elektronischen Datenträgern wie z. B. Magnetband oder Diskette übermitteln dürfen. Die Nutzung durch die Adreßbuchverlage bleibt ohne Änderung der gesetzlichen Regelung aber auf die Erstellung eines Druckwerks beschränkt.

9.4 Personenstandsgesetz — neuer Anlauf zur Novellierung

Das Bundesministerium des Innern hat im März 1996 einen neuen Vorentwurf zur Änderung des Personenstandsgesetzes vorgelegt. Obwohl die Datenschutzbeauftragten des Bundes und der Länder, so auch ich, die im Hinblick auf die Einhaltung datenschutzrechtlicher Vorgaben im Personenstandswesen dringend erforderliche Gesetzesänderung immer wieder angemahnt hatten, ist dies der erste Anlauf zur Novellierung des bislang geltenden Gesetzes seit fast sieben Jahren.

Im Vergleich zur bisherigen Gesetzeslage enthält der Vorentwurf einige bedeutsame Verbesserungen. So erhält die Ahnenforschung, die in der Vergangenheit oft aufgrund der restriktiven Rechtssituation nicht möglich war, eine klare gesetzliche Grundlage. Auch ist zu begrüßen, daß mit den Bestimmungen des Vorentwurfs erstmals die Übermittlung von Daten des Standesamtes für wissenschaftliche Forschungsarbeiten auf eine gesetzliche Basis gestellt wird.

Zu kritisieren ist die Generalklausel, wonach Übermittlungsbefugnisse des Standesbeamten dann gegeben sind, wenn die Übermittlung zur Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgabe erforderlich ist. Vor dem Hintergrund des Volkszählungsurteils hatten die Datenschutzbeauftragten gefordert, daß der Umfang der Mitteilungspflichten, die Empfänger sowie die Zwecke, zu denen die übermittelten Daten verarbeitet werden dürfen, im einzelnen gesetzlich festgelegt werden. Auch wo im Vorentwurf ausdrücklich Mitteilungspflichten festgelegt sind, wird diesen Anforderungen nicht entsprochen, da entweder der Umfang oder der Empfänger der Übermittlung nicht genau definiert ist.

Soweit den Standesämtern der Einsatz technischer Hilfsmittel gestattet ist, versäumt es der Entwurf, diese zu geeigneten technischen und organisatorischen Sicherungsmaßnahmen zu verpflichten.

Schließlich wären für das Personenstandswesen auch gesetzliche Bestimmungen von besonderer Bedeutung, durch die sich der Schutz des Adoptionsgeheimnisses bei der Unterrichtung der Meldebehörden sowie die Einhaltung des Grundsatzes der Einwilligung des Betroffenen bei der Herausgabe personenbezogener Daten aus den Personenstandsbüchern zum Zwecke der Veröffentlichung gewährleisten ließe; aber auch diese Bestimmungen fehlen.

Ich habe meine Kritik und meine Anregungen zur Verbesserung des Vorentwurfs dem Senator für Inneres mitgeteilt und darum gebeten, sie in das Beratungsverfahren einzubringen. Inwieweit der Senator meiner Bitte nachkommt und ob die genannten Punkte tatsächlich bei der Gesetzgebung Berücksichtigung finden, bleibt abzuwarten.

9.5 „Knöllchen" mit mobilen Erfassungsgeräten

Bereits 1992 war ich bei der Einführung von mobilen Datenerfassungsgeräten zur Überwachung des ruhenden Verkehrs beim Verkehrsüberwachungsdienst des Stadtamtes beteiligt. Nachdem ich davon ausgehen konnte, daß inzwischen ausreichend praktische Erfahrungen gesammelt werden konnten, habe ich das System Ende 1995 geprüft.

Dabei mußte ich feststellen, daß die mir mit dem Antrag auf Einführung der mobilen Datenerfassung zugesandte Programmbeschreibung nicht dem tatsächlich eingesetzten Programm entsprach. Des weiteren fehlten Dateibeschreibung, Geräteverzeichnis, Systemakte und Datenschutzkonzept.

Im Laufe des Jahres 1996 hat das Stadtamt mir aber ein ebenso umfangreiches wie akzeptables Datenschutzkonzept vorgelegt, das u. a. die Beschreibung des aktuellen Programms, das Geräteverzeichnis, die Systemakte und ein Datensicherungs-Konzept enthält.

Unterschiedliche Vorstellungen bestehen jedoch immer noch über die Aufbewahrungsfrist für die Diskettendateien und die im herkömmlichen (manuellen) Verfahren als Papierbelege anfallenden Unterlagen. Die Verwaltungsvorschrift (VV) zu § 71 Landeshaushaltsordung (LHO) sieht eine Frist von fünf Jahren vor. Dies birgt die Gefahr, daß die gesetzliche Tilgungsfrist von zwei Jahren (§ 29 Abs. 1 Straßenverkehrsgesetz i. V. m. § 13 a Straßenverkehrszulassungsordnung) unterlaufen werden kann, weil ein Rückgriff auch nach dieser Zeit noch möglich ist. Hierzu habe ich in früheren Jahresberichten schon Stellung genommen (zuletzt im 14. JB für 1992, Ziff. 2.2.4.1). Aufgrund dieser Prüfung habe ich erneut den Rechnungshof um Mitteilung gebeten, ob er meine Rechtsauffassung teilt oder ob er eine andere Möglichkeit zur Lösung des Zielkonflikts der beiden genannten Regelungen sieht. Der Rechnungshof besteht jedoch auf der längeren Aufbewahrungfrist.

Grundsätzlich vertrete ich jedenfalls die Auffassung, daß Löschungs- und Vernichtungsfristen, die sich aus gesetzlichen Bestimmungen in den Datenschutzgesetzen oder in bereichsspezifischen Einzelgesetzen ergeben, durch Verwaltungsvorschriften und Erlasse nicht verlängert werden können.

9.6 Fall: Ausländerdaten an Privatfirma zwecks Abschiebung

Die Ausländerbehörde Bremen wollte Anfang 1996 mit Hilfe einer Privatfirma („Pandi-Service") Ausländer, deren Staatsangehörigkeit nicht eindeutig feststellbar war, abschieben. Dieses Unternehmen erhielt nicht nur Kopien der Ausreisedokumente; vielmehr wurde ihm zeitweise die gesamte Akte eines Abzuschiebenden überlassen.

Diese Vorfälle wurden in den Bremer Medien ausführlich dargestellt. Meinungsverschiedenheiten bestehen zu der verwaltungs- bzw. ausländerrechtlichen Grundsatzfrage, inwieweit Private zu ausländerpolizeilichen Vollzugsaufgaben, d. h. insbesondere zur Durchführung von Abschiebungen, herangezogen werden können. Fest steht jedenfalls, daß private Gesellschaften (z. B. Reisebüros oder Fluggesellschaften), die im Einzelfall an einer Abschiebung mitwirken müssen, nach § 75 Abs. 2 Ausländergesetz (AuslG) nur die für ihre jeweilige Teilaktivität erforderlichen Daten, wie z. B. Name und Vornamen und Reisepaß, erhalten dürfen. In keinem Fall ist die Zurverfügungstellung der gesamten (ggf. kopierten) Ausländerakte zu rechtfertigen.

Die Ausländerbehörde hat die Beauftragung der Fa. „Pandi-Service" zunächst beendet und zugesagt, mich in Zukunft bei derartigen Plänen wegen der datenschutzrechtlichen Fragen vorher zu beteiligen.

9.7 Fall: Asylbewerberdaten unzulässig nach Zirndorf

Einem Flüchtlingshilfeverein war aufgefallen, daß in Bescheiden des Bundesamtes für die Anerkennung ausländischer Flüchtlinge (BAFl) in der Begründung für die Ablehnung einer Duldung auf Erkenntnisse der Bremer Polizei verwiesen wurde.

Meine Überprüfung ergab, daß zunächst die Polizei die Ausländerbehörde über Strafanzeigen, Platzverbote etc. in korrekter Anwendung von § 76 AuslG unterrichtet hat. Diese Anzeigen hat dann aber die Ausländerbehörde in Kopie weitergeleitet an die Außenstelle Bremen des BAFl. Für diese weitere Datenübermittlung bieten aber weder das Asylverfahrensgesetz noch das Ausländergesetz eine Rechtsgrundlage. Das Bundesamt hat seine Entscheidung ausschließlich nach asylrechtlichen Gesichtspunkten zu treffen: Es entscheidet darüber, ob der Flüchtling als asylberechtigt anzuerkennen ist, weil er aus politischen, rassischen oder religiösen Gründen verfolgt wird. Polizeiliche Erkenntnisse z. B. am Wohnort des Asylbewerbers spielen in diesem Anerkennungsverfahren keine Rolle. Relevant sind diese nur für die Ausländerbehörde bei Entscheidungen und Verfahren nach dem Ausländergesetz, etwa wegen einer Abschiebung.

Die Ausländerbehörde Bremen hat meine Rechtsauffassung schriftlich bestätigt und zugesagt, künftig keine polizeilichen Daten mehr an das BAFl zu übermitteln.

9.8 Sicherheitsüberprüfungsgesetz (SÜG): Neuer Entwurf

Um die Jahreswende 1996/1997 erhielt ich vom Innensenator einen neuen Entwurf zum Bremischen SÜG. Dieses Gesetz soll die alten Sicherheitsrichtlinien ablösen, die das Verfahren zur Überprüfung von Personen regeln, die sog. Geheimsachen (Verschlußsachen) bearbeiten oder in sog. sicherheitsempfindlichen Stellen staatlicher Behörden oder privater Unternehmen beschäftigt werden. Ich hatte in der Vergangenheit immer wieder das Fehlen einer gesetzlichen Regelung für die mit der Sicherheitsüberprüfung verbundenden erheblichen Eingriffe in das Persönlichkeitsrecht der Betroffenen gerügt (zuletzt im 18. JB, Ziff. 7.2.4). Dieser Forderung nach einem Landes-SÜG hatte sich auch der Datenschutzausschuß in seinem Bericht zum 17. Jahresbericht angeschlossen (vgl. Drucks. 14/210, S. 1).

Der jetzige Entwurf baut auf dem Bundes-SÜG von 1994 auf und enthält einige Fortschritte gegenüber früheren Entwurfstexten. So wurde gänzlich auf den sog. personellen Sabotageschutz verzichtet, der in der Vergangenheit immer wieder zu unverhältnismäßig vielen Prüffällen in der Privatwirtschaft geführt hat. Auch sollen Familienangehörige weitgehend aus dem Überprüfungsverfahren herausgenommen werden.

Gleichwohl bleiben einige Kritikpunkte; teilweise geht der bremische Entwurf hinter das Bundes-SÜG zurück. Für nicht sachgerecht halte ich z. B., daß Familienangehörige nicht getrennte, sondern einen gemeinsamen Fragebogen ausfüllen sollen. Auch wende ich mich gegen die Einbeziehung privater Arbeitgeber in die

Abwicklung der Sicherheitsüberprüfung mit der Folge, daß ihnen im Detail sicherheitsrelevante Erkenntnisse bekannt werden. Ich halte eine klare informationelle Trennung zwischen privatrechtlichem Arbeitsverhältnis und staatlichem Überprüfungsverfahren für angebracht. Bei Dienststellen mit nur wenigen Überprüfungsfällen sollte m. E. die Durchführung bei einer Behörde zentralisiert werden, um nicht an zu vielen Ämtern eine Infrastruktur für das SÜG aufzubauen. Zu restriktiv erscheint mir auch der Regelungsvorschlag zum Einsichtsrecht des Betroffenen in seine Sicherheitsakte.

Die dem Bremischen Datenschutzgesetz widersprechende Einschränkung meiner Kontrollbefugnisse kann ich ebensowenig akzeptieren wie das Vorhaben, vom Parlament gewählte Funktionsträger wie z. B. die Mitglieder des Rechnungshofs und den Landesbeauftragten für den Datenschutz nicht aus dem Anwendungsbereich des Gesetzes herauszunehmen.

Meine Änderungswünsche habe ich dem Senator für Inneres in einer umfangreichen Stellungnahme im Februar 1997 mitgeteilt.

9.9 Neues Gewerbe-DV-Verfahren ohne Zugriffstrennung

Vor einem Jahr hatte ich darüber berichtet, daß es in Bremen noch immer kein der novellierten Gewerbeordnung (GewO) angepaßtes Gewerbemelde-DV-Verfahren gibt.

Ich habe vom Stadtamt im Frühjahr 1997 die Anwendungsbeschreibung für ein neues Verfahren erhalten. Es soll eingesetzt werden, ohne die Datenbestände für die Gewerbeanmeldung von denen der Gewerbeüberwachung sauber zu trennen. Dies läßt unberücksichtigt, daß nur ein Teil der angemeldeten Betriebe auch unter die Überwachungsvorschriften der Gewerbeordnung fällt.

In meiner Stellungnahme habe ich daher nicht nur technische Verbesserungsvorschläge gemacht, sondern vor allem auch gefordert, das Gebot der Funktionstrennung bei der Datenverarbeitung einzuhalten: Die für Gaststätten, Makler, Reisebüros, Pfandleiher usw. zuständigen Abschnitte der Gewerbeüberwachung dürfen mithin nur Daten der Gewerbebetreibenden ihres Bereichs abrufen können. Erst recht besteht für diese Abschnitte keine Zugriffsberechtigung für Anmelder, die der Gewerbeüberwachung überhaupt nicht unterliegen.

Trotz mehrmaliger Erinnerung hat sich das Stadtamt bisher nicht zu meiner Stellungnahme geäußert.

10. Justiz

10.1 Staatsanwaltschaftliche Informationssysteme

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

Der Echteinsatz des Systems (zu den jeweiligen Planungsständen vgl. 17. JB, Ziff. 10.3 und 18. JB, Ziff. 12.2) verzögert sich ebenso wie die Fertigstellung des Datenschutzkonzeptes. Mir ist zwar im Berichtsjahr ein Entwurf vorgelegt worden. Dieser Entwurf nimmt aber Bezug auf umfangreiche Anlagen, die mir trotz schriftlicher Anforderungen bis zum Redaktionsschluß nicht vorgelegt worden sind. Er berücksichtigt auch in weiten Teilen meine bisherigen Forderungen nicht (vgl. 18. JB, Ziff. 12.2.2).

Ich hatte im November 1996 anläßlich der Beratung des 18. Jahresberichts Gelegenheit, meine Position im Datenschutzausschuß darzulegen; eine dabei ins Auge gefaßte Besprechung im Hause des Senators für Justiz konnte noch nicht durchgeführt werden. Inwieweit Anforderungen aus dem künftigen Strafverfahrensänderungsgesetz (StVÄG; vgl. u. Ziff. 10.2) das Systemkonzept beeinflussen werden, läßt sich derzeit noch nicht absehen. Jedenfalls will der Datenschutzausschuß die Beratung dann wieder aufgreifen, wenn — was abzusehen ist — die Gespräche mit dem Justizsenator Punkte offen lassen.

Zwar hat mir die Staatsanwaltschaft zugesagt, zu prüfen, ob meine Vorschläge in die Arbeitsgruppe der SIJUS-Anwenderländer eingebracht werden können. Allerdings habe ich inzwischen erfahren, daß die Gruppe beschlossen hat, erst programmtechnisch tätig zu werden, wenn entsprechende Aufträge der einzelnen Landesjustizverwaltungen vorliegen.

10.1.2 Grundsätze für den datenschutzgerechten Einsatz

Um die Diskussion mit den Justizverwaltungen über die datenschutzrechtlichen Vorgaben für staatsanwaltschaftliche Informationssysteme — über einzelne Verfahren wie SIJUS-Straf hinaus — auf eine breitere Basis zu stellen, fand unter meinem Vorsitz im September 1996 eine Arbeitsgruppensitzung mit Teilnehmern von Datenschutzbeauftragten anderer Länder statt. Detaillierte Arbeitsergebnisse wurden zu folgenden System- und Verfahrensaspekten erzielt:

— Zugriffsbeschränkungen für einzelne Anwender,

— Löschroutinen und Zweckbindung der gespeicherten Daten,

— Rechteverwaltung,

— Protokollierung der Zugriffe auf den Datenbestand,

— Verschlüsselung des Datenbestandes innerhalb eines Systems und bei der Datenübertragung,

— Einsatz von PC mit Diskettenlaufwerken,

— Sicherungssoftware und Zugangssicherung,

— Schutz gegen Eigenprogrammierungen,

— Beschränkung der „Allmacht" der Systemverwaltung und Protokollierung von Systemverwaltertätigkeiten.

Das gemeinsam von Juristen und DV-Experten erarbeitete Ergebnispapier bietet eine ausführliche und abgestimmte Grundlage für Datenschutzkonzepte von Informationssystemen der Strafverfolgungsbehörden.

10.1.3 Andere Bundesländer — bessere Datensicherungsmaßnahmen

Bei der Darstellung der Planungen für staatsanwaltschaftliche Informationssysteme in verschiedenen Bundesländern wurde deutlich, daß in Bremen das offenste System eingesetzt werden soll. Zum Teil vorbildliche Vorkehrungen sieht dagegen z. B. das in Schleswig-Holstein eingesetzte Verfahren vor. Es hat fünf angeschlossene Staatsanwaltschaften und besteht aus dem zentralen Großrechner in der Datenzentrale und angeschlossenen Terminals ohne Diskettenlaufwerke. Es sieht umfassende Protokollierungen sowie ein sog. „Datenrumpfungskonzept" vor. Dabei wird der ursprüngliche Datensatz sukzessive entsprechend dem Verfahrensstand verkleinert, so daß nach fünf Jahren nur noch die sog. „Superrumpfdaten" im System verbleiben, die zur Vorgangsverwaltung erforderlich sind. Bereits nach zwei Jahren wird der landesweite Zugriff verhindert. Ein Zugriff auf die gespeicherten Daten ist dann nur noch von der die Angaben einstellenden Staatsanwaltschaft möglich. Nach Ablauf von fünf Jahren kann nur noch ein beschränkter Kreis von berechtigten Personen der einspeichernden Staatsanwaltschaft, wie z. B. die Behördenleitung, auf die Daten zugreifen.

Dieses DV-Konzept macht deutlich, daß auch mit datenschutzfreundlichen Verfahren den Interessen der Staatsanwaltschaften ausreichend Rechnung getragen werden kann und daß die Technik so gestaltbar ist, daß sowohl eine effektive Strafverfolgung als auch die Persönlichkeitsrechte der Betroffenen (Tatverdächtige, Zeugen, Hinweisgeber usw.) gewährleistet werden können.

10.2 Strafverfahrensänderungsgesetz (StVÄG): Kritik des Entwurfs

10.2.1 Neuer Entwurf nach jahrelanger Regelungsabstinenz

Seit Jahren fordern die Datenschutzbeauftragten des Bundes und der Länder gesetzliche Regelungen zur Datenverarbeitung im Strafverfahren. Beschlüsse der Datenschutzkonferenz zu diesem Thema gibt es seit 1980 in regelmäßigen Abständen. Die wichtigsten Anforderungen wurden zuletzt im März 1994 in einer Entschließung zusammengefaßt (vgl. den Beschluß „Informationsverarbeitung im Strafverfahren" vom 9./10. März 1994, abgedr. im 17. JB, Ziff. 20.2). Dennoch gibt es bis heute keine gesetzlichen Regelungen für die Datenverarbeitung in automatisierten staatsanwaltschaftlichen Verfahren, wie sie etwa auch das Land Bremen mit dem DV-Verfahren CANASTA betreibt. Anders ausgedrückt: 13 Jahre nach Festlegung der verfassungsrechtlichen Vorgaben im Volkszählungsurteil des Bundesverfassungsgerichts arbeiten die staatsanwaltschaftlichen Verfahren immer noch, ohne eine normenklare gesetzliche Regelung.

Zwar hat es im Jahre 1988 seitens der Bundesregierung und im Jahre 1994 seitens der Länder einen Vorstoß zur Verabschiedung entsprechender gesetzlicher Regelungen gegeben (vgl. zum StVÄG-Entwurf des Bundesrats 17. JB, Ziff. 10.1). Es kam aber lediglich durch Ergänzung der Strafprozeßordnung zur Einrichtung eines bundesweiten zentralen staatsanwaltschaftlichen Informationssystems (ZStV, zur Kritik an diesem System vgl. 17. JB, Ziff. 10.2).

Die Bundesregierung hat vor kurzem, im Dezember 1996, dem Bundesrat einen neuen Gesetzentwurf zur Änderung der Strafprozeßordnung (StVÄG 1996) zugeleitet (BR-Drucks. 961/96).

Ich habe dem Senator für Justiz und Verfassung in einer ausführlichen Stellungnahme mehr als 20 Vorschläge für Änderungsanträge im Bundesrat unterbreitet. Damit wird deutlich, in welch großem Umfang aus datenschutzrechtlicher Sicht Nachbesserungsbedarf besteht.

10.2.2 Einzelregelungen in der Kritik

Dazu nur einige wenige Beispiele: Der Polizei sollte nicht allein das Entscheidungsrecht darüber überlassen werden, ob sie eine Öffentlichkeitsfahndung der auch eine Abbildung des Betroffenen beigefügt werden darf, einleitet. Angesichts der Tatsache, daß die Staatsanwaltschaft einen Notdienst rund um die Uhr anbieten kann, wenn sie wie in Bremen moderne Telekommunikationstechnik (Handy) einsetzt, kann eine Entscheidung der Staatsanwaltschaft ohne nennenswerten Zeitverlust zu jeder Zeit erreicht werden. Auch habe ich mich gegen eine Vorschrift ausgesprochen, die zwar die Einleitung einer Öffentlichkeitsfahndung von dem Vorliegen der Voraussetzungen eines Haftbefehls abhängig macht, den Ermittlungsorganen aber eine Frist von bis zu einer Woche zur Einholung einer Entscheidung über den Erlaß des Haftbefehls einräumt. Auch hier habe ich angesichts der bei Gerichten und Staatsanwaltschaften auch an Wochenenden organisierten Notdienste vorgeschlagen, daß die Entscheidung über den Erlaß eines Haftbefehls unverzüglich herbeizuführen ist.

Bei der Öffentlichkeitsfahndung habe ich im übrigen insbesondere Vorschläge gemacht, die den dazu auf der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 14./15.03.1996 verabschiedeten Grundsätzen Geltung verschaffen sollen (vgl. u. Ziff. 20.2).

Die Vorschriften zur längerfristigen Observation sehen vor, daß sowohl der Tatverdächtige als auch Dritte über einen Zeitraum von drei Monaten ununterbrochen observiert werden können. Ich habe demgegenüber vorgeschlagen, hier zu unterscheiden und im Falle einer gegen andere Personen als den Beschuldigten gerichteten Maßnahme diese jeweils auf höchstens vier Wochen zu begrenzen.

Bei der Regelung zum Einsichtsrecht in Strafakten habe ich darauf hingewiesen, daß sicherzustellen ist, daß die Datenschutzbeauftragten ihre gesetzlichen Kontrollmöglichkeiten auch gegenüber den Strafverfolgungsbehörden weiterhin uneingeschränkt wahrnehmen können.

Korrekturen habe ich auch zu den Forschungsregelungen und zu den Bestimmungen über Datenübermittlungen an die Geheimdienste für notwendig erklärt.

10.2.3 Unzureichende Dateiregelungen

Besonders bedenklich ist der Abschnitt über die Dateiregelungen in StVÄG. So soll den Strafverfolgungsbehörden ohne Einschränkung erlaubt werden, „für zukünftige Strafverfahren" Daten von Betroffenen zu speichern. Das bedeutet aber, daß sowohl in Bagatellfällen wie auch bei fahrlässig begangenen Taten Personen auch nach Abschluß des Verfahrens weiter in staatsanwaltschaftlichen Informationssystemen gespeichert bleiben können, ohne daß eine Prognose vorgenommen werden müßte, ob sie jemals wieder strafrechtlich in Erscheinung treten werden. Damit kann auch das nach dem Bundeszentralregistergesetz vorgesehene Fristensystem für die Löschung von Verurteiltendaten und die damit beabsichtigte Resozialisierung ausgehebelt werden.

Außerdem sehen die Vorschriften vor, daß Staatsanwaltschaft, polizeiliche Strafverfolgungsbehörden, Gerichte, Strafvollstreckungsbehörden, Bewährungshelfer und Aufsichtsstellen für Führungsaufsicht ohne klare Zweckbindungs- und Zweckbeschränkungsregelungen Daten in gemeinsamen Dateien sowohl in einem Land als auch über Ländergrenzen hinweg verarbeiten dürfen. Mit Hilfe

automatisierter Abrufverfahren soll sich eine Vielzahl von Stellen „bedienen" dürfen. Die klassische datenschutzrechtliche Verantwortlichkeit der „speichernden Stelle" droht damit ebenso verwischt zu werden wie die verfassungsrechtlich gebotene Zweckbindung.

Hinzu kommt, daß im Abschnitt „Dateiregelungen" weder Inhalt noch Umfang der entsprechenden Informationssysteme normiert sind.

Ich habe daher dem Senator für Justiz und Verfassung empfohlen, mit einer Prüfungsbitte an die Bundesregierung den gesamten Komplex der Dateiregelungen noch einmal überarbeiten zu lassen.

Zu meinem Bedauern hat der Justizsenator in den Ausschußberatungen des Bundesrats keinen der von mir vorgeschlagenen Änderungsanträge gestellt. Der Entwurf hat den Bundesrat am 21. Februar 1997 ohne nennenswerte datenschutzrechtliche Verbesserung passiert. Ich hoffe jetzt, daß es meinen Kollegen und mir gelingt, jedenfalls bei den Beratungen im Bundestag noch den einen oder anderen Punkt durchzusetzen.

10.3 Bekanntgabe der Anschriften von Opfern und Zeugen

10.3.1 Gefährdung durch den Täter oder Prozeßgegner

Die Bekanntgabe der Adresse im gerichtlichen Verfahren kann eine besondere Gefährdung für Opfer oder Zeugen darstellen, z. B. für Frauen, die in ein Frauenhaus gezogen sind, um sich vor der Gewalttätigkeit ihrer Ehemänner zu schützen. Zwar lassen sich durch Auskunftssperren im Melderegister und andere Maßnahmen Vorkehrungen treffen, um die Offenbarung des Aufenthaltsortes gefährdeter Personen zu vermeiden. Diese Maßnahmen werden aber in gerichtlichen Verfahren dann wirkungslos, wenn die Adresse durch Angabe in Klage- oder Urteilsabschriften bzw. in sonstigen Schriftstücken doch bekannt wird.

Zur Lösung des Konflikts müssen die konkurrierenden Grundrechte auf rechtliches Gehör und faires Verfahren einerseits und auf Wahrung des Persönlichkeitsrechts und der körperlichen Unversehrtheit andererseits abgewogen werden.

Ich erhalte zu dieser Problematik immer wieder besorgte Eingaben und Anfragen. Zur Klärung der Handhabung im Lande Bremen habe ich mich daher an die hiesigen Amtsgerichte gewandt.

10.3.2 Zur Praxis der bremischen Gerichte

In familienrechtlichen Verfahren reicht das Spektrum von einer großzügigen Beurteilung der Gefährdungskriterien ggf. schon aufgrund der plausiblen Bitte eines/einer Prozeßbeteiligten bis zur Glaubhaftmachung. Bei einem Aufenthalt im Frauenhaus wird — so die Auskunft eines Amtsgerichts — in der Regel auf eine weitere Glaubhaftmachung verzichtet.

Wird ein Antrag auf Geheimhaltung der Anschrift für begründet erachtet, ergreifen die Familiengerichte eine Reihe von Maßnahmen. So kann z. B. die Geschäftsstelle die Worte „Sperrvermerk" oder „Anschrift vertraulich" auf dem Aktendeckel anbringen. Zustellungen und Ladungen gehen dann nur an den Verfahrensbevollmächtigten (z. B. der gefährdeten Frau). Auch in Beschlüssen und Urteilen soll der Aufenthaltsort der Frau in diesen Fällen nicht angegeben werden.

Im Strafprozeß sind in der Anklageschrift grundsätzlich „die Beweismittel" im einzelnen anzugeben (§§ 200 Abs. 1 Satz 2, 409 Abs. 1 Nr. 5 Strafprozeßordnung/StPO). In Rechtsprechung und Fachliteratur wird dazu allgemein die Auffassung vertreten, daß dies auch die Anschrift der Zeugen umfaßt. Auch in der Ladungsmitteilung sind dem Angeklagten die vom Gericht geladenen Zeugen namhaft zu machen und ist ihr Wohn- und Aufenthaltsort anzugeben (vgl. § 222 Abs. 1 Satz 1 StPO). Damit soll der Angeklagte die Möglichkeit erhalten, zur Vorbereitung seiner Verteidigung Erkundigungen über die benannten Zeugen einzuholen. Er hat sogar das Recht, die Aussetzung des Verfahrens zu beantragen, wenn dieser Vorschrift nicht genügt wurde (§ 246 Abs. 2 StPO).

Das Gesetz zur Bekämpfung der Organisierten Kriminalität (OrgKG) aus dem Jahre 1992 hat allerdings den Schutz gefährdeter Zeugen dadurch verbessert, daß bei ihnen die Angabe der sog. ladungsfähigen Anschrift statt der tatsächlichen Wohnadresse ausreichen kann (vgl. § 68 StPO).

Im allgemeinen Zivilprozeß ist nach §§ 253 Abs. 4, 130 Nr. 1 Zivilprozeßordnung (ZPO) grundsätzlich ebenfalls die Angabe der ladungsfähigen (Wohn-)Anschrift des Klägers erforderlich. Wird diese ohne zureichenden Grund verweigert, ist die Klage unzulässig. Nach der Rechtsprechung des Bundesgerichtshofs reicht die allgemeine Befürchtung, von der gegnerischen Partei belästigt zu werden, nicht aus, um die Bekanntgabe der Anschrift zu verweigern. Vielmehr müssen dem Gericht die für die behauptete Gefährdung maßgeblichen Gründe unterbreitet werden, damit überprüft werden kann, ob auf die Mitteilung einer ladungsfähigen Anschrift verzichtet werden kann (BGHZ 102, 332 ff.). Das Kammergericht in Berlin, auf dessen Entscheidungen mich die Justiz in ihrer Stellungnahme ebenfalls hingewiesen hat, erkläre zwar die Angabe der Wohnanschrift im Einzelfall bei schutzwürdigen Geheimhaltungsinteressen für entbehrlich; an diese Voraussetzung seien jedoch strenge Anforderungen zu stellen.

Allerdings sei nach Inkrafttreten des verstärkten Zeugenschutzes im Strafprozeß (s. o.) auch bei der Auslegung zivilprozessualer Bestimmungen eine Tendenz zu einer besseren Sicherung des gefährdeten Klägers feststellbar.

Insgesamt habe ich aus den Antworten den Eindruck gewonnen, daß es den Gerichten wegen der nicht gesicherten Rechtslage sinnvoll erscheint, eine gesetzliche Regelung anzustreben, die auch für das Zivilverfahren den Schutz gefährdeter Personen verbessert. Ich teile diese Auffassung.

Die Beratungen der Datenschutzbeauftragten zu diesem Bereich werden fortgeführt.

10.4 Schuldnerverzeichnis: Übermittlung in maschinenlesbarer Form

Die Gerichte im Geschäftsbereich des Senators für Justiz und Verfassung wollen in Zukunft Abdrucke des Schuldnerverzeichnisses auch auf elektronischen Datenträgern den berechtigten Beziehern zur Verfügung stellen. Eine solche Möglichkeit sieht die Vorschrift des § 915 d Abs. 1 Satz 1 ZPO vor.

Der Senator beabsichtigt, den Gerichten für diese Form der Datenübertragung Vorgaben zur Datensicherung zu machen und hat mir dazu einen Regelungsentwurf übersandt. Ich habe nach Recherche der Praxis in anderen Ländern darum gebeten, diesen Text zu ergänzen.

Für erforderlich halte ich die Verschlüsselung auf den Datenträgern, da es sich um Angaben mit hohem Schutzbedarf handelt. Zur Wahrung der Übermittlungssicherung und von Integrität und Authentizität sollte die Verwendung von kryptografischen Verfahren (Prüfsummenverfahren, digitale Signatur) geprüft werden. Erforderlich sind auch verbindliche Angaben über die Datenlöschung bzw. Regelungen für die Rückgabe nicht mehr benötigter Datenträger, um zu verhindern, daß bei den Empfängern inaktuelle Datenbestände vorhanden sind. Vorgaben sind schließlich für die Verwendung der Daten zu machen. Dazu gehören etwa die ordnungsgemäße Behandlung der Schuldnerdaten, ihre gesonderte Aufbewahrung und die Zugriffssicherung. Die Empfänger sind auch klar darauf aufmerksam zu machen, daß sie die erhaltenen Informationen nur für den Zweck der Bonitätsbeurteilung im Geschäftsverkehr nutzen dürfen.

Meine Vorschläge werden z. Z. im Hause des Senators für Justiz und Verfassung geprüft.

10.5 Justizvollzug

10.5.1 Zustellung von Schriftstücken mit JVA-Adresse

Von Strafgefangenen erhielt ich Beschwerden, wonach vom Amtsgericht den Prozeßgegnern in Mahnsachen wie auch in einem Prozeßkostenhilfe-Verfahren ihre Anschrift in der Justizvollzugsanstalt (JVA) bekanntgegeben worden sei. Ich habe daraufhin das Amtsgericht angeschrieben und darauf hingewiesen, daß in der Regel ein Interesse des Strafgefangenen unterstellt werden könne, daß sein momentaner Aufenthaltsort nur in unvermeidbaren Fällen dritten Personen bekannt werde.

Der Präsident des Amtsgerichts hat mir daraufhin mitgeteilt, daß entsprechend einer Anordnung des Geschäftsleiters des Amtsgerichts der Schriftverkehr mit Insassen einer JVA nur über die Straße und die Hausnummer, aber ohne den Zusatz „JVA" abzuwickeln sei. Da diese Anordnung in einigen Fällen nicht eingehalten worden sei, habe er die Eingaben noch einmal zum Anlaß genommen, die betreffenden Mitarbeiter ausdrücklich auf deren Beachtung hinzuweisen.

10.5.2 Aufbewahrung von Krankheitsunterlagen

Bereits bei meiner Datenschutzprüfung im Jahre 1993 in der JVA Oslebshausen (vgl. 16. JB, Ziff. 6.1) habe ich festgestellt, daß die gesundheitlichen Unterlagen von Gefangenen viel zu lange nach deren Ausscheiden aus einer Vollzugsanstalt aufbewahrt werden. Nach den für diesen Bereich geltenden Bestimmungen über die Aufbewahrungsfristen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden (AufbwBest) werden diese Akten 50 Jahre lang aufbewahrt. Ich habe mich immer wieder mit Hinweis auf die kürzeren Fristen in der Ärztlichen Berufsordnung (mindestens 10 Jahre) und im Krankenhausdatenschutzgesetz (längstens 30 Jahre) für eine Verkürzung auch bei den Vollzugsanstalten eingesetzt.

Nach Auskunft des Senators für Justiz und Verfassung besteht inzwischen eine Abstimmung zwischen den Landesjustizverwaltungen, wonach für die nächste Änderung der bundeseinheitlichen Aufbewahrungsbestimmungen eine Senkung der Frist auf 30 Jahre vorgesehen ist. Im Vorgriff darauf habe er für seinen Geschäftsbereich angeordnet, daß bereits so verfahren werden solle.

10.5.3 Aufbewahrung von Besucherlisten

Nachdem ich erfahren hatte, daß Personalien von Besuchern in der JVA sogar nach Beendigung der Haftzeit des besuchten Insassen in der Gefangenenpersonalakte gespeichert bleiben, habe ich um eine Überprüfung dieser Handhabung gebeten. Mangels anderweitiger spezieller Verarbeitungsregelungen müßten die allgemeinen Regelungen des BrDSG Anwendung finden, wonach personenbezogene Daten zu löschen sind, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung ihrer Aufgaben nicht mehr erforderlich ist (§ 20 Abs. 3 Nr. 2 BrDSG).

Auch hier hat der Senator für Justiz und Verfassung eine Umfrage unter den Justizministerien und -senatoren der Länder abgewartet, bevor er mich im Sommer 1996 über die in Kraft gesetzten Regelungen informiert hat. Danach sind die Besucherscheine nach Übertragung der Daten in die Besuchskartei sofort zu schreddern. Die Besuchskartei wird nicht mehr zur Personalakte genommen, sondern nach Entlassung aus der Untersuchungshaft oder der Strafhaft ebenfalls vernichtet. Der Datenschutz erweist sich in diesem Beispielsfall wie so häufig auch als Mittel der Rationalisierung und Verschlankung von Verwaltungsabläufen.

11. Gesundheit, Jugend und Soziales

11.1 Regelungsaktivitäten im Gesundheitsbereich

11.1.1 Umsetzungsdefizite

Das Gesundheitswesen ist Gegenstand lebhafter und strittiger öffentlicher Debatten auf Bundesebene — in erster Linie unter dem Aspekt der Finanzierung. Derzeit scheint sich der Streit auf die Frage zu reduzieren, zu wessen Lasten gespart wird. Dabei geht es auch um Kontrolle und damit um Datenverarbeitung. Betroffene können Krankenkassen, Beitragszahler, Pharmaunternehmen, Leistungserbringer (d. h. Ärzte, Apotheken, Krankenhäuser und viele andere Beteiligte), aber auch und — so befürchte ich — auf Dauer vor allem die Patienten/Versicherten sein. Ich habe mich immer wieder an der Auseinandersetzung beteiligt und dabei das Ziel verfolgt, die Persönlichkeitsrechte und den Schutz der medizinischen Daten der Patienten/Versicherten sichern zu helfen (vgl. ausführl. 18. JB, Ziff. 15.1).

Auch auf Landesebene ist eine rege Gesetzgebungsaktivität zu verzeichnen. Hier geht es vor allem um zeitgemäße Regelungen der Aufgaben der Gesundheitsdienste und -berufe. Durchweg hat mich die Verwaltung bei der Vorbereitung der Gesetzgebungsvorhaben beteiligt und die datenschutzrelevanten Regelungen mit mir bereits vorher abgestimmt.

Zwei Neuregelungen sind bereits 1995/96 in Kraft getreten; gleichwohl ist ihre Umsetzung noch nicht abgeschlossen.

Zur Umsetzung des Gesetzes über den Öffentlichen Gesundheitsdienst (vgl. 18. JB, Ziff. 7.1.2) bedarf es der noch ausstehenden Rechtsverordnung über den Umfang der Erhebung und Speicherung, die Speicherungsdauer und die Zweckbindung der Patientendaten, vor allem auch als Grundlage für deren ordnungsgemäße automatisierte Verarbeitung (vgl. 18. JB, Ziff. 11.4).

Die Ärzte- und die Zahnärztekammer haben bislang die ihnen durch das Bremische Heilberufsgesetz (vgl. 18. JB, Ziff. 7.1.3) auferlegte Pflicht nicht erfüllt, in ihren Berufsordnungen die rechtlich gebotene Verantwortung der Ärzte und Zahnärzte für die Einhaltung ihrer beruflichen Schweigepflicht beim Verkauf ihrer Praxis festzuschreiben, d. h. sich um die Einwilligung ihrer Patienten zu bemühen, bevor sie deren Unterlagen ihren Praxisnachfolgern übergeben. Bundesweit ist es Ziel der Ärzte- und Zahnärztekammern, die Verkäufer einer Praxis von jeder Verantwortung freizustellen und lediglich die Praxisnachfolger in die Pflicht zu nehmen, die ihnen übergebenen Patientenunterlagen unter Verschluß zu halten und nur mit Einwilligung des jeweiligen Patienten einzusehen. Dies aber wird der Rechtsprechung des Bundesgerichtshofs nicht gerecht.

11.1.2 Neuregelungen in Vorbereitung

Die drei Regelungsvorhaben des Gesundheitssenators, über die ich im 18. Jahresbericht unter Ziff. 7.2.1 bis 7.2.3 berichtete, sind noch nicht abgeschlossen:

Derzeit beteilige ich mich an der Vorbereitung des Bremischen Krebsregistergesetzes mit dem Ziel, daß zum einen die bundesgesetzlich vorgegebene Anonymisierung der im Krebsregister gespeicherten Krankendaten angesichts der Forderung von seiten der Forschung nach kleinräumlicher Zuordnung der Daten nicht aufgehoben wird und daß zum anderen durch die Angliederung des Krebsregisters an Stellen, die Daten von krebskranken Patienten auch zur Erfüllung anderer Aufgaben verarbeiten, die gesetzlich gebotene Zweckbindung der Registerdaten nicht aufgehoben wird.

Wenn die bewährten Regelungen des Bremischen Krankenhausdatenschutzgesetzes inhaltlich nicht abgeschwächt werden, habe ich nach wie vor keine Bedenken gegen ihre Eingliederung in ein umfassendes Bremisches Krankenhausgesetz.

Beim Entwurf des Gesetzes für Psychisch Kranke ist strittig, ob und wenn ja, auf wessen Veranlassung und unter welchen Voraussetzungen die zur Entscheidung über die Einweisung eines Kranken in ein psychiatrisches Krankenhaus durch den Sozialpsychiatrischen Dienst eines Gesundheitsamtes erstellten Gutachten Ordnungsbehörden wie etwa der Führerscheinstelle zugeleitet werden dürfen oder gar müssen. Ein vom Innenressort vorgelegter Regelungsvorschlag hätte zur Konsequenz, daß psychisch Kranke, die einen Führerschein haben, nach einer Einweisung generell unter Heranziehung des psychiatrischen Gutachtens auf ihre Fahrtauglichkeit überprüft werden könnten. Das Gesundheitsressort will demgegenüber die Überprüfung auf die Fälle beschränkt sehen, in denen konkrete Anzeichen dafür bestehen, daß der Kranke, setzte er sich an das Steuer, sich oder andere gefährden würde. Ich werde mich dafür einsetzen, daß die ärztliche Schweigepflicht und die bereits im Bremischen Datenschutzgesetz und im Gesetz über den Öffentlichen Gesundheitsdienst garantierten Zweckbindungsgebote gerade beim Umgang mit den psychiatrischen Gutachten nicht über das unbedingt erforderliche Maß hinaus eingeschränkt werden.

11.2 ZKH Bremen-Ost: Fristverlängerung für Datenschutzkonzept

Aufgrund der geplanten umfassenden Veränderungen im EDV-Bereich im Zusammenhang mit der Erstellung eines neuen Organisationskonzeptes hatte ich dem Krankenhaus Bremen-Ost eine Fristverlängerung bis zum Ende des Berichtsjahres gewährt. Das Krankenhaus hat kürzlich ein umfassendes Datenschutzkonzept vorgelegt.

Die Überprüfung dieser Unterlage war bis Redaktionsschluß noch nicht abgeschlossen. Erst danach lassen sich abschließend die Fragen beantworten, ob die in meinem 18. Jahresbericht (Ziff. 15.4.3) benannten datenschutzrechtlichen Mängel damit behoben sind und ich endgültig von einer Beanstandung gem. § 29 BrDSG absehen kann.

11.3 Gesundheitsamt Bremen: Sensible Daten im Netz

11.3.1 Abteilungsübergreifende Netzstruktur

Das Gesundheitsamt Bremen plant eine abteilungsübergreifende Netzinfrastruktur (vgl. zur Datenverarbeitung im Gesundheitsamt 18. JB, Ziff. 15.3).

Zunächst sind Abteilungsnetze (dezentrale Netze) für folgende Bereiche unter dem Netzbetriebssystem Windows-NT 3.51 geplant:

— Haushaltsstelle (Sachgebiet 12),

— Amts- und vertrauensärztlicher Dienst (Sachgebiet 20),

— Gesundheit und Umwelt (Sachgebiete 30, 31, 32).

Als 2. Stufe wird die Verbindung der dezentralen Netze über das durch das Netzbetriebssystem Windows-NT realisierbare Master Domain Modell angestrebt, das die Strukturierung der Ressourcen im Netz in mehrere Domänen bei gleichzeitig zentraler Administration erlaubt. Die hierbei entstehenden technischen Abschottungsmaßnahmen sollen zu gegebener Zeit mit mir abgestimmt werden.

Parallel zur Planung der unter den Punkten 1 und 2 genannten dezentralen Netze sind aufgabenbezogene Datenschutzkonzepte entwickelt worden, die frühzeitig mit mir abgestimmt wurden bzw. sich noch im Abstimmungsprozeß befinden. Darüber hinaus ist eine Anweisung zur Planung und Nutzung dezentraler DV-Systeme im Gesundheitsamt erstellt worden, die datenschutzgerechte Empfehlungen enthält.

11.3.2 Netz im amts- und vertrauensärztlichen Dienst

Von besonderer datenschutzrechtlicher und -technischer Bedeutung ist wegen der Sensibilität der zu verarbeitenden Daten die Inbetriebnahme eines Windows-NT-Netzes im amts- und vertrauensärztlichen Dienst. Dies gilt sowohl wegen der Komplexität der Mechanismen der Kontrolle von Zugriffsrechten als auch wegen der Sicherheitslücken im Netzbetrieb (vgl. ausführlich o. Ziff. 6.2.). Zu beiden Aspekten habe ich eine umfassende Stellungnahme mit Schwachstellenanalyse und Maßnahmenkatalog erarbeitet, die hier aus Raumgründen nicht wiedergegeben werden kann.

Mit dem Gesundheitsamt ist vereinbart, das bereits in den Grundzügen festgelegte Datenschutzkonzept gemeinsam zügig fortzuentwickeln. Zielsetzung ist, sowohl die komplexen, bereits in den Kern des Betriebssystems integrierten Mechanismen zur Datensicherheit und zum Schutz von Systemressourcen optimal zu konfigurieren als auch die im Netz vorhandenen Sicherheitslücken durch zusätzliche Produkte zu schließen. Ich erhoffe mir aus dieser engen und arbeitsaufwendigen datenschutzrechtlichen und datensicherheitstechnischen Begleitung des Netzprojekts exemplarische Erkenntnisse auch für viele andere Vernetzungsvorhaben in der bremischen Verwaltung.

11.4 Sozialpsychiatrischer Dienst: Software-Anpassung an Vorgaben des ÖGD-Gesetzes

Als psychiatrische Institutsambulanz rechnet der sozialpsychiatrische Dienst seine Behandlungsleistungen mit den Krankenkassen ab. Das Erfordernis, entsprechende Abrechnungsunterlagen EDV-gerecht einreichen zu müssen, führte zunächst zu der Vorstellung, auf einem isolierten PC eine in erster Linie für Arztpraxen entwickelte Standardsoftware einzusetzen, deren Funktionsumfang das für den Zweck der Abrechnung erforderliche Maß weit überschritt (vgl. 18. JB, Ziff. 15.3.3).

Der sozialpsychiatrische Dienst hat nunmehr mit der Entwicklungsfirma vereinbart, den Funktionsumfang der Standardsoftware den Anforderungen des Bremischen Gesetzes über den Öffentlichen Gesundheitsdienst (ÖGDG) anzupassen.

Da die hierfür grundlegende Rechtsverordnung (33 Abs. 3 ÖGDG) noch nicht vorliegt, konnte bisher der entsprechende Entwicklungsauftrag noch nicht vergeben werden.

11.5 PROSOZ: Sicherheitslücken trotz Fortentwicklung des Datenschutzkonzepts

11.5.1 Mängel trotz Kompromißlösung

Die Funktionserweiterungen des dialogorientierten Sozialhilfeberechnungsverfahrens PROSOZ (vgl. 16. JB, Ziff. 8.7.2, 17. JB, Ziff. 12.3.1 und 18. JB, Ziff. 14.3.1) im Bereich der ADV-Verbindungsstelle und an den Arbeitsplätzen der Sachbearbeiter/-innen und der Dienststellenkoordinatoren/-innen machten eine Aktuali-

sierung des Datenschutzkonzeptes und den Einsatz zusätzlicher technischer und organisatorischer Datenschutzmaßnahmen erforderlich. Meine Forderungen orientierten sich dabei an der im Zusammenhang mit der Erweiterung des PROSOZ-Verfahrens um Textverarbeitung von der senatorischen Dienststelle getroffenen Aussage, daß der im bisherigen Datenschutzkonzept festgelegte Sicherheitsstandard erhalten bleiben müsse (vgl. 16. JB, Ziff. 8.7.2).

Aufgrund der Differenz zwischen den von mir geforderten Maßnahmen zur Erhaltung dieses Niveaus und dem von der senatorischen Dienststelle für vertretbar erklärten Aufwand kam es zu einer Kompromißlösung (vgl. 17. JB, Ziff. 12.3.1.2), deren Umsetzung ich anhand einiger ausgewählter Kriterien überprüft habe (vgl. 18. JB, Ziff. 14.3.1). Zu den dabei festgestellten Mängeln habe ich im Berichtsjahr keine Stellungnahme erhalten. Die im Nachgang zur Prüfung von mir angeforderten Dokumentationen des Datenschutzbeauftragten wurden mir bislang nicht zur Verfügung gestellt.

11.5.2 Neue Bestandsaufnahme

Dadurch wurde im Berichtsjahr eine erneute Bestandsaufnahme unter Hinzunahme des Kriteriums der Protokollierung (Revisionsfähigkeit des Verfahrens) erforderlich und führte zu folgendem Ergebnis:

Meine These, daß die im Rahmen der Öffnung eines ehemals geschlossenen technischen Systems entstandenen Datensicherungslücken durch nachträgliche organisatorische Maßnahmen und technische Restriktionen nicht aufgefangen werden, hat sich bestätigt. Bereits im Datenschutzkonzept verankerte und mit der senatorischen Dienststelle einvernehmlich ausgehandelte Maßnahmen wurden insbesondere aus angeblichen Verfahrenszwängen sowie Gründen der Praktikabilität und des erwarteten Aufwands (vgl. die Stellungnahme des Senats zu meinem 18. JB, Bürgerschafts-Drucks. 14/499, Ziff. 5.4) auch in diesem Berichtsjahr nicht umgesetzt. Ausnahme ist lediglich, daß nunmehr die ADV-Verbindungsstelle den Sachbearbeitern/-innen einen automatisch erstellten Beleg zuschickt, wenn sie deren Zugriffsberechtigung übernommen hat.

Einen massiven Datenschutzverstoß stellt die Abschaltung der bei ID-Bremen zu führenden Protokollierung dar. Die Protokollierung der Datenzugriffe ist unverzichtbarer Bestandteil eines funktionsfähigen Datensicherungskonzepts, auch und gerade bei sensiblen Daten. Ein von mir angeforderter und nach vorgegebenen Kriterien auszuwertender Protokollauszug (vgl. 17. JB, Ziff. 12.3.1.2) konnte bis Redaktionsschluß nicht vorgelegt werden. Die senatorische Behörde hat Mitte Februar 1997 diese Vorlage noch einmal verschoben und die erneute Verzögerung mit Hinweis auf die Umstellung auf eine neue Programmversion erklärt. Sollte ich nicht zum jetzt zugesagten Zeitpunkt Anfang April 1997 den Protokollausdruck erhalten, werde ich die bisher zurückgestellte förmliche Beanstandung nach § 29 Abs. 2 BrDSG aussprechen. Außerdem müssen noch Detailfragen wie Protokollinhalt, Zugriffsschutz für die protokollspeichernde Datenbank sowie Auswertungskriterien und Dauer der Speicherung mit mir abgestimmt werden.

12. Umweltschutz

12.1 Stundungsanträge für Abwassergebühren: Fragebögen „entschlackt"

Immer wieder ärgern sich Bürger über den Umfang von Fragebögen, die sie auf den Ämtern ausfüllen müssen. Der Wissensdurst der Behörde erweist sich bei Nachfrage dann häufig als nicht real, sondern als Vollzug von Verwaltungsroutine und/oder Gedankenlosigkeit bei der Gestaltung der Vordrucke. Wenn der Fragebogen aber schon zu lang geraten ist, kommt es entscheidend auf die Bereitschaft der betroffenen Dienststelle an, ihn zu ändern und auf die tatsächlich relevanten Angaben zu konzentrieren. Zusatzeffekt: Je weniger Bürgerdaten zu verwalten sind, desto rationeller kann Verwaltung arbeiten.

Dazu folgendes positive Beispiel: Aufgund mehrerer Anfragen habe ich mir von der Umweltbehörde die Fragebögen für die Prüfung der Voraussetzungen für die Stundung von Abwassergebühren und Kanalanschlußbeiträgen vorlegen lassen, mit denen Daten über Vermögens- und Einkommensverhältnisse von Antragstellern (Eigentümer und Erbbauberechtigte) erhoben werden. Die Vordrucke enthielten sehr detaillierte Fragen, u. a. zu allen zur Haushaltsgemeinschaft gehörenden Personen (Vor- und Zuname, Alter, Beruf, Verwandtschaftsverhältnis, Art des Einkommens).

Ich habe Zweifel geäußert und um Überprüfung gebeten, ob wirklich alle diese Daten zur Feststellung erforderlich sind, ob im Hinblick auf besondere Umstände für den Antragsteller eine offenbare Härte vorliegt. Daraufhin hat die Umweltbehörde die Formulare „entschlackt" und die gestellten Fragen deutlich reduziert.

12.2 Abfallgebührenabrechnung in Großwohnanlagen: Kein Datenschutzproblem

Die Berechnung der Abfallgebühren „pro Kopf" in Großwohnanlagen scheitert nicht am Datenschutz, sondern ist jederzeit möglich, wenn sich die Bremer Entsorgungsbetriebe (BEB) und die jeweiligen Vermieter, insbesondere die Wohnungsbaugesellschaften, auf ein entsprechendes Abrechnungsverfahren verständigen. Die immer wieder aufgestellte Behauptung vom Datenschutz als Hindernis für die verursachergerechte Zuordnung von Müllgebühren konnte in der Sitzung des Datenschutzausschusses am 10. September 1996 im Beisein der Vertreter von BEB, Umweltsenator und Gewoba eindrucksvoll widerlegt werden (vgl. o. Ziff. 7.1.2).

Die Umweltbehörde prüft inzwischen die Variante, dem Grundstückseigentümer in diesen Fällen eine Aufschlüsselung für die einzelnen Mieterhaushalte mit Hilfe eines erweiterten differenzierten Gebührenbescheides zu ermöglichen.

Dies setzt voraus, daß die BEB von den Wohnungsbaugesellschaften als Vermieter die dafür erforderlichen personenbezogenen Daten über die Mieterhaushalte erhält und diese Angaben für die Erstellung der verursacherbezogenen detaillierten Gebührenbescheide verarbeiten kann. Ich habe vorgeschlagen, eine entsprechende ergänzende Regelung in das Ortsgesetz über die Entsorgung von Abfällen in der Stadtgemeinde Bremen aufzunehmen. Bis Redaktionsschluß stand noch nicht fest, ob und ggf. wann diese Gesetzesänderung eingeleitet wird.

12.3 BEB: Vorbildliches Datenschutzkonzept

Die Bremer Entsorgungsbetriebe (BEB) hatten mich gebeten, die aufgrund der völlig veränderten EDV-Landschaft notwendige Überarbeitung des vorhandenen Datenschutzkonzepts von 1990 beratend zu begleiten. Das neu zu entwickelnde Rahmenkonzept soll als Richtlinie für den Einsatz vernetzter Systeme dienen und die Grundlage für die Arbeit mit den Einzelplatz-PC bilden. Ein Grundprinzip ist bei der Umsetzung der technischen und organisatorischen Maßnahmen gem. § 7 BrDSG die Notwendigkeit der Differenzierung für die Betriebssystem- und die Anwendungsebene.

Die Beratungsgespräche waren sehr eingehend und für beide Seiten zeitaufwendig. Ich habe trotz begrenzter Technikkapazität in meinem Amt diesen Aufwand deshalb nicht gescheut, weil sich in Zusammenarbeit mit einem kooperationswilligen und datenschutzbewußten Anwender Lösungen finden lassen, die als Beispiel und Beratungsgrundlage für viele andere Behörden und Unternehmen dienen können. Im Ergebnis wurde mir von den BEB ein vorbildliches Rahmenkonzept vorgelegt. Hervorheben möchte ich nur folgende zentrale Punkte:

- Das Geräteverzeichnis und auf den einzelnen PC installierte Software werden softwareunterstützt dokumentiert und beim Einsatz von Spezialsoftware durch das für die Auftragsvergabe erforderliche Pflichtenheft ergänzt.
- Je nach Sensibilität werden die Daten unterschiedlichen Schutzstufen zugeordnet.
- Identifizierende Daten wie Name, Straße etc. werden anonymisiert, sobald sie für die Aufgabenerfüllung nicht mehr erforderlich sind, spätestens aber nach einem Jahr.
- Auf den PC, auf denen die Verarbeitung sensibler personenbezogener Daten (z. B. Beschäftigtendaten) erfolgt, wird durch Einstellung im BIOS das Booten vom Diskettenlaufwerk und das Schreiben auf Diskette verhindert.
- Sensible personenbezogene Daten werden programmtechnisch verschlüsselt auf der Festplatte gespeichert und bereits nach drei Monaten anonymisiert.

Neben vielen weiteren Vorkehrungen auf der Betriebssystem- wie auf der Anwendungsebene sind noch die umfassende Protokollierung bei der Datenübermittlung und die ausführlichen Datenschutzregelungen in den Verträgen mit Fernwartungsfirmen erwähnenswert. Vorbehalten habe ich mir eine Beteiligung bei

der Umsetzung von Schnittstellen für Datenübermittlungs- bzw. Datenübernahme-Aufgaben sowie eine einzelfallbezogene Beurteilung der Erforderlichkeit einer verschlüsselten Datenübertragung.

13. Arbeit

13.1 Europäischer Sozialfonds: Neue Verwaltungs- und Controlling-Software

Im Mai 1994 war die Datenverarbeitung im Antragsverfahren Europäischer Sozialfonds (ESF) bereits Gegenstand einer datenschutzrechtlichen Beratung (vgl. dazu 17. JB, Ziff. 13.3.1). Sowohl auf der Programmebene (Abrechnung mit dem Bundesministerium für Arbeit und Sozialordnung/EU) als auch auf der Projektebene (Bearbeitung der Anträge der Projektträger) wurden keine personenbezogenen Daten von Teilnehmern/-innen verarbeitet.

Entsprechend der damals getroffenen Verabredung, mich vor der automatisierten Verarbeitung personenbezogener Daten von Teilnehmern/-innen insbesondere im Hinblick auf die gem. § 7 BrDSG zu treffenden technischen und organisatorischen Maßnahmen zu beteiligen, wurde mir im Mai 1996 ein erster Entwurf eines Datenverarbeitungs- und Datensicherungskonzepts für den Einsatz einer neuen ESF-Verwaltungs- und Controlling-Software im Referat 42 des Senators für Arbeit vorgelegt.

Neu gegenüber dem bisherigen Verfahren ist die Hinzunahme von Evaluations- und Abrechnungsdaten und somit auch personenbezogener Daten von Teilnehmern/-innen. Deswegen sind entsprechende Datenschutz- und Datensicherungsmaßnahmen erforderlich. Besondere Vorsicht ist geboten im Hinblick auf Teilnehmer/-innen an Beratungsprojekten angesichts des Gebotes der Vertraulichkeit der Beratung. Anders ausgedrückt: Kontrolle der Teilnahme darf nicht zur Kontrollierbarkeit der Teilnehmer/-innen mutieren.

Die Datenschutzmaßnahmen sind sowohl beim Senator für Arbeit (Verwaltung u. Controlling) als auch beim Arbeitsförderungszentrum des Landes Bremen GmbH (Evaluation) und bei den einzelnen Projektträgern zu treffen, die die neue Software ebenfalls zur Automatisierung ihrer Verarbeitung zwingt. Für die Evaluation beim Arbeitsförderungszentrum kommt es entscheidend darauf an, Verknüpfungen der für diesen Zweck genutzten Daten mit anderen Angaben und damit die Möglichkeit der Reidentifizierung aus aggregierten Teilnehmerzahlen zu verhindern.

Der Senator für Arbeit hat versichert, erst nach Vorlage aller Unterlagen und entsprechender Umsetzung der notwendigen Maßnahmen sollten Daten von Teilnehmer/-innen personenbezogen im Echtbetrieb verarbeitet werden.

14. Häfen und überregionaler Verkehr

14.1 Neues Straßenverkehrsgesetz

14.1.1 Erster Durchgang im Bundesrat abgeschlossen

Nachdem seit drei Jahren der Entwurf eines neuen Straßenverkehrsgesetzes immer wieder — auch unter Beteiligung der Datenschutzbeauftragten — überarbeitet worden ist, steht das Gesetzgebungsverfahren kurz vor dem Abschluß. Der Bundesrat hat im ersten Durchgang in seinem Beschluß vom 19. Dezember 1996 (BR-Drucks. 821/96) zu dem Gesetzentwurf der Bundesregierung Stellung genommen. Die Bundesregierung hat ihre Gegenäußerung Anfang Februar 1997 vorgelegt und dabei eine Reihe von Änderungswünschen des Bundesrats abgelehnt (BT-Drucks. 13/6914 vom 07.02.97, S. 116 ff.). Über den ersten Entwurf und meine Stellungnahme gegenüber dem damals zuständigen Senator für Inneres und Sport hatte ich in meinem 16. Jahresbericht (Ziff. 5.3) berichtet. Auch gegenüber dem neuen Entwurfstext bleiben meine damaligen Bedenken im wesentlichen bestehen.

14.1.2 Zentrales Fahrerlaubnisregister

Der Entwurf sieht unverändert den Aufbau eines zentralen Fahrerlaubnisregisters vor, in dem die Daten von über 50 Millionen Führerscheininhabern zentral gespeichert werden. Die örtlichen Fahrerlaubnisregister sollen nur noch bis spätestens zum 31. Dezember 2005 geführt werden dürfen. Allerdings hat der Bundesrat in seiner Stellungnahme gefordert, diese Frist bis zum Jahre 2009 zu verlängern.

14.1.3 Zu lange Aufbewahrungsfristen

Der Entwurf sieht weiterhin vor, daß Registerauskünfte, Führungszeugnisse, Gutachten und Gesundheitszeugnisse, die sich in den Akten der Fahrerlaubnisbehörden befinden, spätestens nach zehn Jahren zu vernichten sind. Übergangsweise brauchen diese Unterlagen abweichend davon erst dann vernichtet zu werden, wenn sich die Fahrerlaubnisbehörde aus anderem Anlaß mit dem Vorgang befaßt. Meine Bedenken, daß dadurch die nach § 29 Abs. 1 Nrn. 1 und 2 des Entwurfs gesetzlich festgelegten kürzeren, nämlich zwei- bzw. fünfjährigen Tilgungsfristen (z. B. zwei Jahre bei Entscheidungen wegen einer Ordnungswidrigkeit und fünf Jahre bei Teilnahme an einer verkehrspsychologischen Beratung) unterlaufen werden können, sind nicht berücksichtigt worden. Immerhin wird jetzt geregelt, daß eine Überprüfung der Akten spätestens 15 Jahre nach Inkrafttreten des Gesetzes erfolgen muß.

14.1.4 Erweiterung des Verkehrszentralregisters

Nach wie vor sollen im Verkehrszentralregister mehr Daten als bisher gespeichert und das Register für erheblich erweiterte Zwecke verwendet werden. Im Gegensatz zu den bisherigen Regelungen wird nicht präzise festgelegt, welche personenbezogenen Daten an welche Stellen übermittelt werden dürfen. Ich halte daher meine Bedenken aufrecht, daß damit das Verkehrszentralregister zu einem Auskunfts- und Überwachungssystem werden kann für Zwecke, die nichts mit dem Straßenverkehr zu tun haben.

Ich begrüße, daß der zuständige Senator für Bau, Verkehr und Stadtentwicklung meine Bedenken und Anregungen weitgehend übernommen und in diesem Sinne gegenüber dem Bundesministerium für Verkehr Stellung genommen hat, leider ohne Erfolg. Im zuständigen Bundesrats-Ausschuß hat allerdings Bremen meines Wissens keine entsprechenden Anträge (mehr) gestellt. Es bleibt abzuwarten, welche Korrekturen des Gesetzentwurfs noch durch den Bundestag beschlossen werden.

15. Bau

15.1 „Korruptionsdatei" beim Bausenator

Der Senat hat eine Arbeitsgruppe eingesetzt, deren Aufgabe es ist, Vorschläge für Maßnahmen zur Bekämpfung der Korruption in der bremischen Verwaltung zu unterbreiten. Der Senator für Bau, Verkehr und Stadtentwicklung betreibt in diesem Zusammenhang die Entwicklung eines Datenbanksystems, dessen Aufgabe die Speicherung und Auswertung von Daten über vergebene Aufträge sein soll. Als vorgesetzte Dienststelle der bauenden Ämter und Betriebe obliegt es ihm, im Rahmen des Controlling das Vergabeverhalten der nachgeordneten Dienststellen zu überprüfen. Dazu soll u. a. die 1991 zum Zwecke der Angebotsbearbeitung und Auftragsvergabe angelegte Firmendatei zu einer umfangreicheren Datensammlung ausgebaut werden.

Ich habe die senatorische Behörde zu diesem Projekt eingehend beraten. Sie beabsichtigt jetzt zunächst, mit dem Auf- bzw. Ausbau des Datenbanksystems zu beginnen und in den Probebetrieb zu gehen. Die Auswertungsparameter und -programme zur Ermittlung von Korruptionsverdachtsfällen sollen (erst) in dieser Einführungsphase entwickelt und getestet werden. Die senatorische Behörde hat mir rechtzeitige Beteiligung vor der Festlegung dieser Nutzungsmodalitäten zugesagt. In dieser Phase soll auch gemeinsam bewertet werden, welche der vorgesehenen Auswertungen für die Ausübung der Kontrollbefugnis, d. h. zur Ermittlung potentieller Bestechungsfälle, erforderlich, geeignet und damit zulässig sind (vgl. § 12 Abs. 3 BrDSG).

15.2 Fall: Fragebogenaktion im Kleingartengebiet

Großes Aufsehen in den Medien und bei den betroffenen Bürgerinnen und Bürgern löste im vergangenen Jahr die Fragebogenaktion der Bremischen Gesellschaft für Stadterneuerung, Stadtentwicklung und Wohnungsbau (Bremische) im Kleingartengebiet „Waller Fleet" aus. Sie war vom Senator für Bau, Verkehr und Stadtentwicklung beauftragt worden, für die Bereinigung bestimmter Kleingartengebiete eine Erhebung über die Art der Nutzung durchzuführen. Mehrere Parzelleninhaber wandten sich an mich und wähnten einen Verstoß gegen Datenschutzbestimmungen.

Dies konnte ich nach Prüfung der Stellungnahme der senatorischen Behörde und der von ihr zur Verfügung gestellten Unterlagen nicht bestätigen. Nach den Vorschriften der Bremischen Landesbauordnung (BremLBO) darf die Bauordnungsbehörde die Beseitigung baulicher oder sonstiger Anlagen oder Einrichtungen anordnen, wenn diese im Widerspruch zu öffentlich-rechtlichen Vorschriften errichtet oder geändert wurden. Beseitigungsverfügungen und Nutzungsuntersagungen, die auch im Kleingartengebiet „Waller Fleet" in Betracht kommen, sind aber nur auf der Grundlage einer umfassenden Ermessensentscheidung zulässig. Die für diese Verwaltungsentscheidungen notwendigen Informationen ermittelte die Bremische als eingeschaltete sog. sachverständige Stelle nach § 61 Abs. 2 BremLBO.

Die Erhebung selbst wie auch der Umfang des Fragebogens waren mithin nach § 62 Abs. 1 Satz 1 BremLBO zulässig. Dies habe ich den Beschwerdeführern mitgeteilt. Auch den Datenschutzausschuß habe ich wegen des großen öffentlichen Echos entsprechend informiert (vgl. o. Ziff. 7.1.2).

16. Finanzen

16.1 Fall: Falschauskunft führt zu Kontensperrung

Die Vollstreckungsstelle des Finanzamtes Bremen-Mitte hatte durch eine fehlerhafte Datenübermittlung an ein Kreditinstitut dafür gesorgt, daß ein Kontoinhaber, der mit dem Steuerfall nichts zu tun hatte, keine Bankgeschäfte mehr tätigen konnte. Sein Konto war durch die Vollstreckungshandlung gesperrt worden. Er stand nicht nur ohne Bargeld dar, sondern geriet bei der Einlösung eines Schecks in ein „schiefes Licht".

Bei der Überprüfung dieses Beschwerdefalls verweigerte mir der Leiter der Stelle zunächst die Einsicht in die Steuer- bzw. Vollstreckungsakten mit Hinweis auf das Steuergeheimnis. Ich mußte ihn auf die seit 1991 geltenden Bestimmungen des § 24 Abs. 2 Satz 1 i. V. m. Abs. 6 Bundesdatenschutzgesetz (BDSG) hinweisen, die ausdrücklich klarstellen, daß die Kontrollbefugnis des Landesbeauftragten für den Datenschutz sich auch auf die dem Steuergeheimnis unterliegenden Daten bezieht. Erst dann erhielt ich die zur Klärung des Vorfalls erforderlichen Informationen und Akteneinsicht. Erst aus der Akteneinsicht ergab sich im übrigen auch, daß der Eingeber nicht ausreichend darüber aufgeklärt worden war, daß die Falschübermittlung von der Vollstreckungsstelle selbst stammte.

Ich will diesen Fall nicht überbewerten und habe es deshalb bei einer mündlichen Intervention bei dem behördenintern für den Datenschutz zuständigen Mitarbeiter bewenden lassen, der auch entsprechend reagiert hat. Ich muß aber prinzipiell auch und gerade in der Steuerverwaltung darauf dringen, daß meine Kontrolle nicht durch veraltete Rechtskenntisse behindert wird und ausgerechnet dem Landesbeauftragten Berufs- und Amtsgeheimnisse entgegengehalten werden.

17. Magistrat der Stadt Bremerhaven

17.1 Telefonanlage mit Gesprächsaufzeichnung

Der Magistrat der Stadt Bremerhaven modernisiert seine zentrale Telefonvermittlung. In der neuen Telefonanlage sollen alle Gespräche innerhalb eines Endlosbandes für zwölf Minuten aufgezeichnet werden.

Der Magistrat begründet dies mit dem Erfordernis der Gefahrenabwehr. „In heutiger Zeit mehr denn je" sei dafür Sorge zu tragen, mit allen zur Verfügung stehenden vertretbaren Mitteln einem nicht auszuschließenden Sabotage- oder Terror-Anschlag vorzubeugen. Auf Nachfrage konnten mir für den Zeitraum der letzten 15 Jahre jedoch nur ungefähr fünf bis sechs Bombendrohungen benannt werden, die sich alle als Fehlalarm erwiesen hatten.

Ich habe zwar Verständnis für das Anliegen, Drohanrufe in der Telefonvermittlung aufzuzeichnen, um Vorfälle zu verhindern und die Strafverfolgung einzuleiten bzw. zu ermöglichen. Doch wird hier über das Ziel hinausgeschossen: Die Praxis, jeden in der Telefonzentrale eingehenden Anruf auch nur für wenige Minuten aufzuzeichnen, erfüllt tatbestandsmäßig die Voraussetzungen des § 201 Abs. 1 Nr. 1 Strafgesetzbuch (StGB). Diese Bestimmung stellt die Aufnahme des nichtöffentlich gesprochenen Wortes eines anderen auf einen Tonträger unter Strafe; auch telefonische Äußerungen gehören zum Schutzbereich dieser Norm.

Ausnahmen kommen allenfalls unter den Voraussetzungen der Notwehr oder einer notwehrähnlichen Lage in Betracht (§§ 32 und 34 StGB). Dazu kann z. B. die gezielte Aufzeichnung eines konkreten Drohanrufs „auf Knopfdruck" gehören. Sonderbedingungen gelten auch für die Notrufanlagen von Polizei und Feuerwehr.

Ich habe daher den Magistrat gebeten, die Rechtslage zu beachten und nur in Fällen, in denen Drohanrufe zu erwarten sind oder bedrohliche Ferngespräche tatsächlich eingehen, Gesprächsinhalte aufzuzeichnen. Der Mitschnitt kann im Einzelfall auch für begrenzte Zeiträume erfolgen, wenn vorübergehend sämtliche Anrufe wegen einer konkret bestehenden Bedrohungslage festgehalten werden müssen. Die Einhaltung dieser rechtlichen Vorgaben setzt voraus, daß die „Knopfdruck"-Vorrichtung vor der Inbetriebnahme der Telefon- bzw. der Mitschnittanlage installiert und dann auch tatsächlich genutzt wird. Zu kritisieren sind auch mehrere Hersteller, die die Daueraufzeichnung "serienmäßig" anbieten, ohne die Rechtslage zu berücksichtigen.

Der Magistrat hat meine Auffassung abgelehnt und erklärt, er halte an seinem Vorhaben fest.

18. Datenschutz in der Privatwirtschaft

18.1 Elektronische Geldbörse (GeldKarte): Anonymität bei Bezahlung?

Bundesweit haben viele Kreditinstitute die Ende 1996 abgelaufenen EC-Karten und Bankkundenkarten durch neue, sowohl mit einem traditionellen Magnetstreifen als auch mit einem Multifunktionschip ausgestattete Karten ersetzt. Mit Hilfe des neuen Chips soll die herkömmliche EC-Karte um eine zusätzliche „Geldbörsen-Funktion" für Kleingeldzahlungen bis zu 400,— DM erweitert werden. Diese sog. „GeldKarte" soll das elektronische Bezahlen kleinerer Artikel des täglichen Lebens ermöglichen. Mit Hilfe der Geldbörsenfunktion soll die EC-Karte später auch als Telefon-Wertkarte, für Fahrkarten der Bahn und im öffentlichen Nahverkehr, zur Benutzung von Parkhäusern, Warenautomaten, in Taxen sowie bei den Kleineinkäufen genutzt werden.

Nach mir inzwischen vorliegenden Informationen sollen sich die jeweils letzten 15 Kartennutzungen (z. B. Einkäufe) sowie das aktuelle Guthaben und damit ein Ausschnitt des Konsumverhaltens des Karteninhabers über einen bestimmten Zeitraum feststellen lassen (s. u.).

Zeitungsberichten zufolge sind in Bremen allein von der Sparkasse bis Jahresende rund 131.000 neue Karten mit Geldkarten-Chip ausgeliefert worden. Der Chip kann an entsprechenden Terminals „aufgeladen" werden, von denen im Bremer Gebiet allein im Januar 1997 von der Sparkasse in Bremen bereits 15 Stück installiert wurden.

Die Kreditinstitute erwarten, daß möglichst viele Firmen und Betriebe sog. „Akzeptanzstellen" einrichten, an denen mit der „GeldKarte" bezahlt werden kann. Man geht davon aus, daß Anfang März des Jahres 1997 bereits 41 solcher Akzeptanzstellen eingerichtet sind. Beim Bezahlen mit der GeldKarte ist weder eine Geheimzahl notwendig noch wird die Identität des Käufers überprüft. Der Kunde muß lediglich den Betrag durch Knopfdruck bestätigen. Verliert er seine Karte, kann die aktuell geladene Summe, selbst wenn die EC-Karte gesperrt ist, von Dritten unbefugt abgebucht werden.

Entgegen ursprünglicher Annahmen, die Nutzung der GeldKarte werde wie der Bargeldkauf völlig anonym verlaufen, werden bei Zahlungen mit dem bzw. bei Aufladung des Chips Terminal-Nummer, Datum, Uhrzeit, Ein- bzw. Auszahlungsbetrag, Konto-, Karten- und Kartenfolgenummer und Bankleitzahl gespeichert. Diese Daten werden unmittelbar nach dem Aufladen der Karte durch das jeweilige Kreditinstitut an die sog. „Evidenzzentrale" gemeldet. Diese richtet daraufhin mit diesen Daten ein sog. „Schattenkonto" ein. Auch die vom Händler an die Evidenzzentrale übermittelten Daten über Zahlungen per GeldKarte enthalten die genannten Angaben. Die Evidenzzentralen führen so zu jedem Kunden, der seine GeldKarte einsetzt, das „Schattenkonto" mit „Soll" und „Haben". Auf diese Weise soll festgestellt werden, ob mit manipulierten Karten bezahlt wurde.

Wegen der erwartet niedrigen Umsätze pro Kartennutzung wird der Zahlungsverkehr zur Verrechnung mit den Hausbanken der Kunden nicht auf Einzeltransaktionsebene abgewickelt, sondern auf der Basis von aggregierten Daten. Da für die

kartenausgebenden Kreditinstitute somit keine Möglichkeit zur Kontrolle über einzelne Zahlungsvorgänge der Kunden mit der GeldKarte gegeben ist, obliegt es den im Auftrag der teilnehmenden Kreditwirtschaft eingerichteten Evidenzzentralen (s. o.) die bei den Händlern (an den Akzeptanzstellen) erfaßten Daten über die Einzeltransaktionen entgegenzunehmen, zu kontrollieren, per Summenbildung zusammenzufassen und dann für die weiteren Buchungen im Zahlungsverkehr vorzubereiten. Darüber hinaus sollen die Evidenzstellen Sicherheitsprüfungen durchführen. Die Abwicklung des Zahlungsverkehrs geht dann weiter über die von den Evidenzzentralen eingeschalteten sog. Verrechnungsbanken. Diese belasten dann mit einer jeweils errechneten Summe das Sammelkonto des betroffenen Kreditinstituts.

Was letztlich mit der Datenflut bei den Evidenzzentralen geschieht, insbesondere wie diese die Daten verarbeiten und auswerten werden, ist derzeit im einzelnen noch unklar. Wenn der Bericht einer Verbraucherzeitschrift zutrifft und die auf dem Chip verschlüsselt gespeicherte PIN-Geheimzahl decodiert werden kann, liegt hierin ein erhebliches Datenschutzrisiko. Wie schnell die Sicherheitsvorkehrungen eines Chips „geknackt" werden können, hat erst unlängst wieder ein Wissenschaftler dem SPIEGEL (47/96, S. 216 ff.) vorgeführt.

Ich werde mich in Kürze bei ausgewählten Bremer Kreditinstituten über die Einzelheiten der technischen Infrastruktur für den Einsatz der GeldKarte und die mit ihrer Nutzung verbundenen Datenverarbeitungsvorgänge genau informieren.

18.2 Fall: Mitgliederliste an neue Vereinsmitglieder

Das Mitglied eines Tennisvereins wandte sich an mich mit der Befürchtung, daß der Vorstand des Vereins seine Daten weitergegeben habe. Er war nämlich von einem Neumitglied angeschrieben worden, das seine Beratungsdienste als Steuer- und Vermögensberatungsfachmann anpries. Der Vorstand bestätigte mir die Übersendung einer Mitgliederliste an den Absender. Diese übliche Praxis solle es u. a. erleichtern, sich mit Spielpartnern verabreden zu können.

Ich werde immer wieder zur Zulässigkeit der Verteilung von Mitgliederlisten innerhalb von Vereinen gefragt. Die beschriebene Handhabung ist ohne ausdrückliche Einwilligung der Betroffenen keineswegs ohne weiteres zulässig. § 28 Abs. 2 Nr. 1 b Bundesdatenschutzgesetz (BDSG) erlaubt dies nur, wenn kein Grund zur Annahme besteht, daß Mitglieder ihre Vereinszugehörigkeit jedenfalls ohne ihr Einverständnis auch anderen Mitgliedern gegenüber nicht offenlegen wollen. Diese Diskretion kann bei Selbsthilfegruppen ebenso erwünscht sein wie bei Vereinen mit dem Zweck der Spendenaquisition.

Auch wenn bei einem Tennisclub in der Regel nicht von derartigen Vertraulichkeitsinteressen der Mitglieder auszugehen ist, halte ich zumindest einen entsprechenden Beschluß des Vorstands über die Voraussetzungen der Listenverteilung für notwendig, der den Betroffenen bekanntgegeben wird und ihnen die Möglichkeit zum rechtzeitigen Einspruch gegen die Nennung ihres Namens auf der verteilten Liste gibt. Außerdem muß § 28 Abs. 4 BDSG beachtet werden, der verlangt, daß der Empfänger die Daten nur für den Zweck verarbeitet oder nutzt, zu dessen Erfüllung sie ihm übermittelt wurden, in diesem Fall also für den sportbezogenen, vereinsinternen Gebrauch. Die Verwendung für Werbezwecke war nicht erlaubt.

Auf diese Zweckbindung hat die übermittelnde Stelle, in diesem Fall der Vorstand, den Adressaten der Liste ausdrücklich hinzuweisen (§ 28 Abs. 4 Satz 3 BDSG). Dies war nicht geschehen. Ich habe der Vereinsführung dringend geraten, in Zukunft auf der Liste einen entsprechenden Hinweis anzubringen.

18.3 Fall: Offene Bildschirme im Verkaufsraum

Im Verkaufsraum eines Bremerhavener Brillengeschäfts waren fünf PC installiert worden, die so aufgestellt waren, daß der Bildschirminhalt von jedem in der Nähe befindlichen Kunden einsehbar war. Bei der Beratung werden u. a. Name, Anschrift, Krankenkasse und Versichertennummer des Kunden am Bildschirm aufgerufen bzw. bei Neukunden erstmalig erfaßt.

Ich habe die Filialleitung darauf hingewiesen, daß eine unbefugte Kenntnisnahme durch Dritte, d. h. andere als den Optiker und den gerade betreuten Kunden, durch technische bzw. organisatorische Maßnahmen verhindert werden müsse.

Ich habe dann vor Ort die Datensicherung überprüft und festgestellt, daß die Bildschirmschrift so klein ist, daß sie nur der lesen kann, der unmittelbar vor dem Gerät steht. Da dies allein unbefugte Ansicht noch nicht verhindert, ist das Programm inzwischen außerdem mit einem Bildschirmschoner ausgestattet, der sich bereits nach kurzer Zeit einschaltet. Des weiteren wird darauf geachtet, daß nur die PC laufen, die gerade aktuell für eine Kundenberatung benötigt werden.

18.4 Fall: Schlampiger Umgang mit Abonnentendaten

Die folgenden drei Fälle betrafen den gleichen Zeitungsverlag

Ein Bürger reichte mir eine Zustelliste ein, die er auf der Straße gefunden hatte und der er entnehmen konnte, daß ein Nachbar die Zeitung abbestellt hatte und sich offenbar für längere Zeit im Urlaub befand. Ein anderer Eingeber beschwerte sich darüber, daß seine frühere Anschrift noch gespeichert war, obwohl er bereits vor drei Jahren umgezogen war. Eine dritte Beschwerde betraf die Frage, wie lange Nachsendeadressen für die Zeitungszustellung auch nach Ablauf des Nachsendeauftrages noch gespeichert werden dürfen.

Zu dem Fall mit der Zustelliste ergab sich, daß jeder Träger selbst dafür Sorge zu tragen hat, daß die Bögen mit den Änderungsmeldungen datenschutzgerecht entsorgt werden. Das Presseunternehmen bietet ihnen die Entsorgung durch die hauseigene Schredderanlage an. Ein Aushilfsträger hatte offensichtlich schlampig gehandelt und nicht die ihm obliegende Sorgfalt walten lassen. Er wurde daraufhin abgemahnt. Das Presseunternehmen hat außerdem die Zusteller/-innen noch einmal ausdrücklich auf die Pflicht zu sorgsamem Umgang mit den Daten der Leser und zur ordnungsgemäßen Vernichtung von Anschriftenlisten hingewiesen.

In den beiden anderen Fällen erfuhr ich, daß Bezieheradressen in der EDV des Verlags immer dann zentral gelöscht würden, wenn die Speicherkapazitäten im System erschöpft seien. Da die Speicherung von Nachsendeadressen über einen weiten Zeitraum einen Einblick in Aufenthalts- und Reisegewohnheiten geben kann und für die Zustellung auch nicht erforderlich ist, hatte ich eine Änderung des Löschprogramms angeregt.

Das Presseunternehmen hat mir daraufhin mitgeteilt, zu Anfang und zur Mitte des Jahres würden künftig die Nachsendeanschriften und die Lieferbezirksdaten, die länger als ein halbes Jahr gespeichert waren, gelöscht.

19. Meldepflichtige Stellen nach § 32 Bundesdatenschutzgesetz (BDSG)

19.1 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 1997 122 Stellen gegenüber 110 Stellen im Vorjahr aus. Davon befinden sich 102 Stellen (Anfang 1996: 90) in Bremen und 20 Stellen (Anfang 1996 ebenfalls 20 Stellen) in Bremerhaven. Der Schwerpunkt der Veränderungen lag im Bereich der Stellen, die personenbezogene Daten für dritte Stellen be- oder verarbeiten, insbesondere bei den DV- und TK-Dienstleistungsanbietern. Der regionale Schwerpunkt liegt eindeutig in Bremen.

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. Weitere Einzelheiten zeigt die umseitige Übersicht:

Art der Tätigkeit	insgesamt	Bremen	Bremerhaven
1. Speicherung personenbezogener Daten zum Zwecke der Übermittlung (insgesamt)	**8**	**5**	**3**
— Auskunfteien	5	4	1
— Detekteien	1		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)	**111**	**94**	**17**
— Datenerfassung	11	11	
— Dienstleistung/RZ	83	69	14
— Mikroverfilmer	4	4	
— Mailboxdienste	7	4	3
— Datenlöschung/Datenträgervernichtung	6	6	
Gesamt	**122**	**102**	**20**

19.2 Einfache Registerprüfungen

Bei diesen Kontrollen überprüfe ich lediglich das Bestehen einer Meldepflicht nach § 32 BDSG sowie den Inhalt der Registermeldung, die Bestellung und Tätigkeit des betrieblichen Datenschutzbeauftragten nach den § 36/37 BDSG, die Verpflichtungen auf das Datengeheimnis gemäß § 5 BDSG und die Beachtung der Regelungen zur Auftragsdatenverarbeitung nach § 11 BDSG.

In diesem Berichtsjahr habe ich bei insgesamt 18 Stellen Prüfungen dieser Art durchgeführt. Dabei mußte ich immer wieder Mängel feststellen. Änderungen zu vorliegenden Registermeldungen werden entweder gar nicht oder sehr verspätet vorgenommen; Abmeldungen oder auch Neuanmeldungen erfolgen vielfach erst, wenn ich als Aufsichtsbehörde tätig geworden bin. Vor allem die recht häufigen Änderungen im betriebswirtschaftlichen und gesellschaftsrechtlichen Bereich werden der Aufsichtsbehörde entweder gar nicht oder nicht zeitgerecht gemeldet. Auch gibt es erstaunlicherweise immer noch Datenverarbeiter, die vom Bundesdatenschutzgesetz oder der Registermeldepflicht nichts gehört haben oder wissen.

Auch beim betrieblichen Datenschutzbeauftragten gibt es immer wieder Mängel. So gibt es Fälle, in denen die schriftliche Bestellung nicht mehr aktuell ist, da die Firmen- bzw. Gesellschaftsstruktur sich zwischenzeitlich verändert hat. Häufig ist auch das Zeitbudget, das der Beauftragte für seine Tätigkeit zur Verfügung hat, sehr gering. Er hat kaum Zeit zur eigenen Fortbildung und/oder ist mangels ausreichender Freistellung nur unzulänglich tätig.

Auch die Auftragsdatenverarbeitung wird nicht immer BDSG-konform abgewickelt. So entspricht die Vertragsgestaltung, vor allem bei verbundenen Unternehmensstrukturen, nicht den Vorgaben des § 11 BDSG, wenn Regelungen hinsichtlich der Subauftragsvergabe oder konkrete Weisungen des Auftraggebers fehlen.

In einem Fall habe ich ein Bußgeldverfahren wegen erheblich verspäteter Anmeldung eingeleitet.

19.3 Kontrollen bei Service-Rechenzentren und Auftragsdatenverarbeitern

Bei drei größeren Rechenzentren/Auftragsdatenverarbeitern habe ich im Berichtsjahr umfassendere Datenschutzprüfungen durchgeführt.

Auch hier zeigte sich, daß die Registermeldung nicht immer dem aktuellen Sachstand entsprach, insbesondere was die Angaben zum Namen der Stelle, zum Vorstand bzw. zur Geschäftsführung, zu den eingesetzten Datenverarbeitungsanlagen oder zur meldepflichtigen Tätigkeit selbst anbetrifft.

Auch die Bestellung des betrieblichen Datenschutzbeauftragten entsprach nicht immer den gesetzlichen Erfordernissen. Mängelpunkte waren z. B. die fehlende Schriftlichkeit der Bestellung, die Inaktualität der Bestellungsschreiben nach gesellschaftsrechtlichen Veränderungen, vor allem aber immer wieder die angesichts des Umfangs der zu betreuenden Systeme und Verfahren zu geringe Freistellung. Manche Unternehmen verringern die dem Beauftragten zur Verfügung stehende Zeit sogar entgegen der Zunahme der Informations- und Kommunikationstechnik in ihren Betriebsstätten. Selbst völlig freigestellte betriebliche Datenschutzbeauftragte haben nur beschränkte Wirkungsmöglichkeiten, wenn sie bundesweit in vielen Stellen gleichzeitig in dieser Funktion tätig sind. Hier macht sich das Fehlen einer eindeutigen gesetzlichen bzw. gerichtlichen Festlegung der vom Unternehmen dem Beauftragten zu leistenden Unterstützung bemerkbar.

Auch bei diesen ausführlicheren Prüfungen mußte ich wiederholt die unzureichende Einhaltung von § 11 BDSG über die Datenverarbeitung im Auftrag feststellen.

Bei den Datensicherungsmaßnahmen habe ich Empfehlungen gegeben u. a. zu den Punkten Fernwartung der Systeme, Zutrittssicherung, Paßwortgestaltung, zum Verbindungsaufbau bei Online-Datenübertragungen, zum Anschluß externer Stellen an das installierte Datenübertragungsnetz sowie zur Datenträgerentsorgung.

20. Die Entschließungen der Datenschutzkonferenz im Jahr 1996

20.1 Transplantationsgesetz

Entschließung der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 — Transplantationsgesetz

Bei der anstehenden gesetzlichen Regelung, unter welchen Voraussetzungen die Entnahme von Organen zur Transplantation zulässig sein soll, werden untrennbar mit der Ausformung des Rechts auf Selbstbestimmung auch Bedingungen des Rechts auf informationelle Selbstbestimmung festgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont hierzu, daß von den im Gesetzgebungsverfahren diskutierten Modellen die „enge Zustimmungslösung" — also eine ausdrückliche Zustimmung des Organspenders — den geringsten Eingriff in das Recht auf informationelle Selbstbestimmung beinhaltet. Sie zwingt niemanden, eine Ablehnung zu dokumentieren. Sie setzt auch kein Organspenderregister voraus.

Mit einer engen Zustimmungslösung ist auch vereinbar, daß der Organspender seine Entscheidung z.B. einem nahen Angehörigen überträgt.

20.2 Grundsätze für die öffentliche Fahndung im Strafverfahren

Die 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 hat die folgenden „Grundsätze für die öffentliche Fahndung im Strafverfahren" zustimmend zur Kenntnis genommen:

Bei den an die Öffentlichkeit gerichteten Fahndungsmaßnahmen nach Personen (Beschuldigten, Verurteilten, Strafgefangenen und Zeugen) wird stets das Recht des Betroffenen auf informationelle Selbstbestimmung eingeschränkt. Es bedarf daher nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil vom 15. 12. 1983 für alle Maßnahmen der öffentlichen Fahndung nach Personen einer normenklaren und dem Grundsatz der Verhältnismäßigkeit entsprechenden gesetzlichen Regelung, die bisher fehlt.

1. Der Gesetzgeber hat zunächst die Voraussetzungen der öffentlichen Fahndung zu regeln und dabei einen sachgerechten Ausgleich zwischen dem öffentlichen Strafverfolgungsinteresse und dem Recht auf informationelle Selbstbestimmung des Betroffenen zu treffen.

   Die öffentliche Fahndung sollte nur bei Verfahren wegen Verletzung bestimmter vom Gesetzgeber zu bezeichnender Straftatbestände und bei Straftaten, die aufgrund der Art der Begehung oder des verursachten Schadens ein vergleichbares Gewicht haben, zugelassen werden.

Sie soll nur stattfinden, wenn weniger intensive Fahndungsmaßnahmen keinen hinreichenden Erfolg versprechen.

Der Grundsatz der Erforderlichkeit mit der gebotenen Beschränkung des Verbreitungsgebiets ist auch bei der Auswahl des Mediums zu berücksichtigen.

2. Bei der öffentlichen Fahndung nach unbekannten Tatverdächtigen, Beschuldigten, Angeschuldigten, Angeklagten einerseits und Zeugen andererseits erscheint es geboten, die Entscheidung, ob und in welcher Weise gefahndet werden darf, grundsätzlich dem Richter vorzubehalten; dies gilt nicht bei der öffentlichen Fahndung zum Zwecke der Straf- oder Maßregelvollstreckung gegenüber Erwachsenen.

   Bei Gefahr in Verzug kann eine Eilkompetenz der Staatsanwaltschaft vorgesehen werden; dies gilt nicht bei der öffentlichen Fahndung nach Zeugen. In diesem Falle ist unverzüglich die richterliche Bestätigung der Maßnahme einzuholen.

   Die öffentliche Fahndung nach Beschuldigten setzt voraus, daß ein Haftbefehl oder Unterbringungsbefehl vorliegt bzw. dessen Erlaß nicht ohne Gefährdung des Fahndungserfolges abgewartet werden kann.

3. Eine besonders eingehende Prüfung der Verhältnismäßigkeit hat bei der Fahndung nach Zeugen stattzufinden.

   Eine öffentliche Fahndung nach Zeugen darf nach Art und Umfang nicht außer Verhältnis zur Bedeutung der Zeugenaussage für die Aufklärung der Straftat stehen. Hat ein Zeuge bei früherer Vernehmung bereits von seinem gesetzlichen Zeugnis- oder Auskunftsverweigerungsrecht Gebrauch gemacht, so soll von Maßnahmen der öffentlichen Fahndung abgesehen werden.

4. In Unterbringungssachen darf eine öffentliche Fahndung mit Rücksicht auf den Grundsatz der Verhältnismäßigkeit nur unter angemessener Berücksichtigung des gesetzlichen Zwecks der freiheitsentziehenden Maßregel, insbesondere der Therapieaussichten und des Schutzes der Allgemeinheit angeordnet werden.

5. Die öffentliche Fahndung zur Sicherung der Strafvollstreckung sollte zur Voraussetzung haben, daß

   — eine Verurteilung wegen einer Straftat von erheblicher Bedeutung vorliegt und

   — der Verurteilte, der sich der Strafvollstreckung entzieht, (noch) eine Restfreiheitsstrafe von in der Regel mindestens einem Jahr zu verbüßen hat, oder ein besonderes öffentliches Interesse, etwa tatsächliche Anhaltspunkte für die Begehung weiterer Straftaten von erheblicher Bedeutung, an der alsbaldigen Ergreifung des Verurteilten besteht.

6. Besondere Zurückhaltung ist bei internationaler öffentlicher Fahndung geboten. Dies gilt sowohl für Ersuchen deutscher Stellen um Fahndung im Ausland als auch für Fahndung auf Ersuchen ausländischer Stellen im Inland.

7. Öffentliche Fahndung unter Beteiligung der Medien sollte in den Katalog anderer entschädigungspflichtiger Strafverfolgungsmaßnahmen des § 2 Abs. 2 StrEG aufgenommen werden.

   Durch Ergänzung des § 7 StrEG sollte in solchen Fällen auch der immaterielle Schaden als entschädigungspflichtig anerkannt werden.

   Der Gesetzgeber sollte vorsehen, daß auf Antrag des Betroffenen die Entscheidung über die Entschädigungspflicht öffentlich bekanntzumachen ist.

20.3 Modernisierung und europäische Harmonisierung des Datenschutzrechts

Entschließung der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 — Modernisierung und europäische Harmonisierung des Datenschutzrechts

Die Datenschutzrichtlinie der Europäischen Union vom Oktober 1995 verpflichtet alle Mitgliedstaaten, ihr Datenschutzrecht binnen drei Jahren auf europäischer Ebene zu harmonisieren. Die Richtlinie geht zu Recht von einem hohen Datenschutzniveau aus und stellt fest: „Die Datenverarbeitungssysteme stehen im Dienste des Menschen".

Die Datenschutzbeauftragten begrüßen diesen wichtigen Schritt zu einem auch international wirksamen Datenschutz. Sie appellieren an die Gesetzgeber in Bund und Ländern, die Umsetzung der Richtlinie nicht nur als Beitrag zur europäischen Integration zu verstehen, sondern als Aufforderung und Chance, den Datenschutz fortzuentwickeln. Die Datenschutzbeauftragten sprechen sich für eine umfassende Modernisierung des deutschen Datenschutzrechts aus, damit der einzelne in der sich rapide verändernden Welt der Datenverarbeitung, der Medien und der Telekommunikation über den Umlauf und die Verwendung seiner persönlichen Daten soweit wie möglich selbst bestimmen kann.

Die wichtigsten Ziele sind:

1. Weitgehende Vereinheitlichung der Vorschriften für den öffentlichen und privaten Bereich mit dem Ziel eines hohen, gleichwertigen Schutzes der Betroffenen, beispielsweise bei der Datenerhebung und bei der Zweckbindung bis hin zur Verarbeitung in Akten.
2. Erweiterung der Rechte der Betroffenen auf Information durch die datenverarbeitenden Stellen über die Verwendung der Daten, auf Auskunft, auf Widerspruch und im Bereich der Einwilligung.
3. Verpflichtung zu Risikoanalyse, Vorabkontrolle, Technikfolgenabschätzung und zur Beteiligung der Datenschutzbeauftragten bei der Vorbereitung von Regelungen mit Auswirkungen auf den Datenschutz.
4. Verbesserung der Organisation und Stärkung der Befugnisse der Datenschutzkontrolle unter den Gesichtspunkten der Unabhängigkeit und der Effektivität.
5. Einrichtung und effiziente Ausgestaltung des Amtes eines internen Datenschutzbeauftragten in öffentlichen Stellen.
6. Weiterentwicklung der Vorschriften zur Datensicherheit, insbesondere im Hinblick auf Miniaturisierung und Vernetzung.

Darüber hinaus machen die Datenschutzbeauftragten folgende Vorschläge:

7. Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen und Regelung der Video-Überwachung.
8. Stärkere Einbeziehung von Presse und Rundfunk in den Datenschutz; Aufrechterhaltung von Sonderregelungen nur, soweit dies für die Sicherung der Meinungsfreiheit notwendig ist.
9. Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren.
10. Sicherstellung der informationellen Selbstbestimmung bei Multimedia-Diensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsformen anzubieten, durch den Schutz vor übereilter Einwilligung, z. B. durch ein Widerrufsrecht, und durch strenge Zweckbindung für die bei Verbindung, Aufbau und Nutzung anfallenden Daten.
11. Besondere Regelungen für Chipkarten-Anwendungen, um die datenschutzrechtliche Verantwortung aller Beteiligten festzulegen und den einzelnen vor unfreiwilliger Preisgabe seiner Daten zu schützen.
12. Schutz bei Persönlichkeitsbewertungen durch den Computer, insbesondere durch Beteiligung des Betroffenen und Nachvollziehbarkeit der Computerentscheidung.
13. Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing.
14. Verbesserung des Datenschutzes bei grenzüberschreitender Datenverarbeitung; Datenübermittlung ins Ausland nur bei angemessenem Datenschutzniveau.

20.4 Eckpunkte für die datenschutzrechtliche Regelung von Mediendiensten

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 29. April 1996 — Eckpunkte für die datenschutzrechtliche Regelung von Mediendiensten

In letzter Zeit finden Online-Dienste und Multimedia-Anwendungen zunehmend Verbreitung. Mit den — häufig multimedialen — Angeboten, auf die interaktiv

über Telekommunikationsnetze zugegriffen werden kann, sind besondere Risiken für das Recht auf informationelle Selbstbestimmung der Teilnehmer verbunden; hinzuweisen ist insbesondere auf die Gefahr, daß das Nutzerverhalten unbemerkt registriert und zu Verhaltensprofilen zusammengeführt wird. Das allgemeine Datenschutzrecht reicht nicht aus, die mit den neuen technischen Möglichkeiten und Nutzungsformen verbundenen Risiken wirkungsvoll zu beherrschen.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für dringend erforderlich, durch bereichsspezifische Regelungen technische und rechtliche Gestaltungsanforderungen für die elektronischen Dienste zu formulieren, die den Datenschutz sicherstellen. Leitlinie sollte hierbei der Grundsatz der Datenvermeidung bzw. -minimierung sein. Die Datenschutzbeauftragten haben dazu in einer Entschließung vom 14./15. März 1996 zur Modernisierung und zur europäischen Harmonisierung des Datenschutzrechts vorgeschlagen, daß die informationelle Selbstbestimmung bei Multimediadiensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsverfahren anzubieten, durch den Schutz vor übereilter Einwilligung, z. B. durch ein Widerspruchsrecht, und durch strenge Zweckbindung für die bei der Verbindung, Nutzung und Abrechnung anfallenden Daten sichergestellt wird.

Die Datenschutzbeauftragten weisen darauf hin, daß auch mit Inhalten, die durch Mediendienste verbreitet werden, datenschutzrechtliche Probleme verbunden sein können. Auf diese Probleme wird im folgenden jedoch — ebenso wie auf die Datenschutzaspekte der Telekommunikation — nicht näher eingegangen. Bei den datenschutzrechtlichen Eckpunkten wird ferner bewußt darauf verzichtet, den Regelungsort — etwa einen Länder-Staatsvertrag oder ein Bundesgesetz — anzugeben. Die Datenschutzbeauftragten appellieren an die Gesetzgeber in Bund und Ländern, eine angemessene datenschutzgerechte Regulierung der neuen Dienste nicht an Kompetenzstreitigkeiten scheitern zu lassen.

1. Anonyme bzw. datensparsame Nutzung:

Die Dienste und Multimedia-Einrichtungen sollten so gestaltet werden, daß keine oder möglichst wenige personenbezogene Daten erhoben, verarbeitet und genutzt werden; deshalb sind auch anonyme Nutzungs- und Zahlungsformen anzubieten. Auch zur Aufrechterhaltung und zur bedarfsgerechten Gestaltung von Diensten und Dienstleistungen (Systempflege) sind soweit wie möglich anonymisierte Daten zu verwenden. Soweit eine vollständig anonyme Nutzung nicht realisiert werden kann, muß jeweils geprüft werden, ob durch andere Verfahren, z. B. die Verwendung von Pseudonymen, ein unmittelbarer Personenbezug vermieden werden kann. Die Herstellung des Personenbezugs sollte bei diesen Nutzungsformen nur dann erfolgen, wenn hieran ein begründetes rechtliches Interesse besteht.

2. Bestandsdaten:

Bestandsdaten dürfen nur in dem Maße erhoben, verarbeitet und genutzt werden, soweit sie für die Begründung und Abwicklung eines Vertragsverhältnisses sowie für die Systempflege erforderlich sind. Die Bestandsdaten dürfen zur bedarfsgerechten Gestaltung von Diensten und Dienstleistungen sowie zur Werbung und Marktforschung genutzt werden, soweit der Betroffene dem nicht widersprochen hat. Für die Werbung und Marktforschung durch Dritte dürfen Bestandsdaten nur mit der ausdrücklichen Einwilligung des Betroffenen verarbeitet werden.

3. Verbindungs- und Abrechnungsdaten:

Verbindungs- und Abrechnungsdaten dürfen nur für Zwecke der Vermittlung von Angeboten und für Abrechnungszwecke erhoben, gespeichert und genutzt werden. Sie sind zu löschen, wenn sie für die Erbringung der Dienstleistung oder für Abrechnungszwecke nicht mehr erforderlich sind. Soweit Verbindungsdaten ausschließlich zur Vermittlung einer Dienstleistung gespeichert werden, sind sie spätestens nach Beendigung der Verbindung zu löschen. Die Speicherung der Abrechnungsdaten darf den Zeitpunkt, die Dauer, die Art, den Inhalt und die Häufigkeit bestimmter von den einzelnen Teilnehmern in Anspruch genommener Angebote nicht erkennen lassen, es sei denn, der Teilnehmer beantragt eine dahingehende Speicherung. Verbindungs- und Abrechnungsdaten sind einer strikten Zweckbindung zu unterwerfen. Sie dürfen über den hier genannten Umfang hinaus nur mit der ausdrücklichen Einwilligung des Betroffenen erhoben, verarbeitet und genutzt werden. Unberührt hiervon bleibt die Speicherung von Daten von Verantwortlichen für Angebote im Zusammenhang mit Impressumspflichten.

4. Interaktionsdaten:

Werden im Rahmen von interaktiven Dienstleistungen darüber hinaus personenbezogene Daten erhoben, die nachweisen, welche Eingaben der Teilnehmer während der Nutzung des Angebots zur Beeinflussung des Ablaufs vorgenommen hat (Interaktionsdaten; hierzu gehören z. B. Daten, die bei lexikalischen Abfragen, in interaktive Suchsysteme — etwa elektronische Fahrpläne und Telefonverzeichnisse — und bei Online-Spielen eingegeben werden), darf dies nur in Kenntnis und mit ausdrücklicher Einwilligung des Betroffenen geschehen. Interaktionsdaten dürfen nur unter Beachtung einer strikten Zweckbindung verarbeitet und genutzt werden. Sie sind grundsätzlich zu löschen, wenn der Zweck, zu dem sie erhoben wurden, erreicht wurde (so müssen Daten über die interaktive Suche von Angeboten unmittelbar nach Beendigung des Suchprozesses gelöscht werden). Eine weitergehende Verarbeitung dieser Daten ist nur auf Grundlage einer ausdrücklichen Einwilligung des Betroffenen zulässig.

5. Einwilligung:

Der Abschluß oder die Erfüllung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, daß der Betroffene in die Verarbeitung oder Nutzung seiner Daten außerhalb der zulässigen Zweckbestimmung eingewilligt hat. Soweit Daten aufgrund einer Einwilligung erhoben werden, muß diese jederzeit widerrufen werden können. Für die Form und Dokumentation elektronisch abgegebener Einwilligungen und sonstiger Willenserklärungen ist ein Mindeststandard zu definieren, der einen fälschungssicheren Nachweis über die Tatsache, den Zeitpunkt und den Gegenstand gewährleistet. Dabei ist sicherzustellen, daß der Teilnehmer bereits vor der Einwilligung soweit wie möglich über den Inhalt und die Folgen seiner Einwilligung und über sein Widerrufsrecht informiert ist. Deshalb müssen die Betroffenen sowohl vor als auch nach Eingabe der Erklärung die Möglichkeit haben, auf Einwilligungen, Verträge und sonstige Informationen über die Bedingungen der Nutzung von Diensten, Multimedia-Einrichtungen und Dienstleistungen zuzugreifen und diese auch in schriftlicher Form zu erhalten. Da Verträge oder andere rechtswirksame Erklärungen, die in einer Fremdsprache verfaßt sind, unter Umständen juristische Fachbegriffe enthalten, die nur vor dem Hintergrund der jeweiligen Rechtsordnung zu verstehen sind, sollten zumindest diejenigen Dienste, die eine deutschsprachige Benutzeroberfläche anbieten, derartige Unterlagen auch in deutscher Sprache bereitstellen.

6. Transparenz der Dienste und Steuerung der Datenübertragung durch die Teilnehmer:

Die automatische Übermittlung von Daten durch die beim Betroffenen eingesetzte Datenverarbeitungsanlage ist auf das technisch für die Vertragsabwicklung notwendige Maß zu beschränken. Eine darüber hinausgehende Übermittlung ist nur aufgrund einer besonderen Einwilligung zulässig. Im Hinblick darauf, daß die Teilnehmer bei der eingesetzten Technik nicht erkennen können, in welchem Dienst sie sich befinden und welche Daten bei der Nutzung von elektronischen Diensten bzw. bei der Erbringung von Dienstleistungen automatisiert übertragen und gespeichert werden, ist sicherzustellen, daß die Teilnehmer vor Beginn der Datenübertragung hierüber informiert werden und die Möglichkeit haben, den Prozeß jederzeit abzubrechen. Die zur Nutzung vom Anbieter oder Netzbetreiber bereitgestellte Software muß eine vom Nutzer aktivierbare Möglichkeit enthalten, den gesamten Strom der ein- und ausgehenden Daten vollständig zu protokollieren. Bei einer Durchschaltung zu einem anderen Dienst bzw. zu einer anderen Multimedia-Einrichtung müssen die Teilnehmer über die Durchschaltung und damit mögliche Datenübertragungen informiert werden. Diensteanbieter haben zu gewährleisten, daß sie keine erkennbar unsicheren Netze für die Übertragung personenbezogener Daten nutzen bzw. den Schutz dieser Daten durch angemessene Maßnahmen sicherstellen. Entsprechend dem Stand der Technik sind geeignete (z. B. kryptographische) Verfahren anzuwenden, um die Vertraulichkeit und Integrität der übertragenen Daten sowie eine sichere Identifizierung und Authentifikation zwischen Teilnehmern und Anbietern zu gewährleisten.

7. Rechte von Betroffenen:

Die Rechte von Betroffenen auf Auskunft, Sperrung, Berichtigung und Löschung sind auch bei multimedialen und sonstigen elektronischen Diensten zu gewährleisten. Soweit personenbezogene Daten im Rahmen eines elektronischen Dienstes veröffentlicht wurden, der dem Medienprivileg unterliegt, ist das Gegendarstellungsrecht der von der Veröffentlichung Betroffenen sicherzustellen.

8. Datenschutzkontrolle:

Eine effektive, unabhängige und nicht anlaßgebundene Datenschutzaufsicht ist zu gewährleisten. Den für die Kontrolle des Datenschutzes zuständigen Behörden ist ein jederzeitiger kostenfreier elektronischer Zugriff auf die Dienste und Dienstleistungen und der Zugang zu den eingesetzten technischen Einrichtungen zu ermöglichen. Bei elektronischen Diensten, für die das Medienprivileg gilt, ist die externe Datenschutzkontrolle entsprechend zu beschränken.

9. Geltungsbereich:

Der Geltungsbereich der jeweiligen Regelungen ist eindeutig festzulegen. Es ist sicherzustellen, daß die Datenschutzbestimmungen auch gelten, sofern personenbezogene Daten nicht in Dateien verarbeitet werden.

10. Internationale Datenschutzregelung:

Im Hinblick auf die zunehmende Bedeutung grenzüberschreitender elektronischer Dienste und Dienstleistungen ist eine Fortentwicklung der europäischen und internationalen Rechtsordnung dringend erforderlich, die auch bei ausländischen Diensten, Dienstleistungen und Multimedia-Angeboten ein angemessenes Datenschutzniveau gewährleistet. Die Verabschiedung der sog. ISDN-Datenschutzrichtlinie mit einem europaweiten hohen Schutzstandard ist überfällig. Kurzfristig ist es notwendig, den Betroffenen angemessene Mittel zur Durchsetzung ihrer Datenschutzrechte gegenüber ausländischen Betreibern und Dienstleistern in die Hand zu geben. Die in Deutschland aktiven Dienste aus Nicht-EG-Staaten haben im Sinne der EG-Datenschutzrichtlinie (95/46/EG) vom 24.10.1995 einen verantwortlichen inländischen Vertreter zu benennen.

20.5 Forderung zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 9. Mai 1996 — Forderung zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten

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

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

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

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

20.6 Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen

Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996 — Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen

Mit der Markteinführung des digitalen Fernsehens eröffnen sich für die Anbieter — neben einem deutlich ausgeweiteten Programmvolumen — neue Möglichkeiten für die Vermittlung und Abrechnung von Sendungen. Hinzuweisen ist in erster Linie auf Systeme, bei denen die Kunden für die einzelnen empfangenen Sendungen bezahlen müssen. Dort entsteht die Gefahr, daß die individuellen Vorlieben, Interessen und Sehgewohnheiten registriert und damit Mediennutzungsprofile einzelner Zuschauer erstellt werden. Die zur Vermittlung und zur Abrechnung verfügbaren technischen Verfahren können die Privatsphäre des Zuschauers in unterschiedlicher Weise beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter und Programmlieferanten auf, den Nutzern zumindest alternativ auch solche Lösungen anzubieten, bei denen die Nutzung der einzelnen Programmangebote nicht personenbezogen registriert werden kann, wie es der Entwurf des Mediendienste-Staatsvertrages bereits vorsieht. Die technischen Voraussetzungen für derartige Lösungen sind gegeben.

Die technischen Verfahren sind so zu gestalten, daß möglichst keine personenbezogenen Daten erhoben, gespeichert und verarbeitet werden (Prinzip der Datensparsamkeit). Verfahren, die im voraus bezahlte Wertkarten — Chipkarten — nutzen, um die mit entsprechenden Entgeltinformationen ausgestrahlten Sendungen zu empfangen und zu entschlüsseln, entsprechen weitgehend dieser Forderung. Allerdings setzt eine anonyme Nutzung voraus, daß beim Zuschauer gespeicherte Informationen über die gesehenen Sendungen nicht durch den Anbieter abgerufen werden können.

Die Datenschutzbeauftragten sprechen sich außerdem dafür aus, daß für die Verfahren auf europäischer Ebene Vorgaben für eine einheitliche Architektur mit gleichwertigen Datenschutzvorkehrungen entwickelt werden.

20.7 Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich

Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996 — Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich

Die Entwicklung moderner Informations- und Telekommunikationstechniken führt zu einem grundlegend veränderten Kommunikationsverhalten der Bürger.

Die Privatisierung der Netze und die weite Verbreitung des Mobilfunks gehen einher mit einer weitreichenden Digitalisierung der Kommunikation. Mailboxen und das Internet prägen die Informationsgewinnung und -verbreitung von Privatleuten, von Unternehmen und öffentlichen Institutionen gleichermaßen.

Neue Dienste wie Tele-Working, Tele-Banking, Tele-Shopping, digitale Videodienste und Rundfunk im Internet sind einfach überwachbar, weil personenbezogene Daten der Nutzer in digitaler Form vorliegen. Die herkömmlichen Befugnisse zur Überwachung des Fernmeldeverkehrs erhalten eine neue Dimension; weil immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden, können sie mit geringem Aufwand kontrolliert und ausgewertet werden. Demgegenüber stehen jedoch auch Gefahren durch die Nutzung der neuen Technik zu kriminellen Zwecken. Die Datenschutzbeauftragten erkennen an, daß die Strafverfolgungsbehörden in die Lage versetzt werden müssen, solchen mißbräuchlichen Nutzungen der neuen Techniken zu kriminellen Zwecken wirksam zu begegnen.

Sie betonen jedoch, daß die herkömmlichen weitreichenden Eingriffsbefugnisse auch unter wesentlich veränderten Bedingungen nicht einfach auf die neuen Formen der Individual- und Massenkommunikation übertragen werden können. Die zum Schutz der Persönlichkeitsrechte des einzelnen gezogenen Grenzen müssen auch unter den geänderten tatsächlichen Bedingungen der Verwendung der modernen Informationstechnologien aufrechterhalten und gewährleistet werden.

Eine Wahrheitsfindung um jeden Preis darf es auch insoweit nicht geben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher Thesen zur Bewältigung dieses Spannungsverhältnisses entwickelt.

Sie hebt insbesondere den Grundsatz der spurenlosen Kommunikation hervor. Kommunkationssysteme müssen mit personenbezogenen Daten möglichst sparsam umgehen. Daher verdienen solche Systeme und Technologien Vorrang, die keine oder möglichst wenige Daten zum Betrieb benötigen. Ein positives Beispiel ist die Telefonkarte, deren Nutzung keine personenbezogenen Daten hinterläßt und die deshalb für andere Bereiche als Vorbild angesehen werden kann. Daten allein zu dem Zweck einer künftig denkbaren Strafverfolgung bereitzuhalten, ist unzulässig.

Bei digitalen Kommunikationsformen läßt sich anhand der Bestands- und Verbindungsdaten nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Eine staatliche Überwachung dieser Vorgänge greift tief in das Persönlichkeitsrecht der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse (z. B. Arztgeheimnis, anwaltliches Vertrauensverhältnis). Die Datenschutzbeauftragten fordern daher, daß der Gesetzgeber diesen Gesichtspunkten Rechnung trägt.

Die Datenschutzbeauftragten wenden sich nachhaltig dagegen, daß den Nutzern die Verschlüsselung des Inhalts ihrer Nachrichten verboten wird. Die Möglichkeit für den Bürger, seine Kommunikation durch geeignete Maßnahmen vor unberechtigten Zugriffen zu schützen, ist ein traditionelles verfassungsrechtlich verbürgtes Recht.

Aus Sicht des Datenschutzes besteht andererseits durchaus Verständnis für das Interesse der Sicherheits- und Strafverfolgungsbehörden, sich rechtlich zulässige Zugriffsmöglichkeiten nicht dadurch versperren zu lassen, daß Verschlüsselungen verwendet werden, zu denen sie keinen Zugriff haben. Eine Reglementierung der Verschlüsselung, z.B. durch Schlüsselhinterlegung, erscheint aber aus derzeitiger technischer Sicht kaum durchsetzbar, da entsprechende staatliche Maßnahmen — insbesondere im weltweiten Datenverkehr — ohnehin leicht zu umgehen und kaum kontrollierbar wären.

20.8 Automatisierte Übermittlung von Abrechnungsdaten durch Kassenzahnärztliche Vereinigungen an gesetzliche Krankenkassen

Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996 — Automatisierte Übermittlung von Abrechnungsdaten durch Kassenzahnärztliche Vereinigungen an gesetzliche Krankenkassen

Der in dem Schiedsspruch vom 20. Februar 1995 für die Abrechnung festgelegte Umfang der Datenübermittlung zwischen Kassenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen erfüllt nicht die Anforderungen des Sozialgesetzbuches an diesen Datenaustausch. § 295 SGB V fordert, daß Daten nur im erforderlichen Umfang und nicht versichertenbezogen übermittelt werden dürfen.

Die Datenschutzbeauftragten begrüßen es deshalb, daß der größte Teil der gesetzlichen Krankenkassen in „Protokollnotizen" — Stand 22. März 1996 — den Umfang der zu übermittelnden Daten reduziert hat. Das Risiko der Identifizierbarkeit des Versicherten wurde dadurch deutlich verringert. Zum letztlich erforderlichen Umfang haben die Spitzenverbände der gesetzlichen Krankenkassen erklärt, daß genauere Begründungen für die Erforderlichkeit der Daten erst gegeben werden könnten, wenn das DV-Projekt für das Abrechnungsverfahren auf Kassenseite weit genug entwickelt sei.

Der Verband der Angestellten-Ersatzkassen (VdAK) hat bisher als einziger Spitzenverband der gesetzlichen Krankenkassen diese Datenreduzierungen nicht mitgetragen. Die Datenschutzbeauftragten fordern den VdAK auf, sich in der Frage der Datenübermittlung zwischen Kassenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen der einheitlichen Linie anzuschließen. Dies liegt im gesetzlich geschützten Interesse der Versicherten.

Die besonderen Vorgaben des Sozialgesetzbuches für die Prüfung der Wirtschaftlichkeit der ärztlichen Abrechnungen werden dadurch nicht berührt.

21. Index

Druck: Anker-Druck Bremen