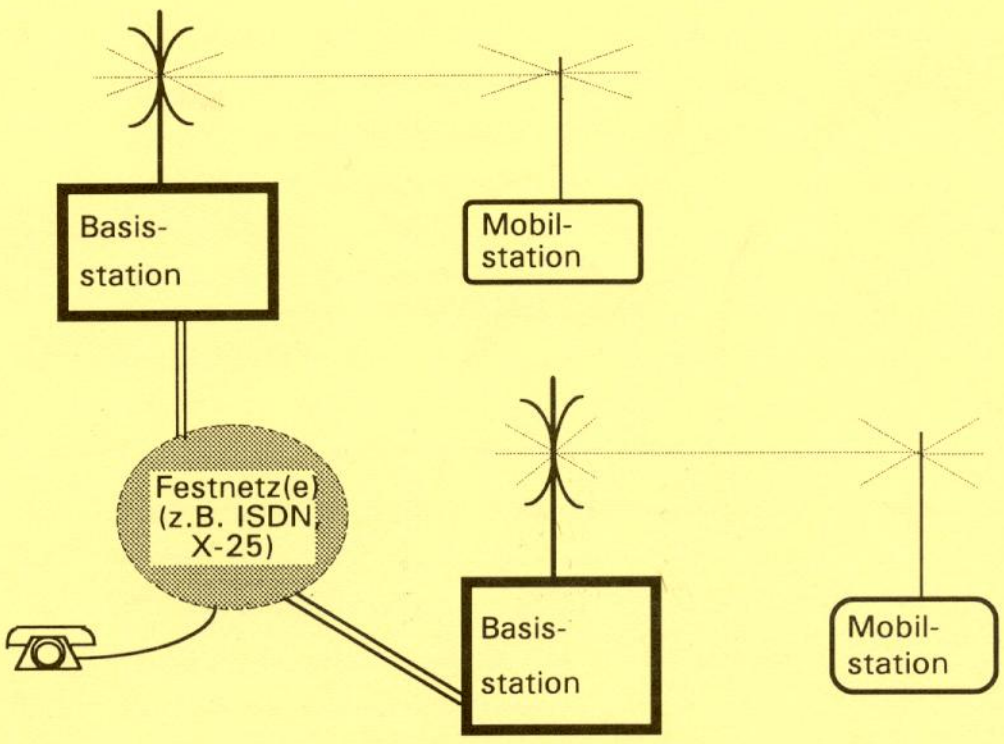
FREIE HANSESTADT BREMEN

Landesbeauftragter für den Datenschutz

17. Jahresbericht



Mobilfunknetz - Zufahrt zum "Information Superhighway"

Vorgelegt zum 31. März 1995

BREMISCHE BÜRGERSCHAFT
Landtag
13. Wahlperiode

Drucksache 13/1181
31.03.95

17. Jahresbericht

des Landesbeauftragten für den Datenschutz

Hiermit erstatte ich der Bremischen Bürgerschaft (Landtag) und dem Präsidenten des Senats meinen 17. Bericht über das Ergebnis meiner Tätigkeit im Jahre 1994 zum 31. März 1995 (§ 33 Abs. 1 Bremisches Datenschutzgesetz - BrDSG)

Dr. Stefan Walz, Landesbeauftragter für den Datenschutz

Inhaltsübersicht

1. Situation und Perspektiven ... 8
1.1. Zur Situation - Digitalisierung der Privatsphäre ? ... 8
1.1.1. Informationelle Selbstbestimmung - das poröse Grundrecht ... 8
1.1.2. Wider das blinde Vertrauen in die Technik ... 9
1.1.3. Zu diesem Bericht ... 10
1.2. Verdichtung des Datennetzes und neue Datenflüsse 1994: die Gesetzesänderungen im Überblick (Tabelle) ... 11
1.3. Zur Lage in Bremen ... 17
1.3.1. Gesetzgebung ... 17
1.3.2. Praktizierter Datenschutz – Anspruch und Wirklichkeit ... 18
2. Ergebnisse der Beratungen des Datenschutzausschusses ... 18
2.1. Themen ... 18
2.2. 16. Jahresbericht für 1993 ... 19
3. Bürgerberatung, Medienkontakte, Fort- und Weiterbildung ... 22
3.1. Eingaben, Beschwerden und Hinweise - der Datenschutzbeauftragte als Ombudsmann ... 22
3.1.1. Verwaltung ... 22
3.1.2. Privatwirtschaft ... 22
3.2. Presse- und Öffentlichkeitsarbeit ... 22
3.3. Aus- und Fortbildung, Vortrags- und Lehrtätigkeit ... 23
4. Die Novellierung des Bremischen Datenschutzgesetzes ... 24
4.1. Regelungsziele und Gang der Beratungen ... 24

4.2. Mehr Rechte für den Einzelnen 24
4.2.1. Schadensersatzanspruch 24
4.2.2. Auskunftsanspruch bei Verbunddateien 25
4.2.3. Erweiterung von Auskunftsanspruch und Akteneinsichtsrecht 25
4.2.4. Eingaben von Mitarbeitern der Verwaltung 25
4.3. Korrekturen beim Anwendungsbereich 25
4.3.1. Bürgerschaft und Gerichte 25
4.3.2. Verwaltung durch Private 26
4.4. Entbürokratisierung 26
4.4.1. Verwaltungsvorschriften nur fakultativ 26
4.4.2. Abschaffung des Dateienregisters 26
4.5. Status und Befugnisse des Landesbeauftragten für den Datenschutz 26
4.5.1. Wahl und Unterrichtungsrechte 26
4.5.2. Kontrollbefugnisse 27
4.5.3. Entscheidungsbefugnis bei der Stellenbesetzung 27
4.5.4. Rederecht in der Bürgerschaft 28
4.6. Bürgerschaft: Auskunftsrecht und Datenschutzausschuß 29
4.7. Entscheidungsbefugnis über Aussage und Aktenvorlage in gerichtlichen Verfahren 29
4.7.1. Element der Unabhängigkeit 29
4.7.2. Besondere Rechtsstellung des Landesbeauftragten 29
4.8. Résümé 30
5. Regelungs- und Kontrollprobleme der Informations- und Kommunikationstechnik 31
5.1. Entwicklungen und Projekte in Bremen 31
5.1.1. Das TuI-Regelwerk - eine unendliche Geschichte ? 31
5.1.2. Einführung von Electronic Mail (X.400) 31
5.1.3. Pilotprojekt "Elektronisches Postsystem" 33
5.1.4. Bürgerinformations-System 33
5.2. Kontrolle der Vernetzung durch Protokollierung von PC-Aktivitäten 33
5.3. Mobilfunk: Informationsbroschüre publiziert 34
6. Datenschutzrichtlinie der Europäischen Union - der Durchbruch 34
6.1. Gemeinsamer Standpunkt verabschiedet 34
6.2. Weiteres Verfahren 35
6.3. Konsequenzen 35
7. Bürgerschaft 35
7.1. Rundfunkübertragungen aus Untersuchungsausschüssen 35
7.1.1. Verfassungsrechtliche Ausgangslage und Abwägungsgebot 35
7.1.2. Zur Interpretation von § 7 BremUAG 36
7.1.3. Die Abwägungskriterien 37

7.2. Gläserne Abgeordnete? ... 38

7.2.1. Parlamentarisches Informations- und Kommunikationssystem (ParlIS) in Planung ... 38

7.2.2. Datenschutzrelevante Systembereiche ... 39

7.3. Bürgerantrag - Zweckbindung für Unterschriftenlisten ... 39

8. Personalwesen ... 40

8.1. KIDICAP - Fremdverarbeitung von Mitarbeiterdaten der Krankenhäuser ... 40

8.1.1. Rechtliche Vorgaben für die Auftragsgestaltung ... 40

8.1.2. Technisch-organisatorisches Sicherungskonzept ... 41

8.2. PUMA - DV-Unterstützung von Personalkostenbugdetierung und Personalverwaltung ... 41

8.2.1. Dezentralisierung der Personal-DV ... 41

8.2.2. Sicherungsdefizite der Netzsoftware ... 42

8.3. Beihilfe - Zentralisierung der Berechnung ... 42

8.3.1. Wegfall des "Instanzenwegs" ... 42

8.3.2. Einhaltung des Trennungsgebots in der SKP ... 43

8.4. Neue Personalaktenrichtlinien ... 43

8.5. Fall: Die gestoppte Stasi-Überprüfung ... 44

8.6. Fall: Adoptionsgeheimnis beim Kindergeld ... 45

8.7. Prüfungsergebnisse ... 45

8.7.1. Telefonanlagen ... 45

8.7.2. Einhaltung der PC-Richtlinien ... 46

8.7.3. Unzulässige Personalnebenakte ... 47

9. Inneres ... 48

9.1. Polizei ... 48

9.1.1. Verbrechensbekämpfungsgesetz: Vermischung von Strafverfolgung und nachrichtendienstlicher Auslandsaufklärung ... 48

9.1.2. EUROPOL-Konvention: Gefährdung der Länderbefugnisse von Polizei und Datenschutz ... 50

9.1.3. Prüfergebnisse: Überlange Speicherung in Polizeidateien und Kriminalakten ... 53

9.2. Ausländer ... 55

9.2.1. Das Ausländerzentralregister - das neue Gesetz und die Folgen ... 55

9.2.2. Erkennungsdienstliche Behandlung aller Bürgerkriegsflüchtlinge? ... 57

9.2.3. Fall: Ausländerbehandlung trotz deutscher Staatsangehörigkeit ... 59

9.2.4. ASYL-CARD ... 60

9.2.5. Verfassungsschutzüberprüfung bei Einbürgerung ... 61

9.3. Straßenverkehr ... 61

9.3.1. Verwertung von Strafurteilen trotz Löschung im Verkehrszentralregister ... 61

9.3.2. Abbildung von Beifahrern auf Radarfotos ... 63

9.4. Melde- und Personenstandswesen ... 63
9.4.1. Wahlkampf mit Wählerdaten ... 63
9.4.2. Meldesperren und Wählerverzeichnis ... 64
10. Justiz ... 66
10.1. Strafakten als multifunktionale Informationsquelle ... 66
10.1.1. Der Entwurf des Bundesrates für ein Strafverfahrensänderungsgesetz 1994 (StVÄG 1994) ... 66
10.1.2 Die Datenschutzkritik ... 66
10.2. Bundesweites staatsanwaltschaftliches Informationssystem ... 67
10.2.1. Ziele des neuen Bundes-SISY ... 67
10.2.2. Fehlende Differenzierung bei der bundesweiten Speicherung ... 67
10.2.3. Risiken des neuen Bundesregisters ... 68
10.3. Sijus-Straf - Rechnernetz und Datenkommunikation für Staatsanwälte ... 68
10.3.1. Systembeschreibung ... 68
10.3.2. Beteiligung des Landesbeauftragten für den Datenschutz ... 69
10.3.3. Datenschutzrechtliche und technische Bewertung ... 69
10.4. Bilanz: Prüfung der Justizvollzugsanstalt Oslebshausen ... 70
10.4.1. Konsequenzen der Beanstandung ... 70
10.4.2. Der erste Schritt: Neue Allgemeinverfügung ... 70
10.4.3. Archivierung inaktueller Unterlagen ... 71
10.4.4. Neue Aktenfunde ... 71
10.4.5. Weitere Maßnahmen ... 71
10.4.6. Abschluß in Sicht ... 72
10.4.7. ADV in den Vollzugsgeschäftsstellen (ADIV) ... 72
11. Bildung und Wissenschaft ... 73
11.1. Schülerbefragung in Bremerhaven ... 73
11.1.1. Die Befragung ... 73
11.1.2. Die Rechtslage ... 73
11.1.3. Die Konsequenzen ... 73
11.2. Erhebungen, Untersuchungen und Forschungsvorhaben an öffentlichen Schulen im Lande Bremen ... 74
11.3. Datenschutz bei Forschungsprojekten ... 74
11.3.1. Merkblatt als Handlungshilfe ... 74
11.3.2. Ausgangspunkt Einwilligungserfordernis ... 75
11.3.3. "File-Trennung", Zweckbindung und Datensicherung ... 75
11.3.4. Genehmigungsvorbehalte ... 76
11.4. Öffentlicher Aushang von Klausur- und Prüfungsergebnissen ... 76
11.4.1. Erster Fall: Hochschule Bremen ... 76
11.4.2. Zweiter Fall: Universität Bremen ... 77

12. Gesundheit, Jugend und Soziales ... 77

12.1. Krankenhäuser ... 77

12.1.1. Fall: Patientendaten im Maßregelvollzug ... 77

12.2. Gesundheit ... 78

12.2.1. Zweckbindung der Klientendaten trotz Funktionsvielfalt der Gesundheitsämter ... 78

12.2.2. Anonymität in der Schwangerschaftskonfliktberatung und beim Sozialamt ... 78

12.3. Jugend und Soziales ... 79

12.3.1. Sozialhilfe per Computer - neues Datenschutzkonzept für das PROSOZ-Verfahren ... 79

12.3.2. Datenverarbeitung und Statistik nach dem Betreuungsgesetz ... 81

12.3.3. Sozialhilfestatistik- das Sozialamt als Zähler ... 82

12.3.4. Fall: Jugendamtsakten auf dem Schuttcontainer ... 83

12.3.5. Fall: Intime Fragen nach "eheähnlicher Gemeinschaft" ... 83

12.3.6. Schutz des Beratungsgeheimnisses im Amt für Soziale Dienste ... 84

12.3.7. Wirtschaftlichkeits- und Qualitätsprüfung - auch mit Mitarbeiter- und Klientendaten ? ... 85

13. Arbeit und Frauen ... 86

13.1. Krankenversicherung ... 86

13.1.1. Die Krankenversichertenkarte (KVK) ... 86

13.1.2. Das Projekt TARZAN der AOK ... 89

13.1.3. Methadon-Substitution — Wegfall der umfassenden Doppelregistrierung ... 91

13.2. Bekämpfung illegaler Beschäftigung: Richtlinien für den Informationsaustausch ... 91

13.3. Teilnehmerkontrollen bei Zuschüssen aus dem Europäischen Sozialfonds ... 92

13.3.1. Gefährdung zugesicherter Vertraulichkeit ... 92

13.3.2. Bundesweite Konsequenzen ? ... 93

14. Umweltschutz und Stadtentwicklung ... 93

14.1. Das Umweltinformationsgesetz - Umsetzung in Bremen ... 93

14.2. Datenaustausch im Umweltbereich - Bund/Länder-Vereinbarung ... 94

14.3. Altlastenkataster noch immer ohne gesetzliche Grundlage ... 94

14.4. Codierte Mülltonne ... 95

14.4.1. Fragen nach der körperlichen Verfassung ... 95

14.4.2. Haushaltsbezug und Fremdabrechnung der Müllgebühren ... 95

15. Bauwesen ... 96

15.1. Überprüfung der Einkommensverhältnisse nach dem Wohnungsbauförderungsgesetz ... 96

16. Finanzen **96**

16.1. Vorlage des Steuerbescheides statt Nachweis von Einzelangaben **96**

16.2. Laptops für die Steuerfahndung **96**

16.3. Finanzamt hilft Handels- und Handwerkskammern **97**

17. Datenschutz in der Privatwirtschaft **97**

17.1. Anordnung und Untersagung - die neuen Sanktionsinstrumente der Aufsichtsbehörde nach dem BDSG 1990 ..... **97**

17.1.1. Datenschutzkontrolle als Teil staatlicher Wirtschaftsaufsicht 97

17.1.2. Voraussetzungen und Verfahren 98

17.2. Kreditinformationssysteme und Handelsauskunfteien **99**

17.2.1. Bedeutung für Wirtschaft und Bürger 99

17.2.2. Nachträgliche Einspeicherung von Negativmerkmalen 100

17.2.3. Nachmeldeverfahren 100

17.2.4. Schufa-online-Verfahren 101

17.2.5. Versandhäuser als Schufakunden 102

17.2.6. Stichprobenkontrolle des "berechtigten Interesseses" 102

17.2.7. Datenabfrage bei angeblicher Vertragsabsicht 102

17.3. Schufa-Selbstauskunft von Mietinteressenten **103**

18. Register der nach dem Bundesdatenschutzgesetz meldepflichtigen Stellen **104**

19. Anlage **105**

Merkblatt zum Datenschutz bei Erhebungen, Untersuchungen und Forschungsvorhaben an öffentlichen Schulen im Lande Bremen **105**

20. Beschlüsse der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Jahr 1994 ..... **107**

20.1. Chipkarten im Gesundheitswesen **107**

20.2. Informationsverarbeitung im Strafverfahren **108**

20.3. Abbau des Sozialdatenschutzes **110**

20.4. Gesetzentwurf der Bundesregierung zur Neuordnung des Postwesens und der Telekommunikation (Postneuordnungsgesetz - PTNeuOG, BR-Drs. 115/94 = BT-Drs. 12/6718) und zu der dafür erforderlichen Änderung des Grundgesetzes (BR-Drs. 114/94 = BT-Drs. 12/6717) **111**

20.5. Ausländerzentralregistergesetz **112**

20.6. Vorschlag der Kommission der Europäischen Union für eine Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik - EG-Statistikverordnung - (KOM(94) 78 endg.; Ratsdok. 5615/94 = BR-Drs. 283/94) **113**

20.7. Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen **115**

20.8. Fehlende bereichsspezifische gesetzliche Regelungen bei der Justiz 115

20.9. Datenschutzrechtliche Anforderungen an ein Übereinkommen der Mitgliedstaaten der Europäischen Union über die Errichtung eines europäischen Polizeiamtes (Europol)..... 116

20.10. Art. 12 Verbrechensbekämpfungsgesetz zur Trennung von Polizei und Nachrichtendiensten 117

20.11. Geänderter Vorschlag für eine Europäische Richtlinie zum Datenschutz im ISDN und in Mobilfunknetzen vom 13. Juni 1994 (KOM (94) 128 endg. - COD 288) 117

Redaktionsschluß: 28. Februar 1995

1. Situation und Perspektiven

1.1. Zur Situation - Digitalisierung der Privatsphäre ?

1.1.1. Informationelle Selbstbestimmung - das poröse Grundrecht

"49 Kameras überwachen Straßen und Plätze der Pariser Vorstadtgemeinde Levallois rund um die Uhr" - diese Zeitungsmeldung aus dem Oktober 1994 ist keine Ausgeburt (nach-) Orwellscher Phantasie, sondern Realität 1994. Die Grundidee, die dahiner steht, ist einfach: Der Bürger selbst ist das größte Sicherheitsrisiko, den es darum ohne Pause zu beobachten und zu überwachen gilt.

Die Versuchung ist groß, diese extreme Form der **"vidéo-surveillance"** abzutun als Resultat einer übertriebenen Sicherheitsdoktrin der derzeitigen französischen Regierung. Doch wird man rasch eines besseren belehrt, wenn man vor der deutschen Haustür kehrt. Das vergangene Jahr hat auch in Deutschland tiefe Einschnitte in die grundgesetzlich verbrieften Individualrechte gebracht:

- Das **Fernmeldegeheimnis** im grenzüberschreitenden Telefonverkehr wurde durch das am 1. Dezember 1994 in Kraft getretene **"Verbrechensbekämpfungsgesetz"** (vgl. dazu in diesem Bericht Ziff. 9.1.1.) teilweise aufgehoben. Jeder, der mit dem Ausland telefoniert, muß mit der Aufzeichnung seines Gesprächs durch den Bundesnachrichtendienst (BND) rechnen; sobald bestimmte "Suchbegriffe" (z.B. aus dem Drogenbereich) fallen, schalten sich automatisch die elektronischen Überwachungsanlagen an. Dies kann für den Journalisten, der über Drogenkriminalität recherchiert und dabei ausländische Gesprächspartner anwählt, ebenso gelten wie für mich als Datenschutzbeauftragten, wenn ich mit europäischen Kollegen über die Ausgestaltung von EUROPOL telefoniere. Bezeichnende Parallele zur französischen Video-Gesetzgebung ist übrigens die Einschränkung der externen Datenschutzkontrolle: Wurde in Frankreich der Datenschutzkommission CNIL die Kontrollbefugnis verweigert, wurden hier die Überprüfungsrechte des eigentlich zuständigen Bundesbeauftragten für den Datenschutz beschnitten.
- Das neue **Ausländerzentralregister-Gesetz** (AZR-G) macht die Daten aller Nichtdeutschen für den Zugriff der Sicherheitsbehörden frei: Ob Angestellter einer japanischen Großbank, ob ziviler Mitarbeiter der hier stationierten US-Streitkräfte, ob Manager einer norwegischen Feinkostfirma: Alle werden über den gleichen Kamm des potentiell straffälligen Ausländers geschoren. Sie müssen sich, weil ohne deutschen Paß, eine bundesweit zentrale Registrierung und jederzeitige Kontrolle ihres Aufenthaltsorts, Status' usw. gefallen lassen. Direkten Computerzugriff auf die Daten des AZR haben u.a. Bundeskriminalamt, Bundesgrenzschutz, Bundesamt und Landesämter für Verfassungsschutz, Bundesnachrichtendienst, Zoll und die Länderpolizeien. Aus einem Verwaltungsregister zur Erleichterung der Arbeit der Ausländerbehörden ist auf diese Weise ein multifunktionales Überwachungsregister geworden (vgl. dazu in diesem Bericht Ziff. 9.3.1.).

Verbrechensbekämpfungs- und AZR-Gesetz sind die vielleicht spektakulärsten, doch keineswegs einzigen Beispiele für die teils schleichende, teils offensichtliche **Aushöhlung des Grundrechts auf informationelle Selbstbestimmung.** Die drohende Entwicklung hin zum Ausbau überwachungsstaatlicher Strukturen war 1994 wie im Jahr davor gekennzeichnet durch eine Fülle gesetzgeberischer Maßnahmen, und zwar nicht nur im Bereich der inneren Sicherheit. Schwerpunkt der Rechtfertigung neuer Datenbanken und Datenflüsse war wieder einmal der Sozialleistungsbereich.

In diesem Jahresbericht habe ich mich wie im letzten Bericht der Mühe unterzogen, diese Tendenz nicht nur zu behaupten, sondern im Detail zu belegen. Die **Aufstellung der 1994 neu eingeführten Befugnisse der Verwaltung zur Erhebung, Speicherung und Übermittlung von Bürgerdaten** (vgl. Ziff. 1.2.) macht deutlich, wie das Datennetz um den Einzelnen zunehmend und in schnellen Schritten engmaschiger wird - eine Ge-

samtperspektive, die bei allen guten Gründen, die es für das jeweils verabschiedete Einzelgesetz geben mag, allzu leicht aus dem Blickfeld gerät.

Bestätigt werden die Befürchtungen, die schon von den Gründervätern der modernen Datenschutzgesetzgebung in den siebziger Jahren geäußert worden sind: Das technisch Machbare drängt immer nach Umsetzung. Anders ausgedrückt: Was der Computer leisten kann, wird irgendwann auch ausgenutzt. Anderweitige Politikerzusagen, aber auch zunächst vorhandene rechtliche Barrieren wie Zweckbindungsgebote oder das Trennungsgebot von Polizei und Nachrichtendiensten erweisen sich bei Änderung des politischen und sozialen Umfelds schnell als poröse Dämme, die den Schutz des Einzelnen nicht mehr zu sichern vermögen.

1.1.2. Wider das blinde Vertrauen in die Technik

Unkritische Technikgläubigkeit steht hier vielfach zusätzlich Pate, obwohl die Verletzlichkeit der kleinen ebenso wie der großen, weltweiten Computernetze, die mangelnde Beherrschbarkeit komplexer Techniksysteme auch 1994 wieder durch spektakuläre, z.T. weltweit beachtete Aktionen belegt wurden. So drangen Hacker auf elektronischem Wege in die Zentrale von British Telecom ein und besorgten sich dort Geheiminformationen der Nachrichtendienste und vertrauliche Angaben aus der Königsfamilie. Auch der zentrale Rechner des Pentagon wurde geknackt.

Nur wer die **Verletzlichkeit hochkompexer IuK-Systeme** und die potentiell dramatischen Auswirkungen von Funktionsstörungen auf die Gesellschaft und den Einzelnen kennt und ins Kalkül zieht, behält den nüchternen Blick für die realistische Abschätzung von Chancen und Risiken neuer Technikentwicklungen für Arbeit, Freizeit und gesellschaftliche Partizipation. Dieser rationale Blick in die nächsten Jahre tut auch bitter not, wenn man nur die wichtigsten Teilelemente den Technikszenarios der Zukunft Revue passieren läßt:

Die **Digitalisierung** von Text, Grafik und Ton ermöglicht die beliebige Kombination dieser Medien und damit die perfekte Manipulation, etwa beim "electronic imaging". Sie erlaubt die Herstellung von Sprachspeichersystemen, die die Bürokommunikation revolutionieren und die herkömmlichen Schreibdienste überflüssig machen werden. Der "information superhighway", die **"Datenautobahn"** oder "Infobahn", stellt die Infrastruktur für die globale Vernetzung, insbesondere für alle Spielarten interaktiver Dienste (**"Multimedia"**). Im "Genomzeitalter" schließlich droht die in der Grundtendenz totalitäre Normung menschlicher Existenz mit biologistisch definierter Abgrenzung zwischen Normalität und Abweichung.

Einiges davon ist bereits heute Realität, andere Entwicklungen gehen allerdings auch langsamer voran, als es die Protagonisten vorausgesagt haben. So wird es "Multimedia" in großem Umfang nach einer jüngeren Prognos-Studie nicht vor Ende dieses Jahrzehnts geben.

Das Gegenkonzept gegen unkritische Technikfaszination ist die **verfassungs- und sozialverträgliche Technikgestaltung** in der Informationsgesellschaft. Ihre wichtigste Zielsetzung ist die Wahrung des infomationellen Selbstbestimmungsrechts der Bürgerinnen und Bürger. Die Datenschutzbeauftragten sollen und werden auch in Zukunft in diesem Sinne mahnen, beraten und kontrollieren. Als kritische Reisebegleiter auf der "Datenautobahn" werden sich die Datenschützer nicht abschütteln lassen. Doch bleibt ihre Arbeit Stückwerk, wenn sie nicht eingebettet ist in ein möglichst breit verankertes **Datenschutzbewußtsein**, vor allem aber unterstützt wird von Aktivitäten politischer und gesellschaftlicher Gruppen, die die Sorge um die Bewahrung der Integrität der Privatsphäre in der Informationsgesellschaft umtreibt.

Entscheidend für eine datenschutzkonforme Ausgestaltung der Informations- und Kommunikationstechnologie ist aber vor allem die **technische Intelligenz.** Um so erfreulicher ist die Feststellung, daß es in Deutschland vor allem an Universitäten, aber auch in Verwaltung und Wirtschaft kritische Informatiker gibt, die sich gegen blinde Technikbegeisterung wehren, die sich über die Auswirkungen ihrer Verfahren und Programme Gedanken machen oder die alternative, die Anonymität der Nutzer gewährleistende Techniklö-

sungen entwickeln. Gerade Bremen kann sich hier , z.B. mit seinem universitären Studiengang "Angewandte Informatik", durchaus sehen lassen. Diesem Umfeld ist es auch zu verdanken, daß die Tagung "1984 plus 10 - Realität und Utopie der Informatik" des "Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIFF) e.V." im Oktober 1994 gerade in Bremen stattfand[1].

1.1.3. Zu diesem Bericht

Der nachstehende Bericht enthält Beispiele für Schlamperei, Gedankenlosigkeit und Planungsfehler beim Umgang mit personenbezogenen Daten im allgemeinen und beim Einsatz von IuK-Technik im besonderen. Er bringt aber auch Beispiele für gelungene Kooperation zwischen Anwendern und dem Datenschutz, für mitdenkende Behördenmitarbeiter und Kritikbereitschaft von Bürgern. Dieser Bericht belegt auch, wie Anforderungen des Datenschutzes und der Datensicherheit, die früher als übertrieben bürokratisch oder rückständig technikfeindlich angesehen wurden, heute zur akzeptierten Verwaltungsroutine gehören (zur Lage in Bremen vgl. Ziff. 1.3).

Wie der 16. Jahresbericht enthält auch die vorliegende 17. Ausgabe nur eine Auswahl der Datenschutzthemen, mit denen meine Dienststelle im vergangenen Jahr befaßt war. Auch wenn die Redaktion des Berichts meinen Mitarbeitern und mir jedes Mal erneut einen nicht unerheblichen Arbeitsaufwand verursacht, habe ich mich bei der Novellierungsdiskussion zum BrDSG für die Beibehaltung des einjährigen Turnus eingesetzt: Der Bericht stellt Transparenz für Parlament, Bürger, Medien und Behörden her über das, was "der Datenschutz" tut und will. Auch soll er Anregungen für datenschutzgerechte Verarbeitungspraxis bieten und neu aufgetauchte Interpretationsfragen zum Datenschutzrecht beantworten. All dies kann er nur leisten, wenn er möglichst aktuell formuliert und präsentiert wird.

Im letzten Jahr zum ersten Mal gab es das Kapitel über die Arbeit des Datenschutzausschusses der Bürgerschaft und die Tabelle über die neuen gesetzlichen Regelungen zum Datenschutz. Das Echo war positiv, so daß beide Themen auch in diesen Bericht aufgenommen sind vgl. u. Ziff. 1.2. und 2.).

[1] Informationen hierzu können bei mir angefordert werden.

1.2. Verdichtung des Datennetzes und neue Datenflüsse 1994: die Gesetzesänderungen im Überblick (Tabelle)

Betroffene	*von*	*an*	*Verfahren*	*Datenart*	*Zweck*	*Gesetz*
Beschäftige im bremischen öffentlichen Dienst	Senatskommission für das Personalwesen	Beschäftigungsdienststellen	Konventionell	Bruttobesoldungs- bzw. Gehaltsdaten	Budgetierung der Personalkosten	§ 13 Abs. 2 Haushaltsgesetz 1995
verurteilte Straftäter und Verdächtige bei Verfahrenseinstellungen und Freisprüchen	Bundeszentralregister als Bundes-Sisy an Staatsanwaltschaft	Bundeszentralregister als Bundes-Sisy an Staatsanwaltschaft	Datenfernübertragung und on-line	Strafverfahrensdaten		Verbrechensbekämpfungsgesetz
Fernsprechteilnehmer	Bundesnachrichtendienst	Staatsanwaltschaft	unbekannt	Gesprächsinhalte und -erkenntnisse aus nicht leitungsgebundenen Telefongesprächen	Hinweise auf vermeintliche Straftaten betr. insbesondere BTM, Terrorismus, Geldwäsche, u. Waffenhandel	Verbrechensbekämpfungsgesetz
Bürger	Bundesgrenzschutz	öffentliche Stellen	konventionell u. Datenfernverarbeitung über das INPOL-System	Identitäts- und Inhaltsdaten	polizeiliche Aufgaben an der Grenze einschl. Flughäfen, im Ausland und beim Schutz von Verfassungsorganen	Änderung BGS-Gesetz
Funk- und Fernsprechteilnehmer	Bundesgrenzschutz	Verfassungsschutz des Bundes und der Länder	Datenträger	Funkdaten und Funkverbindungsdaten	Daten von vermuteten nachrichtendienstlichen Funkverbindungen	Änderung BGS-Gesetz
Bürger	Bundesgrenzschutz	ausländische Behörden und zwischenstaatliche Stellen	konventionelle Mitteilungen in Papierform	Identitäts- und Inhaltsdaten	grenzpolizeiliche und grenzsichernde Aufgaben	Änderung BGS-Gesetz

Betroffene	*von*	*an*	*Verfahren*	*Datenart*	*Zweck*	*Gesetz*
Bürger	Bundesgrenzschutz	nichtöffentliche Stellen	konventionell	Identitäts- und Inhaltsdaten	Sicherheitsaufgaben	Änderung BGS-Gesetz
Ausländer, Asylbewerber und Visum-Antragssteller	Ausländerzentralregister	nichtöffentliche Stellen einschl. Privatpersonen	konventionell	Identitäts- und Inhaltsdaten	bei Vorliegen eines rechtlichen Interesses des Ersuchenden	Ausländerzentralregistergesetz
Ausländer, Asylbewerber und Visum-Antragssteller	Ausländerzentralregister	öffentliche Stellen (alle Bundes- Landes- und Kommunalbehörden, Körperschaften öffentlichen Rechts (z.B. Kammern) u. Notare	konventionell und Datenfernverarbeitung	Identitätsdaten Hinweisdaten und Inhaltsdaten	Erfüllung öffentlicher Aufgaben	Ausländerzentralregistergesetz
Ausländer, Asylbewerber und Visum-Antragssteller	Ausländerzentralregister	humanitäre nichtöffentliche Stellen	konventionell	Identitäts- und Inhaltsdaten	zur Erfüllung humanitärer und sozialer Aufgaben	Ausländerzentralregistergesetz
Ausländer, Asylbewerber und Visum-Antragssteller	Ausländerzentralregister	ausländische und zwischenstaatliche Stellen	konventionell	Identitäts- und Inhaltsdaten	zur Erfüllung berechtigter Interessen -auf Gegenseitigkeit-	Ausländerzentralregistergesetz
Ausländer, Asylbewerber und Visum-Antragssteller	Ausländerzentralregister	Polizei	Datenfernverarbeitung	alle Daten	für polizeiliche Zwecke im weitesten Sinne	Ausländerzentralregistergesetz
Ausländer, Asylbewerber und Visum-Antragssteller	Ausländerzentralregister	Nachrichtendienste (Verfassungsschutz, Bundesnachrichtendienst u. Militärischer Abschirmdienst)	auch durch Datenfernverarbeitung	alle Daten	für nachrichtendienstliche Zwecke	Ausländerzentralregistergesetz

Betroffene	*von*	*an*	*Verfahren*	*Datenart*	*Zweck*	*Gesetz*
Ausländer, Asylbewerber und Visum-Antragssteller	alle öffentlichen Stellen (insbesondere Ausländerbehörden, Polizei, Staatsanwaltschaften Nachrichtendienste, Staatsangehörigkeitsbehörden u.a.)	AZR	konventionell und durch Datenfernverarbeitung	übermittlungspflichtige Daten (z.B. Namen, Vornamen, andere Schreibweisen, Herkunftsland, Aufenthaltsstatus, Verfahrensdaten, Ausweis-Nr., Aliaspersonalien u.v.a.m. für das Register)	zur Führung des Registers	Ausländerzentralregistergesetz
Ausländer, Asylbewerber und Visum-Antragssteller	alle öffentlichen Stellen	AZR	konventionell und durch Datenfernverarbeitung	Suchvermerke	zur Aufenthaltsfeststellung	Ausländerzentralregistergesetz
Ausländer, Asylbewerber und Visum-Antragssteller	Polizei	AZR	Datenfernverarbeitung	Suchvermerke	zur Festnahme	Ausländerzentralregistergesetz
Ausländer, Asylbewerber und Visum-Antragssteller	Nachrichtendienste (Verfassungsschutz, Bundesnachrichtendienst u. Militärischer Abschirmdienst)	AZR	konventionell und durch Datenfernverarbeitung	Suchvermerke	zur Verbleibskontrolle und zur Feststellung von Sachverhalten	Ausländerzentralregistergesetz
Einwohner / Wohnungsgeber	Meldepflichtige Einwohner / Wohnungsgeber	Meldebehörden	Vorlage	Bestätigung des Ein- oder Auszugs des Meldepflichtigen durch den Wohnungsgeber	An, Um- oder Abmeldung des Betroffenen	§ 14 Brem. Meldegesetz

Betroffene	*von*	*an*	*Verfahren*	*Datenart*	*Zweck*	*Gesetz*
Einwohner	Meldebehörden	öffentlich-rechtliche Religionsgesellschaften	Magnetbänder / Listen	Künstlernamen, Staatsangehörigkeiten, Haupt- und Nebenwohnung/ bei Verheirateten: Tag der Eheschließung	Aufgabenerfüllung der öffentlich-rechtlichen Religionsgesellschaften	§ 19 Melderechtsrahmengesetz (Erweiterung der übermittelbaren Angaben)
Einwohner	Meldebehörden	Parteien, Wählergruppen und sonstige Träger von Wahlvorschlägen	Adreßaufkleber	Vor- und Familiennamen, Doktorgrad, Anschriften	Durchführung von Wahlen zum Deutschen Bundestag oder Europäischen Parlament	§ 22 Melderechtsrahmengesetz (Erweiterung der übermittelbaren Angaben)
Schüler	Öffentliche Schulen	Öffentliche Schulen	Listen/ Aktenauszüge	Entwicklungs- und Verhaltensdaten	Gemeinsame Unterrichtung, Erziehung und Betreuung von Schülern durch mehrere Schulen	§ 6 Schuldatenschutzgesetz
Schuldner	Amtsgericht	Kammern Verbände Auskunfteien	Listen, überwiegend Datenträgeraustausch	"Offenbarungseid"	Informationen aus dem Schuldnerverzeichnis	§ 915 ff. ZPO
Handwerksmeister und -firmen	Handwerkskammer	Statistisches Landesamt	Magnetbänderaustausch ist vorgesehen	Namen und Anschriften der gewerblichen Niederlassung in die Handwerksrolle eingetragener Personen, eingetragene Handwerke, Eintragungsgrund nach der Handwerksordnung	Durchführung der Handwerkszählung	§ 8 Handwerksstastikgesetz

Betroffene	*von*	*an*	*Verfahren*	*Datenart*	*Zweck*	*Gesetz*
Abfallförderer und Betreiber genehmigter Abfallentsorgungs- und verwertungsanlagen	Senator für Umweltschutz und Stadtentwicklung	Statistisches Landesamt	noch offen	Namen und Anschriften	Durchführung der Erhebung der Abfallentsorgung einschl. bestimmter Rückstände gem. Umweltstatistikgesetz	§ 19 Umweltstastikgesetz
Mieter/ Bezieher von Wohngeld	Wohngeldstelle	Amt für Wohnung und Städtebauförderung	Datenübermittlung auf Ersuchen / automatischer Datenabgleich	Identifikationsdaten / Tatsache des Wohngeldbezugs	Überprüfung der Fehlsubventionierung	2. SGB-Änderungsges. neuer § 37a Wohngeldges. / in Kraft seit 14.6.1994
gesetzlich Krankenversicherter	**Ärzte**	1. Kassenärztliche Vereinigungen 2. Krankenkassen	noch unbekannt	1. ärztliche Befunde 2. Angaben über Leistungen	1. Prüfung ärztlicher Abrechnungen auf Rechtmäßigkeit 2. Prüfung späterer Leistungsgewährung	2. SGB-Änderungsges. Ergänzung von § 295 SGB V
Kranken- und Pflegeversicherte	1. Pflegekassen 2. Krankenkassen	1. Pflegekassen 2. Krankenkassen	gemeinsame Datenverarbeitung	Angaben über Leistungsvoraussetzungen	Vermeidung von Doppelleistungen	Pflegeversicherungsgesetz v. 28.5.1994
Eltern	Meldebehörden	Kindergeldstellen	regelmäßige Übermittlungen, voraussichtlich automatisiert; nach Maßgabe einer noch zu erlassenden Rechtsverordnung	Daten nach § 18 Abs. 1 Melderechtsrahmengesetz (insbesondere Namen, Anschrift und Geburtsdatum)	Prüfung der Rechtmäßigkeit des Bezugs von Kindergeld	§ 21 des Neufassung des Bundeskindergeldgesetzes vom 9.2.1994

Betroffene	*von*	*an*	*Verfahren*	*Datenart*	*Zweck*	*Gesetz*
Beteiligte an grenzüberschreitender Sonderabfallentsorgung einschließlich Erzeuger und Entsorger	Landesabfall- und Umweltbehörden, Zoll, Polizei und verschiedene Bundesbehörden	Landesabfall- und Umweltbehörden, Zoll, Polizei und verschiedene Bundesbehörden	Datenfernübertragung	Adress- und Geburtsdaten der an der Entsorgung Beteiligten	Überwachung der grenzüberschreitenden Sonderabfallentsorgung und Erfüllung von Informationspflichten	§ 6 Ausführungsgesetz zum Basler Übereinkommen
Ingenieure	Ingenieurkammer	andere Ingenieurkammern, Aufsichtsbehörden, Bau-, Wirtschafts- und Wissenschaftsbehörden	Auskunft	Datenkatalog aus der Liste der beratenden Ingenieure	Erfüllung der Aufgaben der Ingenieurkammer oder der auskunftsuchenden Stelle.	§ 10 Brem. Ingenieurgesetz
Steuerbürger mit Schulden gegenüber öffentlichen Stellen	Finanzamt	Zentrale Vollstrekkungsstelle beim Finanzamt Bremen-Mitte	konventionell	alle Steuerdaten	für die Zwangsvollstreckung auch anderer fiskalischer Forderungen brem. öffentlicher Stellen	Änderung § 249 AO
Gewerbetreibende Steuerbürger	Finanzamt	Handels- oder Handwerkskammer	Datenträgeraustausch und Datenfernverarbeitung	Steuermeßzahl und Identitätsdaten	Berechnung der Kammerbeiträge (bisher weitgehend pauschaliert)	§ 31 AO

1.3. Zur Lage in Bremen

1.3.1. Gesetzgebung

Auch in diesem Jahresbericht kann es keine pauschale Gesamtnote für den Stand des Datenschutzes in Bremen geben. Licht und Schatten wechseln sich ab; dies belegen die folgenden Beiträge. Im Zentrum der zu vermeldenden positiven Ereignisse steht ohne Zweifel das Ende der Ausschußberatungen zur Novellierung des Bremischen Datenschutzgesetzes. Der Datenschutzausschuß verabschiedete seinen Bericht am 2. Februar 1995 (Bürgerschafts-Drucks. 13/1139 vom 07.02.95). Erst nach diesem Zeitpunkt wurde in der Bürgerschaft die Frage des Anwendungsbereichs des Gesetzes im Hinblick auf die Stadtbürgerschaft, die Deputationen usw. problematisiert. In der Plenarsitzung am 23. Februar wurde daher die erste Lesung unterbrochen und der Gesetzentwurf noch einmal an den Datenschutzausschuß sowie erstmals an den Verfassungs- und Geschäftsordnungsausschuß verwiesen. Bei Redaktionsschluß dieses Berichts stand daher noch nicht fest, ob die Novellierung des BrDSG noch in dieser - verkürzten - Legislaturperiode verabschiedet werden kann. Die Neuregelung soll die Rechte der Bürgerinnen und Bürger gegenüber den Behörden ebenso wie meine Unabhängigkeit und Kontrollbefugnisse stärken (ausführl. dazu u. Abschnitt 4).

In mehreren Bereichen hat der bremische Gesetzgeber spezielle Datenschutznormen erlassen, so etwa

- im Bürgerantragsgesetz zur Zweckgebundenheit und Vernichtung von Unterschriftenlisten (vgl. Ziff. 7.3),
- im Haushaltsgesetz 1995 zur Übermittlung von Besoldungs- und Gehaltsdaten an die Personalstellen (vgl. dazu Ziff. 8.2),
- im Ingenieurgesetz über die Datenverarbeitung der Ingenieurkammer und
- im Schuldatenschutzgesetz zur Anpassung an die Schulrechtsnovelle.

Dagegen konnten andere datenschutzrechtlich bedeutsame Regelungsvorhaben in dieser Wahlperiode nicht verwirklicht werden.

Diese Aussage gilt u.a. für die seit langem angemahnte gesetzliche Regelung des Verfahrens der Sicherheitsüberprüfung für die Bediensteten der Verwaltung in Bremen (vgl. 15. JB, Ziff. 5.3.2), um deren Vorlage auch der Datenschutzausschuß den Senator für Inneres gebeten hatte (vgl. 16. JB, Ziff. 1.2 und 1.4). Die Dringlichkeit ebenso klarer wie restriktiver Verfahrensregelungen wird nachhaltig unterstrichen durch die auch in den Medien ausführlich wiedergegebenen Ergebnisse der von meinem niedersächsischen Kollegen beim dortigen Verfassungsschutzamt durchgeführten Überprüfung von Akten aus Sicherheitsüberprüfungen (vgl. LfD Niedersachsen, 12. Tätigkeitsbericht für 1993/1994, Ziff. 14.3.). Zwar erhielt ich vom Senator des Innern im Januar 1995 einen ersten Arbeitsentwurf, doch habe ich in meiner Stellungnahme deutlich gemacht, daß die Regelungen in bezug auf den Kreis der Betroffenen und die Intensität der Überprüfung viel zu weit gingen.

Der verkürzten Wahlperiode zum Opfer fällt möglicherweise auch der Entwurf für ein Gesetz über den öffentlichen Gesundheitsdienst mit dringend notwendigen Bestimmungen über die Verarbeitungsbefugnisse der Gesundheitsämter, die Geheimhaltungspflichten für Klientendaten und die amtsinterne Zweckbindung (vgl. u. Ziff. 12.2.1; s. bereits 16. JB, Ziff. 8.5.1).

Entscheidungen des Landesgesetzgebers in der nächsten Wahlperiode stehen an u.a. bei der aufgrund Bundesgesetzes notwendigen Novellierung des Bremischen Meldegesetzes (vgl. u. Ziff. 9.4.1) und - falls der Bundesgesetzgeber nicht umgehend tätig wird (Stichwort: Bodenschutzgesetz) - für den Aufbau und die Nutzung von Altlastenkatastern.

1.3.2. Praktizierter Datenschutz – Anspruch und Wirklichkeit

Die Beiträge in diesem Jahresbericht bieten wie immer ein breites Spektrum behördlicher Reaktionen auf die gesetzlichen Anforderungen ebenso wie auf meine Kritik, Anregungen und Ratschläge. Von meiner schärfsten gesetzlichen Waffe, der förmlichen Beanstandung nach § 29 BrDSG, habe ich nur im Fall des TARZAN-Projekts der AOK Bremen/Bremerhaven Gebrauch machen müssen, der durch die Dauer und den Umfang der aus meiner Sicht unzulässigen Datenverarbeitung und die Sensibilität der genutzten Informationen hervorsticht (vgl. u. Ziff. 13.1.2), und bei der Befragungsaktion an einer Bremerhavener Schule (vgl. u. Ziff. 11.1). Nur knapp an der Beanstandung vorbeigeschrammt ist die Senatskommission für das Personalwesen (SKP) im Hinblick auf die sehr unbefriedigenden Ergebnisse meiner Prüfung vor Ort, die sich auf die Einhaltung der diversen Richtlinien beim Betrieb der dortigen Arbeitsplatzrechner bezog, Richtlinien, die pikanterweise zum Teil von der SKP selbst erlassen worden sind (vgl. dazu u. Ziff. 8.7.2).

Insbesondere - dies gilt keineswegs nur für die SKP - das Fehlen oder die Unzulänglichkeit der nach § 7 Abs. 3 BrDSG zu führenden Geräteverzeichnisse macht für mich deutlich, daß viele Dienststellen die wichtige Funktion dieser Übersicht nicht nur für Datenschutzkontrollen, sondern auch und gerade für die Transparenz der Arbeitsorganisation und der vorhandenen Betriebsmittel und damit für den sparsamen Umgang mit Haushaltsmitteln verkennen. Positives Beispiel für ein aktuelles Geräteverzeichnis ist das Statistische Landesamt.

Zu den ständigen Kritikpunkten im Jahresbericht gehört die Tatsache, daß ich immer wieder von senatorischen Behörden über wichtige Regelungsvorhaben oder Automationsprojekte zu spät oder unzureichend informiert werde. Deshalb habe ich auch darauf gedrungen, daß die Informationspflichten der Ressorts mir gegenüber, d.h. deren Pflicht zur vorherigen unaufgeforderten Unterrichtung, im novellierten BrDSG erweitert bzw. präziser gefaßt wird (vgl. § 27 Abs. 4 BrDSG in der Neufassung des Ausschußentwurfs).

Die Chronistenpflicht gebietet aber, auch auf die zahlreichen Beispiele intensiver und gelungener Kooperation zwischen bremischen Behörden und dem Datenschutzbeauftragten hinzuweisen. Dazu gehören etwa die zügige Reaktion der SKP bei der Korrektur eines Kindergeldformulars (vgl. u. Ziff. 8.6), die rechtzeitige Einschaltung beim "Schwarzarbeitserlaß" des Senators für Arbeit (vgl. u. 13.2), die intensive Konsultation durch den Senator für Gesundheit beim Entwurf für ein ÖGD-Gesetz (vgl. u. 12.2.1) und die bereitwillige Kooperation der BreKom bei der Lösung von Datenschutzfragen im Netzbereich und bei der Mobilkommunikation.

Sorge bereitet mir, wie sich zwar einerseits die technische Infrastruktur im TuI-Bereich Bremens dynamisch entwickelt, vor allem was die interne wie behördenübergreifende Vernetzung angeht, andererseits aber die zugehörige Regelungsstruktur, Voraussetzung und Instrument für eine konzeptionelle Gesamtplanung, nur zögerlich vorankommt. Diese Diskrepanz jedenfalls zu verringern halte ich für eine äußerst wichtige politische Führungsaufgabe: Das sog. TuI-Regelwerk, das ja auch und gerade den einzelnen Behörden Planungssicherheit geben soll, muß mit Nachdruck fertiggestellt werden (vgl. dazu u. Ziff. 5.1.1).

Last but not least erwähne ich wieder die wichtige Unterstützung, die ich durch den Datenschutzausschuß der Bürgerschaft erhalten habe, und zwar nicht nur bei der Beratung des 16. Jahresberichts (zu den Ergebnissen vgl. Ziff. 2.2), sondern auch bei aktuellen Auseinandersetzungen mit Ressorts sowie in Personal- und Haushaltsangelegenheiten meiner Dienststelle.

2. Ergebnisse der Beratungen des Datenschutzausschusses

2.1. Themen

Erster Schwerpunkt der Arbeit des Datenschutzausschusses im Berichtszeitraum war die Novellierung des Bremischen Datenschutzgesetzes (dazu ausf. Ziff. 4), die in nicht weniger als 12 Sitzungen auf der Tagesordnung stand. Zweiter Schwerpunkt war die Bera-

tung meines 16. Jahresberichts (16. JB) für 1993. Behandelt wurden daneben zahlreiche aktuelle Themen.

2.2. 16. Jahresbericht für 1993

Von den Ergebnissen und Erkenntnissen der Ausschußberatungen zu den Einzelpunkten des 16. Jahresberichts, die am 7. März mit der Annahme des Ausschußberichts abgeschlossen wurden, greife ich folgende Punkte heraus:

Zu 16. JB, Ziff. 2.3.1.2 Funkverkehr der Behörden und Organisationen mit Sicherheitsaufgaben

Der Ausschuß äußerte seine Erwartung, daß der Senat die notwendigen Vorkehrungen trifft, um so schnell wie möglich die erforderliche Vertraulichkeit der Funkkommunikation sicherzustellen.

Zu 16. JB, Ziff. 2.3.2.1 Organisatorische Veränderungen

Ich hatte darauf hingewiesen, daß der Abschluß der Überarbeitung der Regelungen zur Planung und zum Einsatz der ADV in der bremischen Verwaltung (TuI-Regelwerk) immer wieder verschoben worden ist. Der Datenschutzausschuß hat sich nach der Diskussion vorbehalten, den Sachstand im Sommer 1995 erneut zu prüfen (vgl. dazu unten Ziff. 5.1.1).

Zu 16. JB, Ziff. 4.1. Verkürzung des Akteneinsichtsrechts

Strittig war zwischen dem Schulsenator und mir die Frage, ob über die Zuordnung von Unterlagen über Lehrer zu den Personalakten oder zu den Sachakten nur in dem von mir berichteten Einzelfall unzutreffend entschieden worden war oder sich daraus auch auf Unsicherheiten in der Handhabung an anderen Schulen schließen ließ, was zu einer klarstellenden Intervention des Schulsenators hätte führen müssen. Der Ausschuß kam überein, daß zunächst der Bildungssenator mir eine Aufstellung der für die Aktenführung im Bildungsbereich geltenden Regelungen zuleitet. Dies ist inzwischen geschehen. Ich werden dem Ausschuß in einer der künftigen Sitzungen berichten, ob aufgrund meiner Prüf- und Beratungserfahrungen Bedarf für eine Information an alle Schulleitungen zur Personal- und Sachaktenführung besteht.

Zu 16. JB, Ziff. 4.2 Mitteilung von Schwangerschaften an den Betriebsarzt

Thematisiert hatte ich die Frage, unter welchen Voraussetzungen der Betriebsarzt über Schwangerschaften von Beschäftigten informiert werden darf. Im konkreten Fall ging es um die Beschäftigten in Krankenhäusern. Inzwischen hat der Senator für Gesundheit, Jugend und Soziales ein Formblatt entwickelt, das noch mit den Krankenhäusern abgestimmt werden muß.

Zu 16. JB, Ziff. 5.1.1 Informationssystem ISA-D ohne ausreichenden Datenschutzstandard

Nach Einführung des DV-Systems ISA-D (Informationssystem Anzeigen - Dezentral) habe ich darauf hingewiesen, daß hierzu eine Rechtsverordnung gem. § 14 Abs. 2 BrDSG erforderlich ist sowie ein Datenschutzkonzept zu erarbeiten und Dienstanweisungen zur Benutzung von ISA-D zu erlassen sind. Des weiteren hatte ich gefordert, daß bei der technischen Ausgestaltung alle abfrageberechtigten Polizisten Chip- oder Magnetkarten erhalten müssen, um die Abwehr unberechtigter Benutzer sicherzustellen.

Im Datenschutzausschuß wurde dargelegt, die Rechtsverordnung sei in der internen Abstimmung. Das Datenschutzkonzept und die Dienstanweisung sind mir im Januar 1995 vorgelegt worden. Ich habe dazu noch kleinere Änderungen vorgeschlagen.

Zur Frage der Magnet- oder Chipkarten will das Ressort nicht zwingend an der Magnetkarte festhalten, sondern erwägt, bei Gelegenheit evtl. auf ein Chipkartensystem umzustellen.

Erledigungspunkt ist auch nach wie vor die Bereinigung der Datenbestände in ISA. Der Senator für Inneres und Sport hat darauf hingewiesen, von 1987 bis 1993 seien 520.000 Datensätze gelöscht worden. Es werde weiterhin eine Optimierung angestrebt. Wenn das Datenbanksystem umgestellt werde, werde bei der Überführung der alten Datenbestände parallel eine Prüfung der Speichernotwendigkeit durchgeführt.

Zu 16. JB, Ziff. 5.1.2 Erfolgskontrolle der erweiterten Fahndungsbefugnisse

Im Zusammenhang mit diesem Problem habe ich betont, daß es eine Anforderung des Bundesverfassungsgerichts an den Gesetzgeber ist, eine Prognose aufzustellen, wenn er in Grundrechte eingreifende Maßnahmen vorsieht. Dazu gehören auch Eingriffe in das Persönlichkeitsrecht und das Grundrecht auf informationelle Selbstbestimmung. Diese Risikoprognose, besteht darin festzustellen, was die bisherigen Instrumente bewirkt haben und welchen Nutzen neue Mittel bringen können. Kern der Stellungnahme des Senators für Inneres und Sport war es aber, Aussagen über die Wirksamkeit einzelner polizeilicher Ermittlungsmethoden ließen sich allgemein nicht machen.

Außerdem teilte er mit, daß er den Vorschlag der Datenschutzkonferenz, eine sogenannte Rechtstatsachensammlung einzuführen, unterstützt. Er bezweifle aber, daß die zu Umfang und Tiefe der Erhebung aufgestellten Forderungen aus der polizeilichen Praxis heraus erfüllt werden könnten.

Zu 16. JB, Ziff. 5.1.3 Automatisiertes Fingerabdruckidentifizierungssystem (AFIS)

Im Jahre 1993 ist das automatisierte Fingerabdruckidentifizierungssystem (AFIS) in Betrieb genommen worden. Auch Bremen beteiligt sich an diesem System, in dem Fingerabdrücke von Asylbewerbern, von anderen Ausländern und von Deutschen, die von der Polizei erkennungsdienstlich behandelt wurden, gespeichert sind. AFIS wurde allerdings in Betrieb genommen, ohne daß die erforderlichen datenschutzrechtlichen Voraussetzungen getroffen worden sind.

Insbesondere habe ich ergänzende Regelungen für erforderlich gehalten, weil die Rechtsgrundlagen sowohl im Bremischen Polizeigesetz als auch in der StPO nicht bestimmt genug sind.

Der Senator für Inneres und Sport hat darauf hingewiesen, daß der Bund beabsichtige, eine Errichtungsanordnung zu erlassen. Ich habe daraufhin vorgeschlagen, noch einmal die Dringlichkeit dieser Anordnung gegenüber dem zuständigen Bundesinnenministerium deutlich zu machen. Diesem Vorschlag hat sich der Ausschuß angeschlossen.

Zu 16. JB, Ziff. 5.4.1 Fall: Der Standesbeamte als unberechtigter Bevölkerungsstatistiker

Hierbei ging es um das Grundsatzproblem, daß Verwaltungsvollzugsaufgaben, nämlich die Beurkundung von Personenstandsfällen, verknüpft werden mit bevölkerungsstatistischen Erhebungsvorgängen, die im Auftrag des Statistischen Landesamtes erfolgen. Diese Vermischung von Verwaltung und Statistik hat das Bundesverfassungsgericht im Volkszählungsurteil für unzulässig erklärt.

Um das Trennungsgebot zu verwirklichen, halte ich die Änderung des Bevölkerungsstatistikgesetzes für notwendig. Der Ausschuß hat den Senator für Inneres und Sport gebeten, auf Bundesebene die Änderung des Gesetzes zu forcieren.

Zu 16. JB, Ziff. 6.3 Mitteilung von Bußgeldschuldnern an gemeinnützige Organisationen

Ich hatte in meinem Jahresbericht darauf hingewiesen, daß derzeit gemeinnützige Organisationen im Rahmen der Zuweisung von Geldauflagen aus Strafverfahren nicht nur die Höhe der Geldbuße, sondern auch den Namen des Zahlungspflichtigen, die Kontonummer und das gerichtliche Aktenzeichen erfahren. Ich sehe keine Notwendigkeit, die Empfänger von Geldbußen über die Identität des Schuldners zu informieren. Der Zahlungspflichtige könnte den fälligen Betrag an die Justizkasse bzw. Landeshauptkasse entrichten, diese

könnte wiederum unmittelbar oder in regelmäßigen Abständen die eingegangenen Zahlungen an die Adressaten weiterreichen.

Der Senator für Justiz und Verfassung verwies auf verwaltungspraktische Einwände des Generalstaatsanwalts und des Präsidenten des Oberlandesgerichts. Auch die anderen Bundesländer hätten die Auffassung vertreten, daß der Mehraufwand zu groß sei. Deshalb sei vorgesehen, in die Strafprozeßordnung (StVÄG 1994, s.u. Ziff. 10.1.) eine Rechtsgrundlage für solche Mitteilungen an die gemeinnützigen Einrichtungen aufzunehmen.

Ich habe dem Datenschutzausschuß verdeutlicht, daß der Mehraufwand im Verhältnis zum Risiko und zu den Auswirkungen der Streuung von Daten aus Tausenden von Bußgeldverfahren zu beurteilen ist. Der Ausschuß forderte den Senator für Justiz und Verfassung auf, eine nochmalige Überprüfung des derzeitigen Verfahrens vorzunehmen, um sicherzustellen, daß nicht in unverhältnismäßiger Weise in die Persönlichkeitsrechte der Betroffenen eingegriffen wird.

Zu 16. JB, Ziff. 7.1. Forschungsprojekte in Schulen

Der Ausschuß nahm Kenntnis vom Stand der Vorarbeiten für ein Merkblatt zum Datenschutz bei Erhebungen und Untersuhungen an Schulen und der Abstimmung dazu zwischen der Bildungsbehörde und meiner Dienststelle. Dieses Merkblatt sowie eine Checkliste für Datenschutzanforderungen an Personen und Institutionen, die Befragungen an Schulen planen und durchführen, sind inzwischen fertiggestellt (vgl. dazu Ziff. 11.2).

Zu 16. JB, Ziff. 8.3.1 Chipkarten für "gläserne Patienten"

Im Berichtsbeitrag hatte ich vor allem auf die Risiken von Gesundheitskarten in der technischen Form von Chipkarten hingewiesen, die in Speicherumfang (z.B. Diagnosen, Befunde) und Auswertungsmöglichkeiten weit über die zum 1.1o.1994 auch in Bremen eingeführte Krankenversichertenkarte (KVK) hinausgehen. In den Ausschußberatungen erklärte der Staatsrat der senatorischen Behörde für Arbeit und Frauen, sein Ressort lehne Forderungen nach weitergehenden Anwendungen von Chipkarten über die derzeit verwandte KVK hinaus ab. Die neueren Entwicklungen zu Planung und Einsatz von Kartensystemen im Gesundheitswesen werden in diesem Jahresbericht ausführlich dargestellt (vgl. Ziff. 13.1.1).

Zu 16. JB, Ziff. 8.4.1.3 ZKH Bremen-Nord

Kernpunkt meiner Kritik war die hohe Zahl an Eigenprogrammierungen, die in der Regel schlechter dokumentiert und schwerer kontrollierbar sind als Standardsoftware. Der Ausschuß ließ sich von beiden Seiten den Sachstand zu den zahlreichen von mir monierten Mängeln vortragen. Ich habe im Ausschuß weitere Prüfungen angekündigt und 1994 auch durchgeführt, kann und werde mich aber, falls erforderlich, erst im 18. Jahresbericht nach Abschluß aller Nachkontrollen und -gespräche äußern.

Zu 16. JB, Ziff. 8.6.3 Schutz des Beratungsgeheimnisses inerhalb des Amtes für soziale Dienste

Bei diesem Dauerthema ging und geht es im Kern nach wie vor um die Frage, welche Daten die Sozialarbeiter an die Mitarbeiter der wirtschaftlichen Jugendhilfe weitergeben dürfen, ohne das in § 36 KJHG verankerte "Beratungsgeheimnis" zu verletzen. Mit den Ausführungen zu Ziff. 12.3.6. in diesem Jahresbericht erfülle ich meine im Ausschuß gegebene Zusage, die Ergebnisse meiner Aktenprüfungen vor Ort sowie der Gespräche mit dem Jugendressort aktualisiert zu dokumentieren.

Zu 16. JB, Ziff. 8.6.4 Raumnot und Sozialgeheimnis

Im Ausschuß wurde über eine Zusage des Leiters des Ortsamtes Osterholz berichtet, im Laufe des Jahres 1995 könnten durch innerorganisatorsiche und bauliche Maßnahmen die räumlichen Voraussetzungen geschaffen werden, um die Verstöße gegen das Sozialgeheimnis zu verhindern, die sich aus mehreren gleichzeitigen Klientengesprächen in einem

Raum ergeben. Der Sozialsenator erklärte, man sei auch für das Amt in der Wilhelm-Leuschner-Straße bemüht, ausreichend Räumlichkeiten zu finden.

Zu 16. JB, Ziff. 8.7.1 Mitarbeiter- und Klientenlisten

Der Sozialsenator berichtete dem Ausschuß, der von Kindertagesheimen für ihre Mitarbeiter auszufüllende Fragebogen werde ab 1.2.1995 nur noch ohne die von mir monierten Personalien (Name, Geburtsdatum) verwendet (vgl. Ziff. 8.7.1.1). Ein weiterer von mir dokumentierter Problemfall, der die Weitergabe von Namenslisten an die Sozialbehörden zur Durchführung des Betreuungsgesetzes betrifft (vgl. 8.7.1.2, 1. Anstrich), konnte inzwischen datenschutzgerecht gelöst werden (vgl. in diesem Bericht Ziff. 12.3.2). Meine Forderung nach Anonymisierung der Teilnehmerkontrolle bei einem Berufsberatungsprojekt für ausländische Frauen, das aus Mitteln des Europäischen Sozialfonds bezuschußt wird, ist dagegen zwar im Einzelfall akzeptiert worden. Eine entsprechende generelle und bundesweite Handhabung durch das Bundesministerium für Arbeit und Sozialordnung ist dagegen noch nicht endgültig gesichert. Der neueste Stand ist in diesem Bericht unter Ziff. 13.3. wiedergegeben.

Zu 16. JB, Ziff. 10.2 Religionsmerkmale auf der Lohnsteuerkarte

Hierzu hat der Finanzsenator Anfang 1995 mitgeteilt, daß in Bremen bereits für 1995 die Lohnsteuerkarten so ausgestellt worden sind, daß nur noch bei konfessionsverschiedenen Ehepartnern die Konfessionszugehörigkeit vermerkt wird.

3. Bürgerberatung, Medienkontakte, Fort- und Weiterbildung

3.1. Eingaben, Beschwerden und Hinweise - der Datenschutzbeauftragte als Ombudsmann

3.1.1. Verwaltung

Die Anzahl der Bürger, die sich an mich wenden, ist ein guter Gradmesser für das Interesse in der Bevölkerung an Datenschutzfragen des alltäglichen Umgangs mit Behörden und Betrieben. Aus Gründen der Arbeitsökonomie führe ich keine Gesamtbilanz aller Informations- und Beratungskontakte. Wie im Vorjahr ist daher die Vielzahl telefonischer Anfragen, Hinweise und Auskunftswünsche ebensowenig registriert wie die vielen Einzelgespräche anläßlich von Tagungen und Fortbildungsveranstaltungen. Erfaßt sind lediglich die schriftlichen Eingaben: Von Anfang März 1994 bis Ende Januar 1995 gingen 73 Schreiben mit auf die bremische Verwaltung oder andere Behörden bezogenen Beschwerden, Bitten um Rechtsauskunft usw. ein. Vorrangig ging es dabei wie im vorigen Berichtsjahr um die Bereiche Polizei bzw. Ordnungsverwaltung einerseits und Soziales bzw. Gesundheit andererseits.

3.1.2. Privatwirtschaft

In meiner Funktion als Aufsichtsbehörde für den Datenschutz in der Privatwirtschaft haben mich im gleichen Zeitraum 66 Bürgerinnen und Bürger angeschrieben. Ein Viertel der Briefe bezog sich auf Auskunfteien und Kreditinformationssysteme, ein weiteres Viertel auf den Sektor Banken und Versicherungen. Ausgewählte Fälle und Problemstellungen aus der Überwachungstätigkeit im nicht-öffentlichen Bereich sind in Kapitel 17. dieses Berichts dargestellt.

3.2. Presse- und Öffentlichkeitsarbeit

Schwerpunkt meiner Medienarbeit im Berichtsjahr war das Thema Krankenversicherungskarte. Anläßlich ihrer Einführung in Bremen zum 1. Oktober 1994 habe ich die Landespressekonferenz sowie die Öffentlichkeit u.a. über Rundfunkinterviews über meine Einschätzung der Risiken und Konsequenzen (vgl. dazu ausführl. 16. JB, Ziff. 8.3.1.) informiert. Erstmals habe ich auch - getrennt in Bremen und Bremerhaven - eine Telefonaktion durchgeführt, und zwar jeweils am Freitagnachmittag bis 18 Uhr, um auch Berufstätigen nach Büroschluß bzw. nach Arbeitsende Gelegenheit zu Datenschutzfragen zur

Krankenversichertenkarte zu geben. Das Thema wird in diesem Bericht erneut aufgegriffen (vgl. u. Ziff. 13.1.1).

Auch die Titelgeschichte des SPIEGEL Nr. 47/94 über den "Chip-Bürger", die zusammenfassend Trends in der Entwicklung und Nutzung von Chip-Karten in den verschiedensten gesellschaftlichen Anwendungsfeldern dargestellt und problematisiert hat, hat meine im letzten Jahresbericht geäußerten kritischen Überlegungen zu den Risiken dieser Technik aufgegriffen. Anfang Januar 1995 konzentrierte sich das Medieninteresse auch in Bremen auf Überlegungen einer Bund-Länder-Arbeitsgruppe, für Asylbewerber obligatorisch eine "Asyl-Card" ebenfalls in der technischen Form einer Chipkarte einzuführen (vgl. in diesem Bericht Ziff. 9.2.4.)

In weiteren Presseerklärungen habe ich u.a. das Ausländerzentralregistergesetz kritisiert ("Kontrolle statt Gastfreundschaft", vgl. dazu in diesem Bericht Ziff. 9.2.1) und - in den folgenden Fällen gemeinsam mit der Mehrzahl meiner Kollegen - erhebliche Bedenken geäußert gegen das inzwischen in Kraft getretene Verbrechensbekämpfungsgesetz ("Strafverfolgung durch Geheimdienst"; vgl. u. Ziff. 9.1.1) sowie den bisher zunächst nur vom Bundesrat verabschiedeten Entwurf für ein Strafverfahrensänderungsgesetz ("Datenschutz für Strafakten in Gefahr"; dazu u. Ziff. 10.1).

Weitere meiner Stellungnahmen gegenüber Print- und Funkmedien betrafen die Themen

- Gentests bei Vorsorgeuntersuchungen als Gefahr der sozialen Selektion im Zusammenhang mit dem seinerzeit geplanten Arbeitsschutzrahmengesetz,
- die - in diesem Punkt gescheiterte - Novellierung des Sozialgesetzbuchs mit dem Ziel, Sozialbehörden auch zu Auskünften über Klientenbesuche an die Polizei zu verpflichten,
- den "Etikettenschwindel" bei der unzulänglichen Umsetzung der einschlägigen EG-Richtlinie durch das Umweltakteneinsichtsgesetz des Bundes,
- die Sicherung des Arztgeheimnisses bei gleichzeitiger Behandlung mehrerer Patienten,
- die mangelnde Einhaltung des Sozialgeheimnisses bei der Raumknappheit in Ortsämtern.

Zu den Publikationen: Eine zusammen mit meinen Kollegen aus Hamburg und Berlin erarbeitete Broschüre zum "Datenschutz beim Mobilfunk" ist im Januar 1995 erschienen und kann bei mir bestellt werden.. Sie soll jetzt breit gestreut werden an Hersteller, Anwender, Fachpublikationen und nicht zuletzt an interessierte Käufer und Nutzer von mobilen Geräten. Zum novellierten Bremischen Datenschutzgesetz (vgl. u. Kapitel 4) werde ich, falls es noch in der laufenden Wahlperiode zur Verabschiedung kommt, bis zum Sommer ein Informationsheft mit dem dann neu gefaßten Gesetzestext sowie den wichtigsten Änderungen vorlegen und an Bürger wie Verwaltungsmitarbeiter zur Verteilung bringen.

3.3. Aus- und Fortbildung, Vortrags- und Lehrtätigkeit

Nur wer seine Rechte und Pflichten nach dem Datenschutzrecht kennt, kann sie voll ausschöpfen bzw. einhalten. Ohne zureichende Information darüber, wann und wie die Persönlichkeitsrechte der Bürgerinnen und Bürger zu schützen sind, kann kein Datenschutzbewußtsein entstehen; Datenschutz bleibt im gesellschaftlichen Alltag dann Makulatur. Meine Mitarbeiter und ich engagieren uns daher - im allerdings beschränkten Rahmen der für diesen Bereich verfügbaren Kapazitäten - in zahlreichen Aus-, Fort- und Weiterbildungsaktivitäten.

Auf die Zielgruppe der künftigen technischen Elite gerichtet sind die in den drei Semestern des Berichtszeitraums abgehaltenen Kurse an der Universität Bremen im Informatik-Grundstudium ("Datenschutz und Datensicherung" im Rahmen der Veranstaltung "Informatik und Gesellschaft") und an der Hochschule Bremerhaven im Studiengang Systemanalyse.

Das durch Mitarbeiter meines Amtes durchgeführte Lehrangebot zur Weiterqualifizierung von Mitarbeiterinnen und Mitarbeitern des bremischen öffentlichen Dienstes umfaßte u.a. zwei Lehrgänge für Sachbearbeiter in den Sozialämtern, vier Vorträge auf Schulleiterversammlungen und zwei Workshops für Personalräte. Hinzu kommt der traditionelle, viertägige allgemeine Lehrgang am AFZ zur Einführung in das Datenschutzrecht.

Referate auf Fachtagungen zielen ab auf ein themenspezifisch interessiertes Publikum. Vorträge bzw. Statements von mir und meinen Mitarbeitern auf verschiedenen derartigen Veranstaltungen betrafen u.a. die Themen

- Datenschutz in Europa,
- Mailboxen und Datenschutz,
- Der "gläserne Fremde" - Datenschutzrechte der Nichtdeutschen,
- "Gläserne Klienten" - Datenschutz und inter-institutionelle Zusammenarbeit.

4. Die Novellierung des Bremischen Datenschutzgesetzes

4.1. Regelungsziele und Gang der Beratungen

Die Novellierung des Bremischen Datenschutzgesetzes (BrDSG) in der Fassung der Bekanntmachung vom 14. Oktober 1987 (vgl. dazu 16. JB, Ziff. 1.2) konnte im Berichtszeitraum noch nicht abgeschlossen werden. Zwar hat der Datenschutzausschuß der Bürgerschaft in 12 Sitzungen die Neufassung gründlich beraten und am 2. Februar 1995 seinen Bericht an das Plenum vorgelegt (vgl. Bürgerschafts-Drucks. 13/1139 vom 07.02.95). Wegen gleichsam in letzter Sekunde aufgeworfener Fragen zum Anwendungsbereich des Gesetzes wurde die erste Lesung am 23. Februar 1995 jedoch unterbrochen und der Entwurf an den Verfassungs- und Geschäftsordnungsausschuß (federführend) sowie noch einmal an den Datenschutzausschuß überwiesen.

Ich hoffe dringend, daß diese Verzögerung wegen eines Detailpunkts nicht zum Scheitern des gesamten Novellierungsprojekts führt, sondern daß der Entwurf trotz des Zeitdrucks wegen der Verkürzung der Wahlperiode noch vor der Bürgerschaftsneuwahl verabschiedet werden kann. Trotz dieser Unsicherheit halte ich es für angemessen, in diesem Bericht ausführlich über die vorgesehenen Änderungen (zitiert als BrDSG-E) zu berichten.

Ausgangspunkt für den vom Senat am 17. Mai 1994 verabschiedeten Entwurf war der in Abschnitt V.5. der Koalitionsvereinbarung für die 13. Wahlperiode enthaltene Auftrag, das BrDSG zum einen dem 1990 neugefaßten Bundesdatenschutzgesetz (BDSG) anzupassen, zum anderen die Rechtsstellung des Bürgers sowie die Befugnisse und den Status des Landesbeauftragten für den Datenschutz zu verbessern. Die Koalitionsvereinbarung wiederum beruhte zu maßgeblichen Teilen auf Änderungsanträgen der Fraktionen von F.D.P. und GRÜNEN aus der letzten Legislaturperiode (vgl. Bürgerschaftsdrucks. 12/931 und 12/967), die damals von der Bürgerschaftsmehrheit abgelehnt worden waren (vgl. Bericht des Datenschutzausschusses vom 04.12.1990, Bürgerschaftsdrucks. 12 / 1086). Ich selbst hatte dem Justizsenator im Frühjahr 1993 ein umfangreiches Paket mit weiteren Verbesserungsvorschlägen zugeleitet, von denen er eine Reihe in den Senatsentwurf übernommen hat. Die nicht berücksichtigten Anregungen habe ich in den Ausschußberatungen weiterverfolgt. Im folgenden werden nur die wichtigsten im Ausschuß verabschiedeten Neuerungen vorgestellt; eher redaktionelle Korrekturen bleiben unerwähnt.

4.2. Mehr Rechte für den Einzelnen

4.2.1. Schadensersatzanspruch

Wichtigste Neuerung bei den Individualrechten ist die Einführung eines sog. "verschuldensunabhängigen Schadensersatzanspruchs" (vgl. § 5 BrDSG-E): Bürger, die durch eine unzulässige oder unrichtige automatisierte Verarbeitung ihrer Daten einen Schaden erleiden, haben Anspruch auf Schadensersatz, ohne daß sie der verantwortlichen Behörde ein konkretes Verschulden nachweisen müssen. Vorbild für diese Regelung waren entspre-

chende Normen im BDSG (§ 7) sowie in neueren Landesdatenschutzgesetzen. Der zentrale Unterschied zu den traditionellen Amtshaftungsansprüchen, die schuldhaftes Verhalten einer Behörde bzw. ihrer Mitarbeiter voraussetzen, hat allerdings in der bisherigen Haftungspraxis für fehlerhafte Datenverarbeitung noch kaum eine Rolle gespielt.

4.2.2. Auskunftsanspruch bei Verbunddateien

Bürgerfreundlicher werden soll auch die Handhabung bei sog. Verbunddateien, in die mehrere Behörden Daten eingeben. Für den Außenstehenden ist vielfach nicht erkennbar, welche der einspeichernden Stellen im datenschutzrechtlichen Sinne verantwortlich und damit für die Ansprüche auf Auskunft, Berichtigung und Löschung zuständig ist. § 4 Abs. 2 BrDSG-E stellt nunmehr klar, daß der Betroffene sich mit seinem Begehren an jede der dateneingebenden Behörden wenden kann. Ist diese selbst für die Rechtmäßigkeit der Datenverarbeitung nicht zuständig, hat sie den Antrag des Bürgers an die verantwortliche Stelle weiterzugeben und den Antragsteller davon zu informieren (Parallelregelung in § 6 Abs. 2 Satz 1 und 2 BDSG).

4.2.3. Erweiterung von Auskunftsanspruch und Akteneinsichtsrecht

Korrekturen im Interesse des Einzelnen wurden auch bei seinen Informationsrechten vorgenommen: Sein kostenfreies (§ 4 Abs. 1 Satz 2 BrDSG-E) Auskunftsrecht erstreckt der Entwurf auch auf die Personen und Stellen, an die seine persönlichen Daten weitergegeben worden sind, damit er auch dort ggf. seine Berichtigungs- oder Löschungsansprüche anbringen kann (§ 19 Abs. 1 Satz 1 Nr. 3 BrDSG).

Die vielleicht wichtigste Änderung: Auskunftsrecht und Recht auf Akteneinsicht stehen nach dem Ausschußentwurf dem Einzelnen ausdrücklich "wahlweise" zu. Nicht die Behörde, sondern der Betroffene selbst kann mithin entscheiden, ob er mit Informationen aus den Verwaltungsunterlagen zufrieden ist oder es vorzieht, selbst in die behördlichen Vorgänge einzusehen, um sich von Art und Umfang der Aufzeichnung und Nutzung seiner Daten zu überzeugen. Hinzu kommt noch, daß der Bürger nicht mehr auf den bloßen Augenschein beschränkt bleibt; die Neufassung stellt vielmehr klar, daß er sich auch Auszüge, Abschriften und Kopien fertigen (lassen) kann (§ 19 Abs. 1 Sätze 4 und 6 BrDSG-E). Staatsanwaltschaft, Polizei, Verfassungsschutz und Steuerfahndung sind nicht mehr wie bisher pauschal von der Auskunftspflicht gegenüber dem Betroffenen ausgenommen. Wollen sie die Auskunft oder die Akteneinsicht etwa aus Gründen der öffentlichen Sicherheit verweigern, müssen sie dies wie alle anderen Dienststellen auch begründen.

4.2.4. Eingaben von Mitarbeitern der Verwaltung

Für die bremischen Bediensteten wurde eine bisher lediglich in den Allgemeinen Verwaltungsvorschriften zum BrDSG enthaltene Regelung in Gesetzesrang erhoben, wonach sie bei Eingaben beim Landesbeauftragten, die sich auf ihre eigenen Daten beziehen, den Dienstweg nicht einzuhalten brauchen (§ 30 Satz 2 BrDSG-E). Nach wie vor können sie sich aber wegen möglicher Datenschutzverstöße auch dann direkt an meine Dienststelle wenden, wenn diese nicht ihre eigene Person, sondern den Dienstbetrieb betreffen; insoweit bleibt es wie bisher beim Maßregelungs- und Benachteiligungsverbot (§ 30 Satz 3, bisher Satz 2).

4.3. Korrekturen beim Anwendungsbereich

4.3.1. Bürgerschaft und Gerichte

Nicht geändert, sondern lediglich klargestellt werden soll die Reichweite des Landesdatenschutzgesetzes in bezug auf die Bürgerschaft (Landtag): Sie unterliegt aufgrund ihrer verfassungsrechtlichen Stellung als Legislative dem BrDSG wie bisher nur bei der Datenverarbeitung für Verwaltungsangelegenheiten, also etwa bei der Verarbeitung von Mitarbeiterdaten (§ 1 Abs. 3 BrDSG-E), nicht aber beim Umgang mit Personendaten zu parlamentarischen Zwecken.

Für die Datenverarbeitung der Gerichte gilt das Landesdatenschutzgesetz (BrDSG) nach wie vor nur außerhalb ihrer durch die Verfassung als unabhängig garantierten richterli-

chen Tätigkeit, also bei der Erledigung von Verwaltungsaufgaben. Allerdings übernimmt § 1 Abs. 4 Satz 1, 2. Halbsatz BrDSG-E ausdrücklich die im neuen BDSG enthaltene Regelung, daß die Justiz auch bei ihrer richterlichen Tätigkeit das Datenschutzgesetz des Bundes zu beachten hat, soweit die Prozeßordnungen keine abweichenden Vorgaben machen. Eine Kontrollkompetenz des Landesbeauftragten besteht allerdings insoweit nur für die technischen und organisatorischen Maßnahmen der Datensicherung (§ 27 Abs. 1 Satz 2 BrDSG-E).

4.3.2. Verwaltung durch Private

Als Reaktion auf die zunehmende Privatisierung traditioneller Administrationsaufgaben auch in Bremen stellt § 2 Satz 2 des Entwurfs klar, daß alle Personen oder Unternehmen, die zwar außerhalb des öffentlichen Dienstes stehen, aber Aufgaben der öffentlichen Verwaltung wahrnehmen, an die gegenüber dem BDSG strengeren Bestimmungen des BrDSG gebunden bleiben. Anders ausgedrückt: Für materielle Verwaltungstätigkeit gilt einheitlich das Landesdatenschutzgesetz, gleich ob sie durch Behörden oder durch Privatunternehmen ausgeübt wird. Dabei ist dieses Prinzip nicht auf die im engeren Sinne hoheitliche Verwaltung ("Beliehene") beschränkt.

4.4. Entbürokratisierung

Die Novellierung des BrDSG ist eine eine auch von mir begrüßte Gelegenheit, das in Bremen sehr dichte Regelwerk zum Datenschutz ein wenig zu entschlacken und unverhältnismäßigen Verwaltungsaufwand zu beschneiden.

4.4.1. Verwaltungsvorschriften nur fakultativ

So wird im Entwurf die Pflicht des Senats abgeschafft, zur Gesetzesdurchführung allgemeine Verwaltungsvorschriften (AVV) zu erlassen (bisher § 9). Die bisher gültigen AVV vom 18. Juli 1989 (BremABl. S. 379) gelten jedoch weiter, soweit die Novellierung oder zwischenzeitliche Änderungen in anderen Bundes- oder Landesgesetzen die Rechtslage nicht verändert haben, da das BrDSG ja nicht neu erlassen wird, sondern lediglich das bestehende Gesetz vom 14.10.87 modifiziert wird.

4.4.2. Abschaffung des Dateienregisters

Abgeschafft werden soll auch das bei meiner Dienststelle bisher geführte Dateienregister (bisher § 28). Keine Behörde muß künftig dann noch von ihr eingerichtete bzw. betriebene Dateien bei mir melden. Der Melde-, Betriebs- und Aktualisierungsaufwand stand in keinem Verhältnis mehr sowohl zum Einsichtsinteresse des Publikums als auch zum Informationsertrag für meine Prüftätigkeit. Es bleibt aber bei der Pflicht jeder Dienststelle, alle personenbezogenen Dateien zu beschreiben und diese Dateibeschreibungen - auch zur Transparenz der eigenen DV-Struktur - vorzuhalten. Auf Anforderung sind sie dem Landesbeauftragten vorzulegen (§ 8 Abs. 5 BrDSG-E). Zur Vorbereitung konkreter Prüfungen brauche ich also zwar kein flächendeckendes Register; ich kann und will aber auch weiterhin auf eine behördenbezogene Dateienübersicht zugreifen können.

4.5. Status und Befugnisse des Landesbeauftragten für den Datenschutz (LfD)

Im Dritten Abschnitt des BrDSG verbessert der Ausschußentwurf die Rechtsstellung des LfD in mehreren Punkten.

4.5.1. Wahl und Unterrichtungsrechte

Zunächst wurde seine parlamentarische Legitimation erhöht: Zur Wahl des Landesbeauftragten schreibt der Entwurf die Mehrheit der Mitglieder der Bürgerschaft, also die qualifizierte Mehrheit vor; bisher genügte die einfache Majorität der am Wahltag anwesenden Abgeordneten. Weitergehende Überlegungen, sogar eine Zwei-Drittel-Mehrheit zu verlangen, wurden nicht realisiert.

Um den präventiven Datenschutz zu stärken, also die frühzeitige technische wie juristische Beratung der bremischen Behörden in Datenschutzfragen sicherzustellen, sieht der

neugefaßte § 27 Abs. 4 jetzt vor, daß der LfD nicht nur wie bisher rechtzeitig über geplante ADV- Systeme zu unterrichten ist, sondern auch über Entwürfe der Ressorts für datenschutzrelevante Rechts- und Verwaltungsvorschriften.

4.5.2. Kontrollbefugnisse

Beim Rechnungshof beschränkt der Ausschußtext die Kontrollbefugnis ebenso wie bei den Gerichten auf die Datenverarbeitung in Verwaltungsangelegenheiten. Unbeschadet der verfassungsrechtlich gewährleisteten Unabhängigkeit beider Institutionen kann der Landesbeauftragte aber auch im Bereich der Rechtsprechung bzw. der Rechnungsprüfung jedenfalls die technischen und organisatorischen Maßnahmen der Datensicherung überprüfen (§ 27 Abs. 1 Satz 2 BrDSG-E).

Ein weiterer wichtiger Punkt: Die sog. "Staatswohlklausel" wird abgeschafft. Nach bisherigem Recht konnte in den Bereichen Polizei und Verfassungsschutz der Innensenator eine Überprüfung durch den LfD dann verhindern, wenn die Datenschutzkontrolle im Einzelfall "die Sicherheit des Bundes oder eines Landes gefährdet". Zwar war diese Klausel in Bremen bisher noch nie angewendet worden, auf der anderen Seite gab es für mich keinen ersichtlichen Grund, eine Kontrollücke aufgrund einer derart vagen Generalklausel bestehen zu lassen, zumal in einem Bereich, in dem der Bürger in besonderer Weise eine wirksame Überwachungsmöglichkeit des Datenschutzbeauftragten erwartet. Der neue § 27 Abs. 3 Satz 4 sieht nur noch einen Schutz der Identität von V- Personen auch gegenüber dem LfD vor; die Unterlagen im übrigen kann ich künftig auch bei Polizei und Verfassungsschutz ohne Verweigerungsmöglichkeit durch den zuständigen Senator vollständig einsehen.

4.5.3. Entscheidungsbefugnis bei der Stellenbesetzung

4.5.3.1. Konsequenz der Unabhängigkeit des LfD

Ich hatte zu § 34 Abs. 2, der die Personal- und Sachausstattung des LfD betrifft,folgenden ergänzenden Satz vorgeschlagen: "Die Stellen (sc. beim LfD) werden im Einvernehmen mit dem Landesbeauftragten für den Datenschutz besetzt." Diese personalrechtliche Mitentscheidungsmöglichkeit findet sich, wie die von mir vorgelegte Synopse belegt hat, in fast allen anderen Landesdatenschutzgesetzen sowie im novellierten Bundesdatenschutzgesetz.

Der Grund dafür ist einfach: Diese Befugnis ist integraler Bestandteil der Unabhängigkeit des Landesbeauftragten für den Datenschutz. Diese Unabhängigkeit ist vom Bundesverfassungsgericht im Volkszählungsurteil als zentrale Voraussetzung für die verfassungsrechtlich gebotene effiziente Datenschutzkontrolle ausdrücklich angesprochen (vgl. BVerfG NJW 1984, 419, 422f.) und in späteren Entscheidungen unterstrichen worden (vgl. BVerfG NJW 1985, 121, 125). Sie ist auch in § 25 Satz 1 des Bremischen Datenschutzgesetzes (BrDSG) explizit verankert ("Der LfD ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen"). Sie wird u.a. bekräftigt durch § 34 Abs. 2 BrDSG, wonach die Personal- und Sachausstattung des LfD in einem eigenen Haushaltskapitel auszuweisen ist.

Bei diesem Ergänzungsvorschlag zu § 34 Abs. 2 betr. das Einvernehmen bei der Besetzung der in der Dienststelle des LfD angesiedelten Stellen ging es mit anderen Worten darum, sicherzustellen, daß dort nur Personen arbeiten, die das Vertrauen des vom Parlament gewählten Datenschutzbeauftragten genießen. Mit der verfassungsrechtlich fundierten (s.o.) und im BrDSG verankerten Unabhängigkeit des LfD ist es schwer vereinbar, daß ihm möglicherweise gegen seinen Willen Mitarbeiter zugewiesen werden können; § 34 Abs. 1 BrDSG unterstreicht den Bezug des zur Verfügung gestellten Personals zur Erfüllung "seiner" - also des LfD - Aufgaben.

4.5.3.2. Widerspruch zur Personalhoheit des Senats ?

Auf dieses Ergebnis kam es mir an, nicht auf die Begrifflichkeit, insbesondere nicht um die in Art. 118 Abs. 2 LV genannten und dem Senat vorbehaltenen dienstrechtlichen Akte der Einstellung oder Entlassung. Deshalb habe ich entsprechend den Regelungen in meh-

reren anderen Landesdatenschutzgesetzen den dienstrechtlich untechnischen Begriff der Stellen"besetzung" vorgeschlagen, wäre aber auch mit anderen Termini, die zu dem o.a. Resultat führen, einverstanden gewesen, also etwa mit der Formulierung "Zuweisung des Personals".

Nach der mich nach wie vor nicht überzeugenden Argumentation des Justizsenators soll es hier wegen der nach der Landesverfassung ausschließlich dem Senat vorbehaltenen Personalhoheit (s.o.) überhaupt keinen Regelungsspielraum geben. Der Datenschutzausschuß wiederum konnte bzw. wollte diese verfassungs- und personalrechtliche Frage nicht entscheiden. Als Kompromiß wurde im Entwurf statt des Einvernehmens das schwächere "Benehmen" mit dem Landesbeauftragten zur Voraussetzung für die Stellenbesetzung gemacht. Dies wäre zweifellos gegenüber der derzeitigen Gesetzesfassung ein gewisser Fortschritt, doch bleibt bei dieser Rechtslage das theoretische Risiko einer Personalpolitik am LfD vorbei und damit einer Gefährdung seiner Aufgabenerfüllung im Fall des Konflikts mit dem Senat; und nur für diese Situation spielt die Regelung eine Rolle.

4.5.4. Rederecht in der Bürgerschaft

Wie in der Koalitionsvereinbarung festgelegt enthielt der Senatsentwurf eine Ergänzung des § 33 BrDSG, wonach der Landesbeauftragte "befugt" sein sollte, in der Aussprache der Bürgerschaft über seinen Jahresbericht und die zugehörige Stellungnahme des Senats "das Wort zu ergreifen". Damit wurden wiederum Regelungsvorschläge aus der vergangenen Wahlperiode von FDP und GRÜNEN aufgegriffen.

Dieses Rederecht trägt der besonderen Stellung des Landesbeauftragten als vom Parlament gewählten und diesem insgesamt (nicht nur dem Datenschutzausschuß) gegenüber rechenschafts- und berichtspflichtigen Amtsträger Rechnung. Mit einer ausdrücklichen gesetzlichen Regelung der Möglichkeit des Landesbeauftragten, seinen Bericht in den Schwerpunkten auch mündlich im Plenum vorzustellen, wird außerdem die Information der Bürgerschaft in einem wichtigen, bürgernahen Teilbereich ihrer Zuständigkeit verbessert. Hinzu kommt, daß der Landesbeauftragte nur schwerlich gleichgesetzt werden kann mit den in § 28 Geschäftsordnung der Bürgerschaft genannten "Sachverständigen", die zu Beratungen der Bürgerschaft hinzugezogen werden können.

Gegen die Fassung des Senats hatte ich daher keine Einwände. Da aber von Mitgliedern des Datenschutzausschusses Bedenken wegen einer möglichen Präzedenzwirkung bzw. wegen der Gefahr der Funktionalisierung des Landesbeauftragten in der politischen Auseinandersetzung geäußert wurden, hatte ich als Alternativformulierung vorgeschlagen, die auch in die Ausschußfassung aufgenommen geworden ist:

"In der Aussprache über den Bericht kann die Bürgerschaft dem Landesbeauftragten für den Datenschutz Gelegenheit zur Vorstellung dieses Berichts geben."

Damit wird dem LfD kein eigenständiges Rederecht in dem Sinne eingeräumt, daß er es wahrnehmen kann, aber nicht muß. Vielmehr bleibt es bei dem auch in § 28 der Geschäftsordnung der Bürgerschaft zum Ausdruck kommenden Prinzip, daß die Bürgerschaft über die Hinzuziehung externer Redner autonom entscheidet. Politischer Begründungszwang kann allerdings dann eintreten, wenn die Mehrheit der Bürgerschaft die Vorstellung des Berichts vor dem Plenum verweigert, obwohl eine Minderheit der Abgeordneten diese mündliche Präsentation wünscht.

Hinzu kommt, daß es in der Vergangenheit wiederholt den Wunsch gab, eine Aussprache bereits unmittelbar nach der Vorlage des Berichts durch den LfD zu führen, also bevor der Senat einige Monate später seine Stellungnahme abgegeben hat. Deshalb wurden gegenüber Satz 1 des Senatsentwurfs die Worte "und die Stellungnahme des Senats" gestrichen. Die Bürgerschaft bindet sich m.a.W. nicht hinsichtlich des Zeitpunkts der Aussprache über den Bericht und damit die Zuziehung des LfD: Sie kann sowohl schon bei der Vorlage des Jahresberichts als auch erst nach dem Ende der Ausschußberatungen, d.h. in der Aussprache zum Ausschußbericht, erfolgen.

4.6. Bürgerschaft: Auskunftsrecht und Datenschutzausschuß

Erstmals enthält der BrDSG-E eine Regelung des Verhältnisses von Schutz persönlicher Daten einerseits und parlamentarischen Kontroll- und Auskunftsrechten andererseits, eine Frage, die wiederholt zu teils grundsätzlichen, teils praktischen Problemen bei der Beantwortung parlamentarischer Anfragen geführt hat. Um diese beiden sich auf Verfassungsebene gegenüberstehenden Rechtspositionen zu wahren, habe ich im Fall einer Kleinen Anfrage zu Personen und Konditionen der Vermietung städtischer Liegenschaften empfohlen, in der veröffentlichten Drucksache keine personenbezogenen Mieterdaten aufzunehmen, sondern die umfassenden Unterlagen bei der Verwaltung der Bürgerschaft zur Einsicht für die Abgeordneten bereitzuhalten. Lt. Bürgerschafts-Drucks. 13/930 ist auch so verfahren worden.

Zur Durchführung der parlamentarischen Kontrolle des Datenschutzes hat die Bürgerschaft den Datenschutzausschuß gebildet. Dessen Aufgaben waren ausdrücklich bisher nicht im Gesetz festgelegt. § 35 Satz 2 BrDSG-E erwähnt jetzt explizit die Beratung der Jahres- und Zwischenberichte des LfD. Bedeutsam ist aber vor allem die Neuerung, daß der Datenschutzausschuß auch den speziellen Teilhaushalt des LfD (mit)berät, der bisher aufgrund der "Deputationsfreiheit" des LfD nur dem Haushaltsausschuß der Finanzdeputation vorlag. Dies stärkt sowohl die Kontrolle des Ausschusses über das Finanzgebaren des LfD als auch umgekehrt den LfD bei der Unterstützung seiner Haushaltsanliegen.

4.7. Entscheidungsbefugnis über Aussage und Aktenvorlage in gerichtlichen Verfahren

4.7.1. Element der Unabhängigkeit

Von den aus meiner Sicht nicht befriedigenden Ergebnissen greife ich nur die Auseinandersetzung um eine Ergänzung des § 26 BrDSG über die Verschwiegenheitspflicht des LfD heraus. heraus. Ein entscheidendes Element der Unabhängigkeit des Datenschutzbeauftragten (s.o. 4.5.3.1) stellt es auch dar, daß er ausschließlich selbst darüber entscheiden kann, ob Informationen und Vorgänge, die er in Ausübung seines Amtes von Bürgern und Verwaltungsmitarbeitern erfahren hat, in jedem Falle vertraulich bleiben können oder aber auch gegen seinen Willen in Ermittlungsverfahren und Gerichtsprozessen offenbart werden müssen.

§ 24 Abs. 4 in Verbindung mit § 12 Abs. 3 BDSG 1990 gibt den Landesbeauftragten für den Datenschutz und deren Mitarbeitern ein bundesrechtliches Zeugnisverweigerungsrecht über die Personen, die ihnen in ihrer Eigenschaft als Datenschutzbeauftragter Tatsachen anvertraut haben, und über diese Tatsachen selbst. Im Umfang dieses Rechts besteht auch ein Recht auf Verweigerung von Aktenvorlagen.

Da diese Rechte aber nicht alle Konstellationen abdecken, in denen es auf die strikte Abschottung der Kenntnisse des LfD ankommt, hatte ich entsprechend der Rechtslage in fast allen anderen Landesdatenschutzgesetzen ebenso wie im BDSG 1990 den früheren Textvorschlag von FDP und GRÜNEN aufgegriffen, wonach generell der Landesbeauftragte ebenso allein über die Aushändigung seiner Akten an Staatsanwaltschaften oder Straf- und Verwaltungsgerichte befinden kann wie über die Erteilung von Aussagenehmigungen für sich und seine Bediensteten. Diese Regelung war bereits in den Änderungsanträgen von FDP und GRÜNEN in der letzten Wahlperiode enthalten.

4.7.2. Besondere Rechtsstellung des Landesbeauftragten

SKP und Justizsenator haben in ihrer Stellungnahme gegenüber dem Datenschutzausschuß eine solche Regelung - wie bereits in der vergangenen Legislaturperiode - abgelehnt. Hauptargument war dabei die Berufung auf höchstrichterliche Rechtsprechung, die derartige Entscheidungen nur obersten Dienst- bzw. Landesbehörden vorbehalten habe.

Doch geht diese Argumentation von einer unzutreffenden Parallele aus. Die angeführten Gerichtsentscheidungen beziehen sich auf die Frage, ob und inwieweit nachgeordnete Behörden bzw. untergeordnete Stellen entscheiden können sollen. Das zitierte Urteil des BGH aus dem Jahr 1981 (NJW 1981, S. 1052) behandelt beispielsweise die Frage, ob die

Polizei selbst oder nur der Innenminister über die Preisgabe der Identität von Gewährsmännern befinden darf.

Der LfD ist aber gerade keine nachgeordnete Behörde, er unterliegt keiner Rechts- und Fachaufsicht. Dementsprechend gibt es keine ministerielle Verantwortlichkeit für seine Amtsführung gegenüber dem Parlament; kein Senator kann für Aktivitäten des LfD im Rahmen seiner Aufgaben nach §§ 27 ff. BrDSG von der Bürgerschaft zur Verantwortung gezogen werden. Der LfD steht zwischen Exekutive und Legislative, die ihn gewählt hat und der gegenüber er berichtspflichtig ist. Eine Argumentation, die von einer zwangsläufigen Zuordenbarkeit aller öffentlichen Stellen entweder zur Exekutive oder zur Legislative und von der herkömmlichen Verwaltungshierarchie ausgeht, Vorstellungen, die auch bei der Formulierung der Landesverfassung von 1947 zugrunde lagen, trägt der verfassungsrechtlichen Situation nach dem Volkszählungsurteil nicht ausreichend Rechnung.

Mangels vorgesetzter Behörde mit Rechts- oder Fachaufsicht ist es nur konsequent, daß auch nur der rechtlich und fachlich allein zuständige LfD sachgerecht über eventuelle Hinderungsgründe gegen eine Aussage oder Aktenvorlage entscheiden kann. Mit der vorgeschlagenen Formulierung als Fiktion ("gilt" als oberste Aufsichtsbehörde usw.) wurde klargestellt, daß die Rechtsstellung des LfD im bremischen Behördenaufbau im übrigen nicht verändert werden sollte. So ging es auch nicht darum, im Bereich der Landes- oder Kommunalaufgaben, d.h. im Rahmen der durch die Landesverfassung vorgegebenen bremischen Entscheidungsstruktur bzw. Verwaltungshierarchie allein dem Senat zugewiesene Befugnisse dem LfD "zu übertragen". Vielmehr geht es bei der Anwendung der gerichtlichen Verfahrensordnungen um die Ausführung von Bundesrecht, das es nach meiner Auffassung in den hier in Rede stehenden Fällen der Organisationshoheit der Länder überläßt, welche Stelle konkret als zuständig bezeichnet wird, solange eben keine nach- oder untergeordneten Stellen benannt werden (s.o.).

In meiner Gegenstellungnahme gegenüber dem Datenschutzausschuß hatte ich auch darauf aufmerksam gemacht, daß die vom Senator für Justiz und Verfassung vorgetragenen Belege aus der höchstrichterlichen Rechtsprechung auch in anderen Bundesländern bekannt und geprüft worden sind. Auch dort ist der LfD mit Ausnahme Berlins und von Rheinland-Pfalz institutionell nicht als oberste Landes-, Dienst- oder Aufsichtsbehörde ausgestaltet, gleichwohl haben sich dort die Gesetzgeber fast durchgängig für die autonome Entscheidungsbefugnis des Landesbeauftragten ausgesprochen. Der Datenschutzausschuß konnte sich im Ergebnis jedoch nicht dazu verstehen, die Verschwiegenheitspflicht des LfD wie von mir vorgeschlagen zu erweitern.

4.8. Résümé

Obwohl nicht alle Punkte vom Datenschutzausschuß akzeptiert worden sind, die ich mir insbesondere im Hinblick auf die Absicherung meiner Unabhängigkeit gewünscht hätte, fällt die Gesamtbilanz dieses Gesetzgebungsvorhabens positiv aus. In einer "schlanken" Reform hat man sich auf den wesentlichsten Korrekturbedarf, wie er sich aus der Fortentwicklung von Datenschutzrecht und IuK - Technik seit der letzten Gesetzesänderung von 1987 ergab, konzentriert. Auf der Grundlage eines sorgfältig erarbeiteten Entwurfs des Justizsenators, der eingehenden Beratungen im Datenschutzausschuß und der kooperativen Haltung der Ressorts bei während der parlamentarischen Diskussion aufgetauchten Änderungswünschen wird mit der im Ausschuß verabschiedeten Fassung der Standard der neueren, fortschrittlicheren Landesdatenschutzgesetze in den meisten Punkten erreicht. Zahlreiche Übernahmen gerade von bürgerfreundlichen Regelungen aus dem novellierten BDSG von 1990 in das BrDSG sorgen für mehr Bundeseinheitlichkeit im Datenschutzniveau.

Diese Bewertung unterstreicht die Notwendigkeit, daß das novellierte BrDSG baldmöglichst verabschiedet wird. Dann müssen sich die neuen Regelungen in der Anwendungspraxis bewähren. Ich habe alle Vorbereitungen getroffen, um zur Information von Bürgern und Bediensteten der Behörden nach der Verabschiedung bzw. dem Inkrafttreten eine Broschüre herauszugeben, die die wesentlichsten Änderungen praxisnah erläutert (s.o. 3.2.). Wo sich allerdings herausstellen sollte, daß auch die ggf. neu gefaßten Vorschriften nicht ausreichen, um etwa besonders schutzwürdige Daten zu sichern oder die

Risiken neuer Entwicklungen der IuK-Technik aufzufangen, sind auch in Zukunft bereichsspezifische Regelungen in Einzelgesetzen nicht verzichtbar.

5. Regelungs- und Kontrollprobleme der Informations- und Kommunikationstechnik

5.1. Entwicklungen und Projekte in Bremen

5.1.1. Das TuI-Regelwerk - eine unendliche Geschichte ?

Die bereits im letzten Bericht geschilderten organisatorischen Veränderungen bei der Einführung technikunterstützter Informationsverarbeitung (TuI) in Bremen (vgl. 16. JB., Ziff. 2.3.2.1) sind weiter fortgeschritten. Am 1. Juli 1994 fand die konstituierende Sitzung des TuI-Ausschusses statt. Durch die beratende Mitwirkung im TuI-Ausschuß erhalte ich Informationen über größere geplante TuI-Vorhaben; dies ist notwendig, um meinen gesetzlichen Auftrag erfüllen zu können, zu den Auswirkungen des Einsatzes neuer Informationstechniken auf den Datenschutz Stellung zu nehmen (vgl. § 27 Abs. 4 BrDSG). Der TuI-Ausschuß soll sich grundsätzlich einmal je Quartal treffen.

Durch Senatsbeschlüsse bedingt sind die bisherigen ADV-Bestimmungen zum großen Teil außer Kraft gesetzt worden. Die so entstandene Regelungslücke soll das neue TuI-Regelwerk schließen. Es soll vor allem die zentralen bzw. einheitlichen Vorgaben für die im übrigen dezentrale Ressourcen- und Einsatzverantwortung definieren. In dieser Textsammlung sollen alle Regelungen - entweder direkt oder durch Verweise - vereinigt werden, die für die Beschaffung und den Einsatz von technisch unterstützter Informationsverarbeitung relevant sind. Dadurch soll auch eine Umsetzung der datenschutzrechtlichen Anforderungen an die TuI gewährleistet werden.

Seit dem 1. Juli 1994 liegt dem TuI-Ausschuß ein Entwurf des neuen TuI-Regelwerkes vor. Dieser ist bislang allerdings unvollständig und in seiner Struktur sehr unübersichtlich. Die letzte Stellungnahme der Ressorts ging erst am 22. November im TuI-Referat der SKP ein. Daher konnte in der zweiten Sitzung des TuI-Ausschusses am 24. November noch keine überarbeitete Fassung vorgelegt werden. Das Regelwerk soll thematisch nach Richtlinien sowie Empfehlungen und Handlungshilfen strukturiert werden. Die SKP hat zugesichert, daß bilaterale Gesprächen geführt werden, sofern Einwendungen der Ressorts bzw. von mir in der Überarbeitung nicht berücksichtigt werden sollen.

Die SKP plant, die jeweils überarbeiteten Teile des TuI-Regelwerkes nach und nach in Kraft zu setzen. Die ersten Teile sollen im ersten Halbjahr 1995 in Kraft treten. Ein Termin, zu dem das TuI-Regelwerk abgeschlossen sein wird, wurde von der SKP noch nicht genannt. Der Datenschutzausschuß der Bürgerschaft hat auf seiner Sitzung am 6. Dezember 1994 die Informationen der SKP zum damaligen Sachstand entgegengenommen und sich eine Überprüfung der Angelegenheit im Sommer 1995 vorbehalten (vgl. o. Ziff. 2, zu 16. JB, Ziff. 2.3.2.1)

5.1.2. Einführung von Electronic Mail (X.400)

Electronic Mail bedeutet die Übermittlung von Nachrichten (Daten, Texte, etc.) über elektronische Transportwege (z.B. Telefonleitungen, ISDN, DATEX-P und andere Datenleitungen), bei der die Nachrichten von dem Absender/der Absenderin in ein "Postfach" des Empfängers/der Empfängerin befördert werden; dort müssen sie von dem Adressaten abgerufen werden. Der Absender braucht daher nicht direkt auf die Rechner der Empfänger zuzugreifen. X.400 bezeichnet dabei eine Gruppe von Normen, d.h. einen internationalen technischen Standard für Electronic-Mail-Systeme.

5.1.2.1. Optimierung des Informationsaustauschs - die Planung des Senats

Die zuständigen Gremien der Europäischen Union, die Konferenz der Innenminister des Bundes und der Länder sowie auch der Kooperationsausschuß Automatisierte Datenverar-

beitung von Bund, Ländern und Gemeinden (KoopADV) befürworten bzw. beabsichtigen den Einsatz von Systemen, die dieser Norm entsprechen.

Wegen der Mitwirkung an der Gesetzgebung über den Bundesrat sowie an EU-Angelegenheiten sowie zur Verbesserung des länderübergreifenden Informationsaustauschs plant auch der Senat den Anschluß der eingebundenen Ressorts an ein X.400-System. Dazu wird in der bremischen Verwaltung ein zwölfmonatiger Betriebsversuch mit 25 Anschlüssen durchgeführt.

Mir wurde frühzeitig ein Konzeptentwurf ausgehändigt. Da bei dem elektronischen Versand von Mitteilungen nicht nur die Verbindungsdaten, sondern auch die Inhaltsdaten in digitaler Form anfallen und zwischengespeichert werden, sind zur Verhinderung von Persönlichkeitsprofilen sowie von nicht zugelassenen Leistungs- und Verhaltenskontrollen geeignete Datenschutzvorkehrungen unverzichtbar. Dies gilt umso mehr, als X.400-basierte Mailsysteme nicht nur in der öffentlichen Verwaltung, sondern auch im nichtöffentlichen Bereich eine immer größere Rolle spielen. Es ist damit zu rechnen, daß in einigen Jahren ein großer Teil der Behörden- und Geschäftspost von der herkömmlichen "gelben Post" auf diese Form der Telekommunikation verlagert wird.

5.1.2.2. Standards für die Datensicherung

Einige grundsätzliche Anforderungen an die Datensicherung habe ich vorab dem federführenden TuI-Referat der SKP mitgeteilt:

1. Die sicherheitstechnischen Vorgaben der X.400-Empfehlung des Normungsgremiums aus dem Jahr 1988 müssen erfüllt sein. Wo dies bei vorhandenen Systemen nicht der Fall ist, sollte dieser Standard durch eine Nachrüstung mit geeigneten Zusatzprodukten oder durch Verwendung neuerer Softwareversionen erreicht werden.

2. Die Funktion der Systemverwaltung ist grundsätzlich von der der Netzverwaltung - insbesondere der Verwaltung des E-Mail-Systems - zu trennen.

3. Grundsätzlich sollte - zumindest bei Neuanschaffungen - separat administrierbare Hard- und/oder Software eingesetzt werden (z.B. ein separater Telekommunikationsserver).

4. Bei der Verwendung öffentlicher Übertragungswege sind vorhandene Sicherheitsmechanismen (z.B. geschlossene Benutzergruppen, Rufnummernidentifikation, Teilnehmeridentifizierung und -Authentifikation, automatische Rückruffunktion usw.) zu nutzen.

5. Zur Beweissicherung einer Kommunikation sollte die eingesetzte Software Zustellungs-/Empfangsnachweise und Sende-/Empfangsübergabenachweise anbieten.

6. Bei der Übertragung personenbezogener Daten ist zumindest eine Verbindungsverschlüsselung auf den Übertragungswegen des öffentlichen Netzes vorzusehen. Bei sensiblen personenbezogenen Daten bzw. vertraulichen Kommunikationsinhalten ist eine Übertragung nur mit einer Ende-zu-Ende-Verschlüsselung zuzulassen.

7. Die verwendeten Verschlüsselungsgeräte oder -algorithmen sind durch technische, bauliche und organisatorische Maßnahmen vor dem Zugriff Unbefugter zu schützen.

8. Zur Verschlüsselung der Daten sind hinreichend sichere Verschlüsselungsverfahren zu verwenden. Neben der Auswahl eines sicheren Algorithmus (z.B. Tripple-DES oder IDEA) ist ein sichereres Schlüsselmanagement erforderlich.

9. Zur Sicherung der Integrität der Daten sollte die elektronische Unterschrift eingesetzt werden.

10. Für die Speicherung der Kommunikationsnachweise sollte grundsätzlich eine Frist festgelegt werden; von den Benutzern und Benutzerinnen sollte im Einzelfall eine erforderliche längere Speicherung selbst festgelegt werden können.

Die SKP hat ihre prinzipielle Übereinstimmung mit diesen Anforderungen erklärt. Meine Dienststelle wird an der diesen Betriebsversuch begleitenden Projektgruppe teilnehmen.

5.1.3. Pilotprojekt "Elektronisches Postsystem"

Im Januar 1994 wurde ein Pilotprojekt zum elektronischem Textaustausch zwischen den Pressereferaten der Ressorts und der Informations- und Pressestelle des Senats gestartet. Ziel war es, die von den Pressereferaten erstellten und zur Veröffentlichung bestimmten Texte möglichst zeitnah der Informations- und Pressestelle übermitteln zu können, ohne daß dort die Texte erneut erfaßt werden müssen. Hierzu wurde in der Senatspressestelle ein "elektronisches Postamt" eingerichtet. Eingesetzt wurde das Programm "Windows for Workgroups", um unter Verwendung der - von der BreKom zur Verfügung gestellten - ISDN-Leitungen direkte Verbindungen zwischen den jeweiligen PCs aufzubauen.

Ich habe das Projekt beratend begleitet. Es stellte sich heraus, daß die verwendete Technik nicht nur unter Datensicherheitsaspekten den Anforderungen nicht genügte. So konnte u.a. der PC, der als "elektronisches Postamt" fungierte, nicht ausreichend abgesichert werden. Um Texte dort ablegen zu können, benötigten die Pressereferate den schreibenden Zugriff. Dieser Zugriff war aber nicht weiter differenzierbar, weswegen u.a. auch ein versehentliches Löschen der gespeicherten Texte nicht auszuschließen war.

Daher wird dieses Projekt in dem Betriebsversuch X.400 (s.o. 5.1.2) aufgehen, d.h. die Senatspressestelle soll ein Mailsystem nach dem X.400-Standard erhalten.

5.1.4. Bürgerinformations-System

An der Universität Bremen entwickelt die Forschungsgruppe Telekommunikation des Fachbereichs 3 ein Bürgerinformations-System (BIS). Hierzu habe ich meine Beratung angeboten und bereits auch Hinweise zu möglichen Gefährdungen des Rechts auf informationelle Selbstbestimmung gegeben, die von der Forschungsgruppe berücksichtigt wurden. So gibt es in diesem System z.B. sogenannte "schwarze Bretter", in denen zu unterschiedlichen Themenbereichen von den Benutzern und Benutzerinnen Texte eingegeben werden können. Da nicht festgestellt werden kann, von wem ein Text eingegeben wurde, ist hier ein Mißbrauch möglich; z.B. können die Anschriften und Telefonnummern unbeteiligter Personen eingegeben werden, die dann mit unbestellten Warenlieferungen, Dienstleistungen oder Mitteilungen belästigt werden.

Erste Prototypen von an dieses BIS angeschlossenen Infosäulen stehen bereits an öffentlichen Orten Bremens zur Verfügung.

Im Rahmen dieses BIS soll eine Infothek mit einem Behördenwegweiser eingerichtet werden. Er soll es ratsuchenden Bürgerinnen und Bürgern erleichtern, die jeweils zuständige Stelle sowie deren Anschrift, Öffnungszeiten etc. herauszufinden. Auf meine Anregung hin wird auch meine Dienststelle in den Behördenwegweiser aufgenommen.

5.2. Kontrolle der Vernetzung durch Protokollierung von PC-Aktivitäten

Der Arbeitskreis "Technischer und organisatorischer Datenschutz" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Orientierungshilfe "Datenschutzrechtliche Protokollierung beim Betrieb informationstechnischer Systeme (IT-Systeme)" erstellt. Ich habe dieses Papier der SKP und auch dem Gesamtpersonalrat übermittelt. Für die Umsetzung der von § 6 BrDSG geforderten technischen und organisatorischen Maßnahmen der Datensicherung ist eine Aufzeichnung der Benutzeraktivitäten in vielen Fällen unverzichtbar.

Neben den Rechtsgrundlagen und dem Gegenstand der Protokollierung führt die Orientierungshilfe die nachstehenden technischen und organisatorischen Rahmenbedingungen auf:

1. Die für den TuI-Einsatz verantwortlichen Stellen sollen ein Revisionskonzept erstellen, das die Zielrichtung der Protokolle und der Kontrollen sowie Schutzmechanismen für die Rechte der Mitarbeiter und Mitarbeiterinnen und der sonstigen betroffenen Personen klar definiert.

2. Die Zwangsläufigkeit und damit die Vollständigkeit der Protokolle muß gewährleistet werden.

3. Das gleiche gilt für die Manipulationssicherheit der Einträge in Protokolldateien.

4. Entsprechend der Zweckbindung der Datenbestände müssen wirksame Zugriffsbeschränkungen realisiert werden.

5. Die Protokolle müssen so gestaltet sein, daß seitens der Revisoren eine effektive Überprüfung möglich ist.

6. Die Auswertungsmöglichkeiten sollten vorab mit den Revisoren abgestimmt und festgelegt sein.

7. Kontrollen sollten nach dem Vier-Augen-Prinzip erfolgen.

8. Es sollte vorab definiert werden, welche Konsequenzen sich aus Verstößen ergeben, die durch die Kontrolle von Protokollen aufgedeckt werden.

9. Für Routinekontrollen sollten automatisierte Verfahren (z.B. watch dogs) verwendet werden.

10. Personalräte und Arbeitnehmervertreter(innen) sollten bei der Erarbeitung des Revisionskonzeptes und bei der Auswertung der Protokolle beteiligt werden.

Diese von den Datenschutzbeauftragten übereinstimmend definierten Grundstandards werde ich u.a. bei örtlichen Kontrollen und bei Stellungnahmen zu PC-Anträgen zugrunde legen.

5.3. Mobilfunk: Informationsbroschüre publiziert

In Zusammenarbeit mit dem Hamburgischen und dem Berliner Datenschutzbeauftragten wurde der Bericht über die Netz- und Datensicherheit in der Mobilkommunikation (vgl. 16. Jahresbericht, Ziff. 2.3.1.1.) überarbeitet und aktualisiert. Er ist im Januar 1995 als Broschüre erschienen und in den Fachkreisen einschließlich der Fachpublizistik breit verteilt worden. Das Heft kann bei mir gegen Zusendung von 1,50 DM in Briefmarken bestellt werden

6. Datenschutzrichtlinie der Europäischen Union - der Durchbruch

6.1. Gemeinsamer Standpunkt verabschiedet

Für die Harmonisierung des Datenschutzrechts der Mitgliedstaaten in der Europäischen Union ist zu Anfang dieses Jahres der hoffentlich entscheidende Durchbruch erzielt worden. Viereinhalb Jahre sind seit der Vorlage des ersten Richtlinienentwurfs der EU-Kommission im September 1990 vergangen, bis am 20. Februar 1995 der sog. "Gemeinsame Standpunkt" des EU-Ministerrats zum Geänderten Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 15.10.1992 (ABl EG, Nr. C 311, S. 30 ff.) verabschiedet werden konnte.

Entscheidenden Anteil an diesem immer wieder durch nationale Interventionen in Frage gestellten Erfolg hatte der Bundesbeauftragte für den Datenschutz, Jacob, der in der entscheidenden Phase der deutschen Ratspräsidentschaft im zweiten Halbjahr 1994 die zuständige Ratsarbeitsgruppe leitete. Einen wichtigen Beitrag hat auch die Konferenz der Datenschutzinstitutionen in der EU geleistet, die auf mehreren Sitzungen Regelungsprinzipien und Formulierungsvorschläge für die Richtlinie erarbeitet hat. Ausgangspunkt, Entstehungsgeschichte und Regelungsprobleme habe ich ausführlich in den beiden Vorberichten dargestellt (vgl. 15. JB, Ziff. 2.3; 16. JB, Ziff. 2.4.1).

6.2. Weiteres Verfahren

Mit Inkrafttreten der Richtline wird es in allen EU-Ländern die Gebote der rechtmäßigen Datenerhebung und der Zweckbindung der Datenverarbeitung, den Sonderschutz für besonders sensible Daten, die Rechte des Bürgers auf Auskunft, Berichtigung und Löschung sowie externe unabhängige Kontrollinstanzen geben, alles Kernpunkte auch der deutschen Datenschutzgesetzgebung in Bund und Ländern. Doch steht diese Erfolgsmeldung unter Vorbehalt: Um überhaupt den Konsens der Mehrzahl der Regierungen zu erreichen, findet sich im "Gemeinsamen Standpunkt" eine Reihe vage formulierter Generalklauseln; außerdem mußten zahlreiche Sonderwünsche einzelner EU-Staaten mit Ausnahmebestimmungen erfüllt werden.

Der Richtlinienentwurf geht jetzt zur 2. Lesung ins Europäische Parlament, die im Sommer 1995 abgeschlossen werden müßte, sodann ein weiteres Mal in den Ministerrat. Mit dem Inkrafttreten, dessen genauer Zeitpunkt noch nicht prognostiziert werden kann, beginnt eine dreijährige Übergangsfrist, innerhalb derer die Mitgliedstaaten die Richtlinie in ihr nationales Recht umsetzen müssen.

6.3. Konsequenzen

Die allgemeinen Datenschutzgesetze von Bund und Ländern werden aufgrund der Richtlinie voraussichtlich nur in wenigen Punkten geändert werden müssen, etwa bei den Meldepflichten für Dateien.

Für die bereichsspezifische Gesetzgebung in Deutschland kommt es maßgeblich an auf die zur Wirkung der Richtlinie lange diskutierte Alternative zwischen Sperrwirkung oder Mindeststandard. Es geht dabei um die Frage, ob die Richtlinie über ihr Schutzniveau hinausgehende Bestimmungen verhindert oder auch nach ihrem Inkrafttreten die Befugnis der Mitgliedstaaten bestehen bleibt, für Teilbereich von Verwaltung und Wirtschaft - also z.B. im Arbeits- und Sozialrecht - im Vergleich zum allgemeinen Datenschutzrecht strengere Normen zu erlassen. Der neu formulierte Erwägungsgrund Nr. 9 des Entwurfs spricht insoweit von einem "Spielraum" für Verbesserungen, der allerdings nur "im Rahmen der Durchführung der Richtlinie" ausgefüllt werden kann.

Eine detaillierte Analyse des Änderungsbedarfs für das deutsche Recht kann sinnvollerweise in diesem Jahresbericht noch nicht geleistet werden. Erst wenn der Text nach dem Gesetzgebungsverfahren in allen zuständigen Organen der Europäischen Union (s.o.) endgültig feststeht, kann die dafür erforderliche sorgfältige Interpretation vorgenommen werden. Die dafür notwendigen Vorarbeiten erfolgen im Rahmen der EU- Datenschutzkonferenz sowie auf nationaler Ebene in der deutschen Datenschutzkonferenz.

7. Bürgerschaft

7.1. Rundfunkübertragungen aus Untersuchungsausschüssen

Der Untersuchungsausschuß "Personalbesetzungspraxis bei Eigen- und Beteiligungsgesellschaften" hatte mich um eine Prüfung der Frage gebeten, ob gegen Rundfunkübertragungen aus seinen in öffentlicher Verhandlung durchzuführenden Beweisaufnahmen datenschutzrechtliche Bedenken bestehen (vgl. bereits 12. JB, Abschn. 2.2.1, zur gleichen Fragestellung beim Untersuchungsausschuß ZKH St.-Jürgen-Straße). Diese Frage habe ich unter bestimmten Umständen, die im folgenden näher erläutert werden, bejaht.

7.1.1. Verfassungsrechtliche Ausgangslage und Abwägungsgebot

Das Bremische Datenschutzgesetz (BrDSG) selbst findet dabei unmittelbar keine Anwendung, da die parlamentarische Tätigkeit und die mit ihr verbundene Weitergabe bzw. Publikation persönlicher Daten außerhalb seines Geltungsbereichs liegt.

Auch für die Beurteilung der bremischen Rechtslage ist die insoweit einschlägige Rechtsprechung des Bundesverfassungsgerichts zu den Befugnissen von Untersuchungsausschüssen maßgeblich. Das sog. Flick-Urteil des Bundesverfassungsgerichts hat bekräftigt,

daß sich das Beweiserhebungsrecht eines parlamentarischen Untersuchungsausschusses (Art. 44 Abs. 1,2 GG; Art. 105 Abs. 6 LV) und der grundrechtliche Datenschutz (Artt. 1, 2 Abs. 1 GG) der Zeugen und sonstigen in das Verfahren einbezogenen Personen auf der Ebene des Verfassungsrechts gegenüberstehen und im konkreten Fall einander so zugeordnet werden müssen, daß beide soweit wie möglich ihre Wirkungen entfalten (BVerfGE 67, 143 f.). Diese Aussage beruht auf der weiteren verfassungsgerichtlichen Feststellung, daß parlamentarische Untersuchungsausschüsse öffentliche Gewalt ausüben und dementsprechend nach Art. 1 Abs. 3 Grundgesetz die Grundrechte zu beachten haben (BVerfGE 77,46).

Zu diesen Grundrechten zählen auch das Persönlichkeitsrecht und das aus ihm abgeleitete informationelle Selbstbestimmungsrecht; auf die Nichtanwendbarkeit des BrDSG (s.o.) kommt es insoweit also nicht an. Für diese Abwägung verlangt das Bundesverfassungsgericht, namentlich Art und Bedeutung des mit der beabsichtigten Beweiserhebung verfolgten Ziels im Rahmen des Untersuchungsauftrages der Schutzwürdigkeit und Schutzbedürftigkeit der betroffenen personenbezogenen Daten gegenüberzustellen (BVerfGE 77,47). Immer sei zu prüfen, ob "nach den gegebenen Umständen" eine öffentliche Beweisaufnahme und Erörterung gerechtfertigt sei (BVerfGE 76, 388).

Die zitierte Rechtsprechung des Bundesverfassungsgerichts bezieht sich unmittelbar (nur) auf das Beweiserhebungsrecht, insbesondere auf den Anspruch auf Herausgabe von Akten gegenüber der Exekutive, und auf die unmittelbare Sitzungsöffentlichkeit. Das Gericht hat sich - soweit ersichtlich - noch nicht direkt zur Thematik von Rundfunkübertragungen geäußert. Rundfunkübertragungen stellen jedoch gegenüber der bloßen Teilnahme von Zuhörern bzw. Zuschauern - auch wenn es sich um später über die Sitzung berichtende Medienvertreter handelt - einen zusätzlichen Eingriff in das informationelle Selbstbestimmungsrecht der Zeugen bzw. auch der in Fragen von Ausschußmitgliedern oder in Darlegungen von Zeugen erwähnten Dritten dar. Die Zeugenaussage und damit deren Inhalt werden weit und an einen unbestimmt großen Personenkreis verbreitet.

Diese große Publizität parlamentarischer Untersuchungsausschüsse kann eine möglicherweise noch folgenschwerere soziale Ächtung bewirken als ein Strafverfahren (vgl. Richter, Privatpersonen im parlamentarischen Untersuchungsausschuß, Köln 1990, S. 59 f.). Das Bundesverfassungsgericht hat auf die besondere Problematik des Grundrechtseingriffs durch Veröffentlichung im sog. Entmündigungsbeschluß ausdrücklich hingewiesen (BVerfG NJW 1988, 2031). Das auf die Informationsbeschaffung und die unmittelbare Öffentlichkeit des Untersuchungsausschusses bezogene Abwägungsgebot muß daher auch und erst recht für mögliche Grundrechtsbeeinträchtigungen durch die sog. mittelbare Ausschußöffentlichkeit in Form der elektronischen Medienberichterstattung gelten.

7.1.2. Zur Interpretation von § 7 BremUAG

Für den Teilaspekt der Öffentlichkeit der Beweisaufnahme greift § 7 Abs. 2 BremUAG das verfassungsrechtliche Abwägungsgebot insoweit auf, als der Untersuchungsausschuß die Öffentlichkeit ausschließen kann, wenn "das berechtigte Interesse eines Einzelnen" - gemeint ist in erster Linie der zu vernehmende Zeuge, aber auch in Ausschußunterlagen erwähnte Dritte - dies "gebietet" (s.a. § 7 Abs. 5 BremUAG betr. die Geheim- bzw. Vertraulicherklärung sowie die Parallelregelung für den Strafprozeß in § 171b Gerichtsverfassungsgesetz). Die Vorschrift setzt mithin voraus, daß der Untersuchungsausschuß bei der Vorbereitung von Zeugenvernehmungen, der Verlesung von Schriftstücken usw. die Voraussetzungen für den Ausschluß der Öffentlichkeit prüft und unter diesen vor allem das entgegenstehende Persönlichkeitsrecht der Betroffenen berücksichtigt.

Schon zur Erfüllung des § 7 Abs. 2 BremUAG ist mithin eine auf die besondere Situation bestimmter Zeugen bzw. Betroffener zugeschnittene Einzelfallprüfung zwingend. Wo schon das Beweiserhebungsrecht nicht greift, weil die Weitergabe von Angaben an den Auschuß wegen ihres "streng persönlichen Charakters" nicht zulässig (gewesen) wäre (vgl. BVerfGE 76, 388 unter Hinweis auf BVerfGE 65,46), kommt erst recht keine öffentliche Verhandlung in Betracht. Werden die Vorausetzungen schon für den Ausschluß der unmittelbaren, präsenten Öffentlichkeit wegen entgegenstehender Datenschutzrechte

bejaht, ergibt sich daraus für diese Sitzungen ohne weiteres die Unzulässigkeit von Ton- oder Bildübertragungen.

Liegt kein Fall des völligen Ausschlusses der Öffentlichkeit vor, geht § 7 Abs. 1 Satz 2 BremUAG von einem Entscheidungsspielraum des Ausschusses bei der Zulassung von Rundfunkübertragungen aus. Die gleiche Regelung - teilweise mit der Entscheidungsbefugnis (nur) des Vorsitzenden - enthalten die Ländergesetze von Baden- Württemberg, Berlin und Sachsen. In den Bundesländern Brandenburg, Nordrhein-Westfalen, Rheinland-Pfalz und Schleswig-Holstein erklären die jeweiligen gesetzlichen Regelungen dagegen Rundfunkübertragungen generell für unzulässig; Sachsen- Anhalt beschränkt das Verbot auf live-Übertragungen. Aus den Darlegungen über die Grundrechtsbindung des Untersuchungsausschusses und die verfassungsrechtlich gebotene Abwägung zwischen Art und Umfang der Beweisaufnahme einerseits und dem Datenschutz der Betroffenen andererseits (s.o. 7.1.1) ergibt sich, daß eine undifferenzierte, generelle Zulassung von Rundfunkberichterstattung aus allen öffentlichen Sitzungen des Untersuchungsausschusses nicht in Betracht kommen kann.

7.1.3. Die Abwägungskriterien

7.1.3.1. Argumente für die Zulassung von Übertragungen

Als Entscheidungskriterien im Rahmen der Abwägung kommen zugunsten einer Zulassung u.a. in Betracht (vgl. zusammenfassend Binder, Die "Öffentlichkeit" nach Art. 42 Abs. 1 Satz 1, 44 Abs. 1 Satz 1 GG und das Recht der Massenmedien zur Berichterstattung, DVBl. 1985, 1112,1116 ff.)

a) die Bedeutung des Öffentlichkeitsprinzips im demokratischen Parlamentarismus (vgl. BVerfGE 40, 249; 70, 355), dem das Bundesverfassungsgericht gerade bei sog. "Mißstandsenquèten" einen besonders hohen Stellenwert zumißt (BVerfGE 77,48); dies gilt sowohl für die Darstellungsmöglichkeiten der parlamentarischen Opposition (vgl. dazu Richter, a.a.O., S. 102 ff.) als auch für die Kontrollfunktion der Bevölkerung, die die möglichst umfassende Gelegenheit zur Kenntnisnahme voraussetzt,

b) die Tatsache, daß die unmittelbare Sitzungsöffentlichkeit in ihrer Bedeutung gegenüber der durch die Massenmedien hergestellten Öffentlichkeit weitgehend zurücktritt, der eigentliche Sinn der parlamentarischen Untersuchung vielfach gerade im öffentlichen Vorgang des Ermittelns (und weniger im Abschlußbericht) liegt,

c) die Privilegierung der Presse bzw. die Unmöglichlichkeit gerade der rundfunkspezifischen Berichterstattung beim Ausschluß von Ton- und Bildübertragungen,

d) das Interesse bestimmter Zeugen, auf durch die Medien verbreitete Behauptungen und Feststellungen mit gleichem Wirkungsgrad, d.h.über die gleichen Medien, antworten zu können.

7.1.3.2. Argumente gegen Rundfunkübertragungen

Mit diesen generellen, aus Demokratieprinzip und Parlamentsrecht hergeleiteten Kriterien sind im Einzelfall u.a. folgende Gesichtspunkte abzuwägen:

a) Die Rundfunkübertragung bedeutet gegenüber der Sitzungsöffentlichkeit einen zusätzlichen Eingriff in das informationelle Selbstbestimmungsrecht der Zeugen bzw. sonstiger betroffener Dritter (s.o. 7.1.1).

b) Die bloße Hörfunkübertragung kann für den Gesamteindruck wesentliche Reaktionsformen und Verhaltensweisen der Ausschußmitglieder und der Zeugen, die bei Anwesenheit in der öffentlichen Sitzung wahrnehmbar sind, nicht vermitteln, liefert also technisch bedingt nur einen Teilausschnitt der Kommunikation während der Verhandlung.

c) Bei live gesendeten Rundfunkübertragungen läßt sich aufgrund der Unmittelbarkeit der Informationsweitergabe schwerer sicherstellen, daß die vom Untersuchungsausschuß entweder der aktenübermittelnden Stelle gegenüber zugesagten oder von ihm

selbst zu sichernde Vertraulichkeit bestimmter Unterlagen mit sensiblem Inhalt (s.u. d) gewahrt bleiben kann.

d) Bei der in diesem Untersuchungsausschuß im Vordergrund stehenden Erörterung von Personalvorgängen besteht ein besonders hohes Risiko, daß Sachverhalte angesprochen werden, die weit über den dienstlichen Bereich und den Untersuchungsauftrag des Ausschusses hinaus in die Privatsphäre hineinreichen. Personalakten kommt wegen ihres Charakters als besonders umfangreicher Datensammlung in der Rechtsprechung sowohl des Bundesarbeitsgerichts als auch des Bundesverwaltungsgerichts ein besonderer Vertrauensschutz zu (vgl. BVerwGE 19, 179, 185; OVG Münster, DVBl. 1988, 1o76). Auch der Bremische Staatsgerichtshof hat in seiner Entscheidung vom 13. März 1978 (-St 3/76-) unterstrichen, daß gerade die Vorlage von Personalakten an einen Untersuchungsausschuß mit Grundrechten kollidieren kann.

Dabei sind die Risiken für Grundrechtsbeeinträchtigungen prinzipiell höher, wenn

a) nicht das Verhalten von politischen oder administrativen Entscheidungsträgern, sondern Informationen von oder über Privatpersonen oder gar unbeteiligte(n) Dritten oder

b) persönliche Verhältnisse außerhalb unmittelbar dienstlicher bzw. geschäftlicher Vorgänge (z.B. ärztliche Befunde, Inhalte von Beurteilungen o.ä.)

entweder Gegenstand der Sitzung sein oder zumindest voraussichtlich angesprochen werden sollen.

7.1.3.3. Konsequenzen für die Organisation der Ausschußarbeit

Die o.a. Kriterien für den völligen Ausschluß der Öffentlichkeit bzw. die Zulassung von Rundfunkübertragungen sind für den Untersuchungsausschuß zunächst bei der Zusammenstellung der Zeugenlisten für einzelne Sitzungstermine relevant. Der Ausschuß kann bzw. ggf. muß diese Maßnahmen aber auch während einer laufenden Sitzung treffen, wenn sich bei einer Zeugenaussage das zunächst nicht vorhergesehene Risiko einer Grundrechtsbeeinträchtigung ergibt. Bei Zweifeln hat der Ausschuß auch die Möglichkeit, den betroffenen Zeugen nach seinem Einverständnis mit der Rundfunkübertragung seiner Aussage zu fragen.

7.2. Gläserne Abgeordnete?

7.2.1. Parlamentarisches Informations- und Kommunikationssystem (ParlIS) in Planung

Bereits im Jahre 1990 begannen in der Bremischen Bürgerschaft die Planungen für ein EDV-gestütztes Parlamentarisches Informations- und Kommunikationssystem (ParlIS). Hierzu wurde auch eine Parlamentarische Arbeitsgruppe ParlIS eingesetzt. Der damals noch bestehende ADV-Ausschuß behandelte dieses Thema in zwei Sitzungen jeweils im November der Jahre 1990 und 1991. Im November 1991 informierte mich die Verwaltung der Bremischen Bürgerschaft in einem kurzen Schreiben über die geplante Einführung.

Kernstück sollte das bislang konventionell geführte Sach- und Sprechregister in Form einer vorgangsbezogenen Parlamentsdokumentation werden. Das Sprechregister beinhaltet die in der Bürgerschaft behandelten Themen und ordnet ihnen die Sitzungstermine und die Abgeordneten zu, die zu diesem Punkt im Plenum das Wort ergriffen haben. Darüber hinaus war geplant, den Personalienteil des Handbuchs der Bremischen Bürgerschaft in dieses System einzubeziehen.

Im Januar 1994 erhielt ich dann zunächst die Information, daß die Bremische Bürgerschaft kurz vor der Einführung des ersten Teiles des DV-gestützten ParlIS, dem Sach- und Sprechregister, stehe. Im Juni 1994 erfuhr ich dann, in einem weiterem Schritt sei die DV-technische Umsetzung der Berechnung von Entschädigungsleistungen für Abgeordnete und Deputierte, d.h. von Sitzungsgeldern, Erwerbsausfall und Fahrtkosten geplant. Hinzu kommen sollten später die Integration des Personalienhandbuches und der Aus-

schußunterlagen in das DV-System. Dazu sollte ein Feinkonzept für die Datensicherung erstellt und mir zugesandt werden.

7.2.2. Datenschutzrelevante Systembereiche

Ich nahm dies wiederum zum Anlaß, meine Beratung frühzeitig anzubieten und wies gleichzeitig darauf hin, daß insbesondere die folgenden Bereiche aus datenschutzrechtlicher Sicht einer kritischen Betrachtung bedürfen:

- Berechnung der Entschädigungsleistungen für Abgeordnete,
- Vernetzung der Fraktionen,
- Umfang des Sprechregisters und
- Recherchemöglichkeiten.

In einem ersten Gespräch im August 1994 war Schwerpunkt das DV-Verfahren "Entschädigungsleistungen". Ich empfahl der Verwaltung der Bürgerschaft die Ausarbeitung eines Datenschutzkonzeptes, das eindeutige Regelungen über die Zugriffsrechte, die Auswertungsrechte und die Sperrung sowie Löschung von Daten enthalten sollte. Derartige Sicherungen sind aber auch bei anderen Teilen des ParlIS erforderlich: Wenn etwa Abgeordnete in Parlamentsunterlagen - wie z.B. im Sprech- und Sachregister oder in Plenarprotokollen und Drucksachen - nach bestimmten Vorgängen und Stichworten recherchieren, muß verhindert werden, daß Unbefugte aus der Verwaltung oder dem Kollegenkreis Kenntnis von oder Zugriff auf die Nutzerdaten erhalten und sich damit Informationen z.B. über geplante parlamentarische Aktivitäten verschaffen. Auch die Einbindung der Fraktionsangestellten mit ihren Büros außerhalb des Hauses der Bürgerschaft stellt besondere Anforderungen an die Sicherung der Daten.

Entsprechend dem Wunsch der Bürgerschaftsverwaltung habe ich ihr die Mustergliederung für ein solches Datenschutzkonzept zugeleitet. Das Konzept habe ich kurz vor Redaktionsschluß dieses Berichts erhalten, konnte es aber nicht mehr im einzelnen überprüfen. Im April 1995 werden die Gespräche mit der Leitung der Bürgerschaftsverwaltung fortgesetzt.

7.3. Bürgerantrag - Zweckbindung für Unterschriftenlisten

Die Bürgerschaft hat in ihrer Dezember-Sitzung das Gesetz über das Verfahren bei Bürgeranträgen beraten und beschlossen. Es ist inzwischen in Kraft getreten (Gesetz vom 20.12.94, BremGBl. S. 325). Dieses Gesetz beruht auf Art. 86 Abs. 2 Satz 3 der novellierten Landesverfassung, die erstmals den Bürgerantrag als Instrument verbesserter partizipativer Beteiligung der Bevölkerung am politischen Willensbildungsprozeß eingeführt hat.

Bei der Überprüfung des Entwurfs stellte ich fest, daß er keine Regelungen über den Umgang mit den Unterschriftenlisten bei der Bürgerschaft bzw. bei den Meldebehörden enthielt. Wichtige Voraussetzung dafür, den verfassungsrechtlichen Anforderungen an die Wahrung des Grundrechts auf Datenschutz zu genügen, ist es aber, daß sich die Unterzeichner darauf verlassen können, daß die eingereichten Listen mit ihren Personalien strikt zweckgebunden, d.h. ausschließlich für die Durchführung des Antragsverfahrens, verwendet und nur für die erforderliche Dauer aufbewahrt werden. Für den Bürger muß auch und gerade bei "sensiblen" Antragszielen Gewißheit bestehen, daß Dritte außerhalb des Verfahrens keinen Zugang zu den Unterschriftenlisten erhalten. In der Vergangenheit hat es in anderen Bundesländern mangels präziser Vorgaben wiederholt Probleme beim Umgang mit diesen Unterlagen gegeben.

Um dieses Regelungsziel sicherzustellen, schlug ich eine Ergänzung von § 4 um einen neuen Absatz 5 mit folgendem Wortlaut vor: "Die Unterschriftsbogen dürfen ausschließlich zur Prüfung der Zulässigkeit des Bürgerantrags verwendet werden. Sie sind nach Abschluß des Antragsverfahrens zu vernichten." Dieser Textvorschlag wurde vom Verfassungs- und Geschäftsordnungsausschuß der Bürgerschaft akzeptiert und in den endgültigen Gesetzestext aufgenommen.

Die Vorschrift richtet sich zunächst an die Bürgerschaft bzw. ihren Präsidenten. Ihm obliegt es, u.a. durch organisatorische Maßnahmen zu gewährleisten, daß nur solche Abgeordnete und Verwaltungsmitarbeiter Einblick in die Listen nehmen können, die mit dem Antragsverfahren befaßt sind. Die Vorschrift richtet sich weiterhin an die Meldeämter. Die durch den vorgeschlagenen neuen Absatz vorgeschriebene Zweckbindung soll dort sicherstellen, daß die Anschriften der Unterzeichner nicht zu melderechtlichen Zwecken genutzt werden; eine solche zweckwidrige Nutzung von Personalien hatte das Bundesverfassungsgericht im Volkszählungsurteil von 1983 gerügt. Die Vernichtung der Listen nach Verfahrensende entspricht dem allgemeinen Datenschutzprinzip der Löschungspflicht nach Wegfall des Verarbeitungszwecks. Archivrechtliche Regelungen bleiben dadurch unberührt.

8. Personalwesen

8.1. KIDICAP - Fremdverarbeitung von Mitarbeiterdaten der Krankenhäuser

8.1.1. Rechtliche Vorgaben für die Auftragsgestaltung

Die kommunalen Krankenhausbetriebe Bremens haben seit Jahren Aufgaben der Personalabrechnung und der Personalwirtschaft von der Senatskommission für das Personalwesen (SKP) wahrnehmen lassen. Die Verarbeitung der anfallenden Personaldaten erfolgte im früheren Rechenzentrum der bremischen Verwaltung, der jetzigen ID Bremen. Da nach Angaben der senatorischen Behörde die eingesetzen Verfahren nicht mehr den Anforderungen der Krankenhäuser an flexible Auswertungsmöglichkeiten und Unterstützung bei der personalwirtschaftlichen Arbeit entsprach, haben sich die kommunalen Krankenhausbetriebe von ID Bremen gelöst und das Rechenzentrum Volmarstein (RZV) in Nordrhein-Westfalen auf der Basis des Datenverarbeitungsprogramms KIDICAP mit der Datenverarbeitung beauftragt (vgl. 16. JB, Ziff. 2.2.3).

Dies ist nach meinem Informationsstand der erste Fall, in dem eine bremische öffentliche Stelle ein privates Rechenzentrum außerhalb Bremens in derart großem Umfang mit der Personaldatenverarbeitung beauftragt. Aus diesem Grunde habe ich dieses "Outsourcing"-Projekt mit besonderer Intensität begleitet. Entscheidend ist dabei die genaue Umsetzung der Vorgaben des § 8 Bremisches Datenschutzgesetz (BrDSG) für die "Datenverarbeitung im Auftrag".

Dies betrifft zunächst die Vertragsgestaltung: Weil das beauftragte RZV nicht dem BrDSG, sondern dem kirchlichen Datenschutzrecht unterliegt, ist eine Vertragsklausel erforderlich, wonach sich das RZV sowohl den materiellen Bestimmungen des BrDSG als auch meiner Kontrolle unterwirft. Da das RZV wegen der Nichtanwendbarkeit des BDSG keiner Meldepflicht im Sinne von § 32 Bundesdatenschutzgesetz (BDSG) unterliegt, habe ich die Vorlage einer entsprechenden Bescheinigung des bei der EKD Hannover eingerichteten sog. "Bewertungsausschusses" verlangt.

Des weiteren habe ich darauf hingewiesen, daß der Auftraggeber, d.h. der Senator für Gesundheit, Jugend und Soziales bzw. die Krankenhäuser, Weisungen über die Verarbeitung personenbezogener Daten zu erteilen und sicherzustellen hat, daß die Verarbeitung nur im Rahmen dieser Weisungen vorgenommen wird. Insbesondere hat der Auftraggeber im einzelnen und abschließend per Anweisung festzulegen, welche Personaldaten dem RZV zur Verfügung zu stellen sind und welche Auswertungen dort vorgenommen werden dürfen. Außerdem wurden Vertragsstrafen für Verletzungen der Datenschutzbestimmungen bzw. der vertraglichen Weisungen vorgesehen. Für wichtig hielt ich auch, die Befugnis des Auftraggebers zur fristlosen Kündigung bei Datenschutzverstößen des Auftragnehmers zu vereinbaren. Nach Beendigung des Auftrages sind alle für die Krankenhäuser im RZV gespeicherten Daten an diese herauszugeben oder, soweit dieses aus technischen Gründen nicht möglich ist, zu löschen.

8.1.2. Technisch-organisatorisches Sicherungskonzept

Zusätzlich zu diesen vertraglichen Regelungen habe ich die Vorlage eines Datenschutz- und Sicherungskonzeptes verlangt, aus dem hervorgeht,

- welche Systemgestaltung in den Krankenhäusern zur Anwendung dieses Verfahrens vorgesehen ist und welche Datenflüsse zwischen den einzelnen Komponenten des Systems geplant sind,
- wie die Daten zwischen zentraler Speicherung im Rechenzentrum und dezentraler Haltung in den Krankenhäusern verteilt werden sollen,
- welche Maßnahmen zum Zugriffsschutz vor Ort in den Krankenhäusern, aber auch in der Anwendungssoftware vorgesehen sind,
- welche Möglichkeiten der differenzierten Verteilung von Benutzerrechten bestehen,
- wie und durch wen die Systemverwaltung erfolgt, insbesondere ob ein Vier-Augen-Prinzip vorgesehen ist,
- welche Protokollierungsmöglichkeiten (auf dem Hintergrundsrechner ebenso wie auf den PCs vor Ort) bestehen und wie die Protokolldateien gegen unerlaubte Auswertungen geschützt werden können,
- welche Maßnahmen zur Sicherung der Übertragung der Daten zwischen PC und Host vorgesehen sind und
- ob und wenn ja, welche Regelungen betreffend einer Hard- und/oder Softwarewartung vorgesehen sind.

Inzwischen wurde auch zwischen den kommunalen Krankenhäusern und den Personalräten eine Dienstvereinbarung zum Personalabrechnungsverfahren KIDICAP 2000 sowie der zugehörigen Personalwirtschafts- und -auswertungsmodule abgeschlossen. Das Datenschutzkonzept ist ebenso als Anlage zu dieser Dienstvereinbarung vorgesehen wie die Auflistung der zugelassenen Auswertungen, das Geräteverzeichnis, die Protokolldokumentationen, die Listenmuster über gespeicherte Daten, das Programmverzeichnis mit Kurzerläuterungen sowie die Schnittstellen.

Inzwischen liegt ein Datenschutzkonzept vor, in dem für die Krankenhäuser/Anwender die Verantwortlichkeiten für den internen Datenschutzbeauftragten, den systemverantwortlichen DV-Koordinator und die Nutzungsberechtigten festgelegt werden. Des weiteren legt ein Stufenkonzept die Schutzkategorien fest. Außerdem sollen Hard- und Software in einer Anlage des Datenschutzkonzeptes festgelegt werden. Dem Datenschutzkonzept werden der Vertrag zwischen dem Krankenhaus und dem RZV sowie das hausinterne Datenschutzkonzept des RZV ebenfalls beigefügt.

Dieses Gesamtkonzept sowie die Dienstvereinbarung entsprechen insgesamt den datenschutzrechtlichen Anforderungen. Allerdings müssen für einen datenschutzgerechten Einsatz von KIDICAP auch alle vorgesehenen Anlagen, so z.B. Katalog der zu verarbeitenden Daten, der Datenübermittlungen und der Auswertungen, vorliegen.

8.2. PUMA - DV-Unterstützung von Personalkostenbugdetierung und Personalverwaltung

8.2.1. Dezentralisierung der Personal-DV

Das Haushaltsgesetz 1995 sieht die sog. Personalkostenbudgetierung für die senatorischen und nachgeordneten Dienststellen vor. Darüber hinaus soll auch die bisher von der SKP zentral erledigte Personalsachbearbeitung teilweise auf die Dienststellen verlagert und dort mit DV-Kapazitäten und mit einem einheitlichen Programm unterstützt werden. Für beide Aufgaben soll das integrierte Verfahren PUMA (Personalverwaltungs- und management) eingesetzt werden. Es basiert auf einer Zentraldatei, auf die die örtlichen Dienststellen im jeweils dafür erforderlichen Umfang zugreifen dürfen.

Gegen dieses Konzept der Dezentralisierung der Personaldatenverarbeitung bestehen keine prinzipiellen datenschutzrechtlichen Bedenken. Insbesondere kann die Einheitlichkeit der Anwendung und des vorgesehenen Umfangs der Datenverarbeitung dazu beitragen, den bisherigen "Wildwuchs" an unterschiedlichen Anwendungen und Dateien in den Personalstellen einzuschränken. Einen weiteren Pluspunkt kann eine mit der einheitlichen Anwendung verbundene Verbesserung der Datenschutzkontrolle bedeuten.

Als Zwecke für den Einsatz von PUMA werden lediglich ganz allgemein "Personalsachbearbeitung" und "Personalkostenhochrechnung" genannt, wobei letztere die Steuerung des Beschäftigungsvolumens und der Stellenauslastung zum Zwecke des Personalcontrolling unterstützen soll. Um festzulegen, welche Daten der zentralen Datenbank für welche dieser Zwecke bzw. Benutzergruppen zur Verfügung gestellt werden sollen, bedarf es eines entsprechend aufgabenbezogenen Datenkatalogs, der inzwischen vorliegt.

Die SKP hat den Dienststellen zum Zwecke der Personalkostenbugdetierung Besoldungsdaten der Beschäftigten übermittelt. Weil dies bisher keine originäre Aufgabe der personalverwaltenden Stellen war, hatte ich gefordert, für diese Übermittlung eine gesetzliche Grundlage zu schaffen. Die neue, unter Zeitdruck formulierte Vorschrift des § 13 Abs. 2 Haushaltsgesetz 1995, wonach die Daten den Dienststellen "zur eigenen automatisierten Verwaltung der Personalkosten" zur Verfügung gestellt werden, enthält allerdings nur eine ungenaue Definition des Verarbeitungszwecks. Der Text der Rechtsgrundlage muß sich in Zukunft an der Vorgabe des § 93 Bremisches Beamtengesetz (BremBG) orientieren und den Verarbeitungsrahmen präziser benennen.

Ein ungeklärtes Problem stellt der vorgesehene Datenaustausch zwischen der Personalstelle und der Haushaltsstelle innerhalb der Dienststellen dar. Nach meiner Einschätzung reicht es zur Budgetberechnung aus, wenn der Haushaltsstelle lediglich ohne Bekanntgabe von Personalaktendaten von der Personalstelle mitgeteilt wird, welche konkreten Personalbewegungen anstehen. Die Konzeption der SKP, wonach die Personalkostenbugdetierung als integrierte Aufgabe sowohl der Haushalts- als auch der Personalstelle anzusehen ist, darf nicht zu unzulässigen Offenbarungen von Mitarbeiterdaten führen.

8.2.2. Sicherungsdefizite der Netzsoftware

Die für das PUMA-Projekt vorgesehenen Netzbetriebssysteme "Windows für Workgroups" und "Windows NT, Version 3.5" erfüllen nicht die datenschutzrechtlichen und technischen Anforderungen für die Verarbeitung von Personaldaten. So können insbesondere die Protokolldaten gegenüber der Systemverwaltung (Netzadministration) nicht abgeschottet werden. Damit besteht das Risiko einer mißbräuchlichen Einsicht in die Protokolldaten und ihrer Manipulation durch die Administratoren. Auch sind die Möglichkeiten der Zugriffsorganisation und der Benutzerverwaltung nicht ausreichend.

Offen sind auch Fragen zu den Befugnissen und zur Kontrolle der Datenbankadministration: Neben dem einheitlichen Einsatz von PUMA sollen für den Fall, daß Dienststellen spezifische zusätzliche Bearbeitungs- oder Auswertungsmöglichkeiten benötigen, diese von einem eigens dazu berechtigten Datenbankadministrator eingebaut werden. Die Voraussetzungen derartiger Programmerweiterungen müssen festgelegt werden. Nach § 22 Abs. 2 BrDSG bedarf die automatisierte Verarbeitung von Personaldaten der Zustimmung der obersten Dienstbehörde, also der SKP. Demnach halte ich es für richtig, die Datenbankadministration der SKP zentral zuzuordnen, um nicht auszuschließende unzulässige Manipulationen dezentraler behördeneigener Administratoren zu verhindern.

Die SKP hat sich bereit erklärt, meine Anforderungen in die weiteren Überlegungen einzubeziehen und mich bei der weiteren Umsetzung rechtzeitig zu beteiligen.

8.3. Beihilfe - Zentralisierung der Berechnung

8.3.1. Wegfall des "Instanzenwegs"

Das neue Personalaktenrecht (§ 93b des Bremischen Beamtengesetzes; zu den Einzelheiten der Neuregelung vgl. 16. JB, Ziff. 4.3) sieht vor, daß Unterlagen über Beihilfen stets als

Teilakten zu führen sind und die Beihilfeakte von der übrigen Personalakte getrennt aufzubewahren ist. Außerdem soll die Beihilfe in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden; Zugang sollen nur Beschäftigte dieser Organisationseinheit haben.

Diese Neuregelung hatte zur Folge, daß die Senatskommission für das Personalwesen (SKP) das bisherige Beihilfeverfahren dieser Vorgabe anpassen mußte. Bisher war zwar schon eine separate Organisationseinheit für die Beihilfebearbeitung zuständig, allerdings wurden die eigentlichen Beihilfeakten bei den Beschäftigungsbehörden geführt. Nach dem bisherigen Verfahren übergab ein Beihilfeantragsteller den verschlossenen Umschlag an die Personalstelle; diese wiederum leitete den Beihilfeantrag mit der Beihilfeakte an die SKP weiter. Nach Abschluß der Bearbeitung leitete die Beihilfestelle der SKP den Bescheid einschließlich der zurückgegebenen ärztlichen Unterlagen direkt an den Betroffenen und gab die Beihilfeakte mit einer Kopie des Bescheides an die Beschäftigungsbehörde zurück.

Im Zuge der Neuordnung und insbesondere der Automatisierung des Beihilfeverfahrens (BABSY) entfällt der bisherige "Instanzenweg", in dem die Anspruchsberechtigten nunmehr ihre Beihilfeanträge unmittelbar bei der SKP ohne Umwege über die Personalstellen einreichen. Dies kann über Behördenpost, durch Zustellung über die Bundespost oder durch direkte Abgabe des Antrages bei der SKP erfolgen.

Nach Bearbeitung in der Beihilfestelle werden die Durchschriften der Beihilfebescheide chronologisch in der Beihilfestelle entsprechend den gesetzlichen Bestimmungen fünf Jahre aufbewahrt. Im Zuge der automatisierten Verarbeitung bleiben die Grunddaten des Beihilfebescheides (Name des Anspruchsberechtigten und Datum des Bescheides) als Suchbegriff für das Heraussuchen des betreffenden Bescheides gespeichert, falls ein Anspruchsberechtigter Akteneinsicht begehrt.

Zum Zwecke der Auszahlung der Beihilfe ist die Beihilfestelle an das Personalabrechnungssystem PAADIS angeschlossen. Dabei können die Beihilfesachbearbeiter nur einige Daten aus PAADIS einsehen, eine Änderung dieser Daten ist nicht möglich. Eine Übernahme der Daten aus PAADIS oder aus BABSY auf die Festplatte des Rechners der einzelnen Sachbearbeiter soll nicht möglich sein. Hierzu seien entsprechende Abschottungen programmtechnisch vorgenommen worden.

8.3.2. Einhaltung des Trennungsgebots in der SKP

Nach meinen Feststellungen wurden die Umschläge der eingehenden Beihilfeanträge, in denen sich das Antragsformular sowie in der Regel ein weiterer die einzelnen Arztrechnungen enthaltender verschlossener Umschlag befinden, in der zentralen Poststelle der SKP geöffnet. Danach wurde der Beihilfeantrag mit einem Eingangsstempel versehen und zusammen mit dem die Arztunterlagen enthaltenden verschlossenen Umschlag an die Beihilfestelle weitergeleitet.

Ich habe die SKP auf das Trennungsgebot nach § 93 b BremBG hingewiesen. Dieses beinhaltet auch, daß Stellen außerhalb der Beihilfestelle, insbesondere die zentrale Poststelle, keine Einblicksmöglichkeit in Beihilfeunterlagen haben dürfen. Durch organisatorische Maßnahmen ist sicherzustellen, daß erst in der Beihilfestelle selbst die eingehende Post der Antragsteller geöffnet wird.

Die SKP hat mir inzwischen mitgeteilt, daß die Anträge jetzt von der zentralen Poststelle direkt und ungeöffnet an die zuständige Organisationseinheit weitergeleitet werden.

8.4. Neue Personalaktenrichtlinien

Die Senatskommission für das Personalwesen (SKP) hat mir den Entwurf von Richtlinien über die Führung von Personalakten bzw. die Verarbeitung von Personalaktendaten vorgelegt. Neue Richtlinien sind aufgrund des Gesetzes zur Änderung dienstrechtlicher Vorschriften vom 16.03.1994 (vgl. Brem.GBl. 1994, S. 107 ; § 93a Abs. 2 Satz 4) notwendig geworden.

In meiner Stellungnahme habe ich der SKP eine Reihe von Änderungsvorschlägen unterbreitet. Zu den wichtigsten Punkten aus meiner Sicht gehören folgende Regelungen:

- Der Entwurf enthält den mißverständlichen Hinweis, der Datenfluß zwischen Grund- und Teilakten sowie Nebenakten sei keine Datenübermittlung, sondern lediglich eine Informationsverteilung zwischen personalverwaltenden Behörden. Dies entbindet jedoch nicht von der Beachtung des auch und gerade im Personalaktenrecht bedeutsamen Grundsatzes, wonach Mitarbeiterdaten auch zwischen Stellen mit Aufgaben der Personaladministration nur im jeweils für die Sachbearbeitung erforderlichen Umfang weitergegeben werden dürfen.

- Die Absicht, Gesundheitszeugnisse und ärztliche Untersuchungsergebnisse, die nicht allein dem Zwecke der Eingehung eines Dienstverhältnisses dienen, in einem verschlossenen Umschlag zur Personalakte zu nehmen, scheint im Widerspruch zu einer anderen beabsichtigten Regelung im Entwurf zu stehen, wonach ärztliche und psychologische Untersuchungen und Tests sowie ärztliche Unterlagen überhaupt nicht Bestandteil der Personalakte sind.

- Der im Entwurf vorgesehene Grundsatz, wonach die Personalakte ein möglichst vollständiges Bild über den beruflichen Werdegang und insoweit über die Persönlichkeit des Betroffenen geben soll, stammt aus "vordatenschutzrechtlichen" Zeiten des Beamtenrechts und relativiert das jetzt in § 93 Satz 1 BremBG enthaltene Prinzip, daß nur die für das Dienstverhälntis relevanten Angaben zu erheben bzw. aufzubewahren sind.

- Der Vorschlag der SKP sah vor, daß Personenstandsurkunden (vom Scheidungsurteil nur Urteilstenor, Regelungen über Unterhalt und Versorgungsausgleich o. ä.) in die Grundakte aufgenommen werden, obwohl diese Unterlagen für die laufenden Aufgaben der Personalstellen in den Beschäftigungsbehörden nicht erforderlich sind. Die Grundakte wird jedoch häufig im Rahmen von Auswahl- und Bewerbungsverfahren eingesehen. In mir bekannten Einzelfällen sind Hinweise auf Scheidungen bei Auswahlverfahren berücksichtigt worden. Ich habe daher angeregt, Personenstandsurkunden in die Teilakte "Besoldungsakte" zu nehmen, auch weil diese Daten in erster Linie besoldungsrelevant sind. Zu überprüfen ist m.E. auch die Notwendigkeit der Aufnahme von Dienstunfallunterlagen und Auszügen aus Kindergeldvorgängen in die Grundakte.

- Nach dem Entwurf ist es Personalräten generell nicht gestattet, Personalvorgänge anzulegen. Hierzu habe dargelegt, daß diese Regelung nicht den Bestimmungen des Bremischen Personalvertretungsgesetzes (BremPVG) entspricht, weil der Personalrat anläßlich eines konkreten Mitbestimmungsverfahrens zumindest die hierzu geführte Korrespondenz aufbewahren muß.

Die SKP hat mir mitgeteilt, sie habe meine Bedenken und Anregungen, die ich in diesem Abschnitt nur teilweise aufgeführt habe, im wesentlichen übernommen. Sobald die hausinterne Abstimmung abgeschlossen sei, werde sie mir den überarbeiteten Entwurf zur Prüfung vorlegen.

8.5. Fall: Die gestoppte Stasi-Überprüfung

Aufgrund einer Eingabe und durch Pressemeldungen hatte ich erfahren, daß der Senator für Kultur und Ausländerintegration aufgrund von Gerüchten über mögliche Stasi-Kontakte von Mitarbeitern entschieden hatte, für alle leitenden Beschäftigten eine Überprüfung durch die Gauck-Behörde in Berlin in die Wege zu leiten. Die Betroffenen wurden gebeten, einen hausinternen Fragebogen auszufüllen und ihn unterschrieben an die Verwaltungsleitung weiterzugeben.

Nachdem der Personalrat interveniert hatte, stoppte die Hausspitze die Aktion. Außerdem stellte sich heraus, daß ohnehin nur die Senatskommission für das Personalwesen (SKP) als oberste Dienstbehörde für die Einleitung derartiger Verfahren zuständig gewesen wäre.

Ich habe daraufhin den Senator für Kultur und Ausländerintegration aufgefordert, die Fragebögen, die bereits ausgefüllt und an die Dienststellenleitung weitergegeben worden waren, unverzüglich zu vernichten. Dieser Löschungsverpflichtung wegen unzulässiger Datenerhebung ist die senatorische Behörde nachgekommen.

8.6. Fall: Adoptionsgeheimnis beim Kindergeld

Anfang des Jahres 1994 erreichten mich viele Anrufe von bremischen Bediensteten, die Probleme mit dem neuen Erfassungsbogen zur Überprüfung des Kindergeldanspruchs nach dem 1. Gesetz zur Umsetzung des Spar-, Konsolidierungs- und Wachstumsprogramms (1. SKWPG) hatten. Dieser vom Bundesministerium des Inneren entwickelte und bundesweit eingesetzte Fragebogen enthielt bei der Angabe des Kindschaftsverhältnisses ausdrücklich auch die Rubrik "Adoptivkind".

Ich habe sofort nach Bekanntwerden die Senatskommission für das Personalwesen (SKP) in ihrer Eigenschaft als Kindergeldstelle der Beschäftigten des bremischen öffentlichen Dienstes darauf hingewiesen, daß eine derartige Angabe aufgrund der rechtlichen Gleichstellung des Adoptivkindes aufgrund § 1754 BGB nicht erforderlich ist und außerdem gegen das Ausforschungsverbot nach § 1758 BGB verstoßen wird.

Aufgrund dieser Rechtslage habe ich die SKP gebeten, umgehend durch Änderung des Fragebogens diese unzulässige Differenzierung der Kindschaftsverhältnisse zu beenden. Außerdem habe ich verlangt, alle Fragebögen, die bis dahin bereits ausgefüllt zurückgegeben worden waren, daraufhin durchzusehen, ob Eltern die Rubrik "Adoptivkind" bereits ausgefüllt hatten. Diese Fragebögen sollten unverzüglich vernichtet und den Betroffenen neue, geänderte Vordrucke zugesandt werden. Außerdem habe ich dringend gebeten, öffentlich über die Medien oder mit Maßnahmen wie Rundschreiben o.ä. alle Beschäftigten, die den Antrag noch nicht gestellt hatten, auf die unzulässige Rubrik hinzuweisen.

Die SKP hat zügig reagiert und die Dienststellen gebeten, alle bereits vorliegenden oder eingehenden ausgefüllten Vordrucke auf den Eintrag "Adoptivkind" durchzusehen und diese ggf. mit der Bitte an die Antragsteller zurückzugeben, einen neuen Vordruck mit der Eintragung"leibliches Kind" abzugeben. Die bereits bei ihr eingegangenen Formulare hat die SKP nach ihren Angaben selbst kontrolliert.

8.7. Prüfungsergebnisse

8.7.1. Telefonanlagen

8.7.1.1. Gesprächsdatenerfassung

Im Berichtszeitraum habe ich "vor Ort" die Telefonanlagen von drei bremischen Dienststellen im Hinblick auf Art und Umfang der Gesprächsdatenerfassung und -verarbeitung geprüft. Zwei Kontrollen wurden ohne besondere Veranlassung durchgeführt, die dritte Prüfung war durch eine Bürgereingabe bedingt.

Beim Telefonsystem der Universität Bremen stellte ich nur drei kleinere Mängel fest, deren Beseitigung teilweise bereits erfolgt und teilweise verbindlich zugesichert ist.

Auch die Prüfung einer Telefonanlage des zentralen Bremer Berhördennetzes ergab zu dem Komplex Gebührendatenerfassung und -verarbeitung keine grundsätzlichen Beanstandungen. Die BreKom hat mir für die im Frühjahr 1995 geplante Einführung eines neuen Netzwerkmanagementsystems (DMS) die rechtzeitige Beteiligung zugesichert; erste Informationen hierzu habe ich bereits erhalten.

8.7.1.2. Nutzung zusätzlicher Leistungsmerkmale

Anläßlich dieser Prüfung stellte ich allerdings fest, daß die BreKom Endgeräte installiert hatte, die Leistungsmerkmale bieten, die nicht in den Anlagen 1a und 1b zur Dienstvereinbarung über den Betrieb und die Nutzung von Telekommunikationsanlagen (Fern-

sprechanlagen) (DV-Fernsprechen) enthalten sind. Hierzu gehören insbesondere die Funktionen "Lauthören" und "Freisprechen".

Dies wirft die Frage auf, inwieweit sich die Festlegungen in der "DV-Fernsprechen" nur auf die zentral von der Anlage bereitgestellten Leistungsmerkmale beziehen oder auch die zur Anlage gehörenden Endgeräte einschließen. Für die letztere Auffassung spricht, daß nach § 3 Nr. 1 der Dienstvereinbarung die Endgeräte zu TK-Anlagen gehören und nach § 5 Nr. 4 angestrebt werden soll, die technische Realisierung von Leistungsmerkmalen von der Zentraleinheit in die Endgeräte zu verlagern. Ich empfehle daher, falls der Einsatz bisher nicht vorgesehener Gerätefunktionen gewünscht wird, die Anlagen zu § 5 Nrn. 1 und 2 der Dienstvereinbarung fortzuschreiben.

8.7.1.3. Persönliche Kennummern (PINs)

Bei der Überprüfung der Abrechnungspraxis für die Privatgespräche bei der Wasserschutzpolizei Bremerhaven ging es vor allem um die sichere Zuordnung der Telefonate bei Apparaten, die von mehreren Bediensteten genutzt werden. Im Herbst 1993 wurde die neue Telefon- und Einsatzzentrale - eine Siemens HICOM - von der BreKom (damals FTA) in Betrieb genommen. Bereits im Vorfeld hatte ich zu diesem Zweck die Einrichtung von PIN-Nummern angeregt. Diese Anregung ist auch nach mehreren Interventionen nicht umgesetzt worden. Statt dessen wurde ein mit der Dienstvereinbarung Fernsprechen nicht zu vereinbarendes Verfahren mit Gesprächsnachweislisten praktiziert, obwohl die BreKom mit dem Bereitstellungspreis angesichts der hohen Zahl der pro Anlage einzurichtenden PINs sehr entgegengekommen ist. Inzwischen wurde das Abrechnungsverfahren immerhin dahingehend geändert, daß die Nachweislisten jedenfalls weder die Vorwahl noch Teile der angerufenen Rufnummern ausweisen.

Ich bleibe allerdings bei meiner Ansicht, daß generell die einfachste und gleichzeitig datenschutzfreundlichste Lösung für von mehreren Teilnehmern genutzte Apparate die Einrichtung persönlicher Kennummern (PINs) ist. Dies minimiert zum einen den Verwaltungsaufwand für die Gesprächsabrechnung, zum anderen den Umfang der notwendigen Telefondatenregistrierung. Im Frühjahr 1995 soll in einem weiteren Gespräch anhand der bis dahin gewonnen Erfahrungen entschieden werden, ob das modifizierte Listenverfahren beibehalten wird oder doch PINs eingerichtet werden.

8.7.2. Einhaltung der PC-Richtlinien

Bei einem Kontrollbesuch in der SKP habe ich in mehreren Organisationseinheiten insgesamt 14 mit PC ausgestattete Arbeitsplätze überprüft. Hierbei mußte ich erhebliche Mängel und Versäumnisse feststellen, die darauf schließen lassen, daß die einschlägigen gesetzlichen Bestimmungen ebenso wie die von der SKP selbst herausgegebenen Richtlinien für den Datenschutz am Arbeitsplatz nicht ausreichend beachtet werden. Ich vermute allerdings, daß sich vergleichbare Ergebnisse auch in zahlreichen anderen Dienststellen ergeben würden.

Der SKP obliegt die Koordination der Personalverwaltung und -wirtschaft in der bremischen Verwaltung. Sie war bisher z.B. an sämtlichen Personaleinstellungen beteiligt, prüft und entscheidet über Höhergruppierungen und Stellenbewertungen und ist zuständig für die Besoldung, Versorgung, Gehalts- und Lohnzahlung. Diese Aufgaben können in der Regel nur mit Hilfe automatisierter Verarbeitung personenbezogener Daten der Beschäftigten effizient erfüllt werden. Die Rechtsgrundlagen hierzu ergeben sich aus § 22 Abs. 1 Bremisches Datenschutzgesetz (BrDSG) i.V.m. §§ 93 ff. Bremisches Beamtengesetz (BremBG).

In den letzten Jahren setzt die SKP zunehmend autonome Arbeitsplatzrechner (PC) ein. Ich war an vielen Antragsverfahren auch zu diesen PCs der SKP aufgrund der ADV-Richtlinien beteiligt und habe dabei zu den zu treffenden organisatorischen und technischen Maßnahmen nach § 6 Abs. 2 BrDSG Stellung genommen (vgl. auch die Richtlinien für den Datenschutz am Arbeitsplatz vom 07. August 1990, RiLiDS, Brem.ABl. S. 221). Vielfach waren bereits in den Anträgen selbst Datensicherungsmaßnahmen angegeben und damit zugesagt.

Die PC-Prüfung stellte folgende Mängel fest:

- Ein nach § 7 Abs. 3 BrDSG zu führendes Geräteverzeichnis lag nach Auskunft der SKP nicht vor.
- Es waren keine Systemakten angelegt worden, obwohl dies nach Nr. 9 der RiLiDS für jeden PC vorgeschrieben ist.
- Die nach § 7 Abs. 1 BrDSG vorgesehenen Dateibeschreibungen fehlten fast durchgängig. Nur in einigen Fällen lag der DV-Koordinatorin der SKP ein Entwurf des Datenschutzkonzeptes mit den technischen und organisatorischen Maßnahmen vor.
- Obwohl nach Nr. 2.1 der RiLi DS ein Paßwortwechsel alle 90 Tage stattfinden muß, wurde dieser auf den meisten der überprüften PC nicht vorgenommen. Außerdem wurde entgegen dieser Vorschrift in fast allen Fällen, in denen der PC mindestens zwei Benutzungsberechtigten zur Verfügung steht, ein gemeinsames Paßwort genutzt.
- In drei Fällen hatte die SKP im Rahmen des PC-Antragsverfahrens angegeben, die Sicherungssoftware "Safe-Guard" einsetzen zu wollen. Dieses Zugriffsschutzprogramm war jedoch nicht installiert.
- In der Mehrzahl der Fälle erfolgte keine Löschung der Daten und Texte, obwohl sie nicht mehr benötigt wurden und die rechtlichen Löschvoraussetzungen vorlagen.

Ich habe in diesem Falle noch einmal von einer förmlichen Beanstandung abgesehen, jedoch mit Nachdruck gefordert, die in meinem Prüfbericht im einzelnen aufgeführten Mängel so bald wie möglich abzustellen.

Inzwischen liegt die Stellungnahme der SKP vor. Danach sind alle Organisationseinheiten aufgefordert worden, die Systemakten der Allgemeinen Verwaltung vorzulegen, um sie zu vervollständigen. Im gleichen Arbeitsgang soll das Geräteverzeichnis aufgestellt werden. Auch wird im einzelnen auf die überprüften PCs eingegangen. Ich behalte mir eine Nachprüfung zu gegeben Zeit vor.

8.7.3. Unzulässige Personalnebenakte

Ein Beschäftigter der Oberfinanzdirektion Bremen (OFD) wandte sich dagegen, daß sein Referatsleiter längere Zeit eine Personalnebenakte über ihn führte. Der Referatsleiter habe ihm eine schriftliche Abmahnung erteilt und darauf hingewiesen, daß diese Abmahnung in eine bei ihm geführte Personalnebenakte aufgenommen worden sei. Ich habe aufgrund dessen das Referat aufgesucht und festgestellt, daß sich in einem Zimmer einer Mitarbeiterin des Referatsleiters ein geöffneter Stahlschrank befand, der mehrere Ordner über Personalangelegenheiten und Arbeitszeitnachweise enthielt. In den Ordnern befanden sich neben der vorgenannten Abmahnung auch Duplikate von Urlaubsanträgen und -genehmigungen, Einstellungs- und Höhergruppierungsvorschläge und Beurteilungen und Ablehnungen von Bewerbern. Außerdem wurden sämtliche schriftlichen Arbeitszeitnachweise der zehn Angehörigen des Referats seit 1988 fortlaufend geführt.

Ich habe die OFD um ihr Eingreifen gebeten unter Hinweis auf die einschlägigen Vorschriften zum Personalaktenrecht, insbesondere das Verbot der doppelten Personalaktenführung, und verlangt, daß die personalaktenrelevanten Unterlagen aus den Ordnern den jeweiligen Personalakten einschließlich der Beiakten zugeführt werden müssen.

Auch die Aufbewahrung aller Arbeitsnachweise sämtlicher Referatsmitarbeiter seit 1988 im Referat verstößt gegen die Grundsätze für die gleitende Arbeitszeit. Danach haben die Vorgesetzten nämlich die Aufgabe, die Richtigkeit der Zeiterfassung stichprobenweise zu überprüfen und die Einhaltung der Dienstvereinbarung zu überwachen. Außerdem sind die Zeiterfassungsnachweise von den Betroffenen lediglich 6 Monate aufzubewahren. Ich habe daher die OFD gebeten, den Referatsleiter zu veranlassen, sämtliche Arbeitszeitnachweise, die diese Aufbewahrungsfrist übersteigen, unverzüglich zu vernichten und die noch aufzubewahrenden Arbeitszeitnachweise an die Beschäftigten zu geben.

Um zu ermitteln, ob die in diesem Referat festgestellte Praxis auch in den übrigen Organisationseinheiten üblich war, habe ich die OFD um eine entsprechende hausinterne Überprüfung gebeten.

Die OFD hat mir erklärt, aufgrund der von mir zurecht beanstandeten Führung von Personalakten in einem Referat habe sie zunächst bei allen Referenten nachgefragt, ob ähnliche Vorgänge dort gesammelt werden. Das sei nicht der Fall gewesen. Inzwischen seien sämtliche Duplikate von personalaktenrelevanten Unterlagen vernichtet und die noch aufzubewahrenden Arbeitszeitnachweise zurückgegeben worden. Außerdem hat die OFD in einem Rundschreiben an die Abteilungsleiter und Referenten auf die Einhaltung der einschlägigen Vorschriften zum Personalaktenrecht und darauf hingewiesen, daß es den Vorgesetzten untersagt ist, personalaktenrelevante Unterlagen im Original oder als Duplikat bei sich aufzubewahren. Weiter hat die OFD darauf hingewiesen, daß Abmahnungen als mißbilligende Äußerungen nur durch den Dienstvorgesetzten, nicht aber durch den Fachvorgesetzten wirksam ausgesprochen werden dürfen. Insgesamt hat die OFD auf diesen offensichtlich einmaligen Vorfall in ihrem Hause zügig und umfassend reagiert.

9. Inneres

9.1. Polizei

9.1.1. Verbrechensbekämpfungsgesetz: Vermischung von Strafverfolgung und nachrichtendienstlicher Auslandsaufklärung

9.1.1.1. Der Regierungsentwurf

Nachdem noch Ende 1993 davon die Rede war, die Regierungskoalition beabsichtige, den Verfassungsschutz an der Bekämpfung organisierter Kriminalität zu beteiligen - er solle ihre Strukturen und Entwicklung im Vorfeld beobachten und bei Telefonabhörmaßnahmen eingesetzt werden - wurde dieses Projekt 1994 nicht weiter verfolgt. Was im Inland aus politischen Umständen - nicht zuletzt wegen der Pattsituation im Bundesrat - wie auch aus verfassungsrechtlichen Gesichtspunkten nicht durchsetzbar war, wurde für die Kontrolle von Telefongesprächen mit dem Ausland realisiert. Der von den Fraktionen der CDU/CSU und FDP eingebrachte Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches, der Strafprozeßordnung und anderer Gesetze (bezeichnet als Verbrechensbekämpfungsgesetz) wurde Ende Mai 1994 vom Bundestag angenommen und dem Bundesrat zugeleitet (vgl. Bundesrats-Drucks. 416/94).

Der Entwurf sah in Art. 12 vor, im Gesetz zu Art. 10 GG, dem sogenannten G10-Gesetz, die Befugnisse des Bundesnachrichtendienstes - die bisher auf die Gewinnung von Erkenntnissen über das Ausland von außen- und sicherheitspolitischer Bedeutung beschränkt waren - zu erweitern und ihn u. a. auch bei der Straftatenbekämpfung, insbesondere in den Bereichen Betäubungsmittel, Geldfälschung und Geldwäsche einzusetzen. Zu diesem Zweck wurde der BND zunächst im Entwurf und später auch im verabschiedeten Gesetz befugt, alle im und mit dem Ausland geführten sowie die über das Gebiet der Bundesrepublik durchgeleiteten, nicht leitungsgebunden geführten Telefongespräche abzuhören, aufzuzeichnen und nach gewissen Suchbegriffen technisch durchzurastern. Dabei gewonnene Erkenntnisse sollen den Verfassungsschutzbehörden des Bundes und der Länder, dem MAD, dem Zollkriminalinstitut, dem Bundesausfuhramt, den Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, den Polizeibehörden übermittelt werden.

Nicht Gesetz geworden ist der im Entwurf enthaltene Vorschlag, daß u. a. die Staatsanwaltschaft sich bei ihrer Aufgabenerfüllung der Hilfe des BND bedienen durfte. So war vorgesehen, daß die Staatsanwaltschaft von sich aus an den BND herantreten und von diesem verlangen konnte, bestimmte Suchbegriffe in seine Datenbanken aufzunehmen und den Fernmeldeverkehr auch mit diesen Suchbegriffen gezielt durchzurastern.

9.1.1.2. Datenschutz- und verfassungsrechtliche Kritik am Regierungsentwurf

Damit drohten das im Verfassungsrang stehende Trennungsgebot zwischen den Tätigkeiten von Polizei und Geheimdiensten in beide Richtungen aufgehoben und die Aufgaben und Befugnisse des BND erheblich erweitert zu werden. Die im G10-Gesetz für den BND getroffene Ausnahme vom Verfassungsgrundsatz der Telefonkontrolle nur im Einzelfall (sog. strategische Kontrolle nach dem "Staubsaugerprinzip") sollte erweitert werden, ohne daß bei der Normierung darauf geachtet worden wäre, daß eine den bisherigen gesetzlichen Tatbeständen äquivalente Gefährdung (z.B. die Gefahr eines bevorstehenden Angriffskriegs o.ä.) gegeben wäre.

Auch andere verfahrenssichernde Maßnahmen bei Abhörmaßnahmen, wie z.B. die Kontrolle der Datenverarbeitung durch den Bundesbeauftragten für den Datenschutz beim BND, sind vom Gesetzgeber nicht vorgesehen worden oder können, wie die Pflicht zur Benachrichtigung der Betroffenen, unterlaufen werden, indem der Inhalt der abgehörten Informationen zwar zur Kenntnis genommen, die Erkenntnisse aber vor Ablauf von drei Monaten vernichtet werden. Folgende Punkte des Entwurfs widersprachen eklatant datenschutzrechtlichen Grundsätzen:

- die vorübergehende Totalspeicherung aller Gespräche mit dem Ausland,
- die Rasterfahndung mit Suchbegriffen in allen Auslandsgesprächen,
- nicht ausreichende Rechtsweggarantien bzw. sonstige verfahrenssichernde Maßnahmen für die Betroffenen (auch im Inland),
- das Fehlen einer ausreichenden Datenschutzkontrolle,
- die erhebliche Erweiterung der Eingriffe in das Brief- und Postgeheimnis,
- die fehlende Erfolgskontrolle der bereits vorhandenen vergleichbaren Befugnisse und Maßnahmen.

9.1.1.3. Die Position der Datenschutzbeauftragten

Ich habe den Senator für Justiz und Verfassung auf meine verfassungs- und datenschutzrechtlichen Bedenken hingewiesen. Nachdem im Bundesrat das Verbrechensbekämpfungsgesetz abgelehnt worden war, wurde der Vermittlungsausschuß angerufen. Nachdem mir die Vorschläge einer Unterkommission des Vermittlungsausschusses vorlagen, habe ich mich erneut an den Senator für Justiz und Verfassung und an die Öffentlichkeit gewandt. In einer Presseerklärung habe ich zusammen mit den Datenschutzbeauftragten neun anderer Länder die Landesregierungen aufgefordert, im Vermittlungsausschuß den Formulierungen der Unterkommission nicht zuzustimmen. Danach sollte daran festgehalten werden, durch Abhörmaßnahmen gewonnene Informationen personenbezogen aufzubereiten und an die Strafverfolgungsbehörden weiterzuleiten.

Ich habe zusammen mit den Kollegen anderer Länder darauf hingewiesen, daß sich die vom BND praktizierte Fernmeldeaufklärung gerade nicht auf bestimmte Personengruppen beschränken läßt. Vielmehr wird, wie bei einer Rasterfahndung, unvermeidlich eine große Zahl von Unbeteiligten in Abhörmaßnahmen einbezogen. Damit wird aber im großen Umfang in das Fernmeldegeheimnis eingegriffen, das nicht nur durch Art. 10 GG, sondern auch international durch Art. 8 der Europäischen Menschenrechtskonvention und Art. 17 des Internationalen Paktes über bürgerliche Rechte besonders geschützt ist.

In unserer gemeinsamen Erklärung haben wir deutlich gemacht, daß diese Befugniserweiterung als entscheidender Schritt hin zur verfassungswidrigen Aufhebung des Trennungsgebotes zu werten war: Strafverfolgung durch die Polizei und Nachrichtensammlung durch Geheimdienste sind im demokratischen Verfassungsstaat prinzipiell unterschiedliche Aufgaben und müssen es bleiben. Wer die Datenauswertung durch Nachrichtendienste für die Strafverfolgung zuläßt, geht unüberschaubare Risiken für die rechtsstaatliche Transparenz und die richterliche Überprüfbarkeit in Strafverfahren ein.

9.1.1.4. Das Ergebnis

Trotz dieser Proteste hat der Vermittlungsausschuß die Ergebnisse der Unterkommission bestätigt. Im Ergebnis war aus datenschutzrechtlicher Sicht lediglich ein Teilerfolg zu verbuchen: Das Verbrechensbekämpfungsgesetz enthält nicht mehr die ursprüngliche Absicht (s.o. 9.1.1.1), daß der BND nach Angabe von Suchbegriffen durch die Staatsanwaltschaft die Auslandstelefongespräche durchzurastern verpflichtet ist. Eine gezielte Instrumentalisierung des BND für Zwecke der Strafverfolgung ist damit ausgeschlossen. Aus meiner Sicht bleibt allerdings das Risiko, daß der BND, soweit von der Staatsanwaltschaft entsprechende Wünsche geäußert werden, von sich aus Suchbegriffe in seine Datenbanken einstellen wird.

Die nach der Verabschiedung des Gesetzes terminierte Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigte in einer Entschließung (vgl. u. Ziff. 20.10) ihre Auffassung, bei dem Vollzug des Gesetzes sei darauf zu achten, daß nicht gezielt Informationen gesammelt werden, die vom Auftrag des BND nicht umfaßt werden. Die Konferenz forderte weiterhin die Beseitigung der für den Bundesbeauftragten für den Datenschutz bestehenden Kontrollücke bei Daten, die aus Abhörmaßnahmen stammen (vgl. § 24 Abs. 2 Satz 3 Nr. 1 BDSG). Das Verbrechensbekämpfungsgesetz wird im übrigen von einem Bürger mit einer Verfassungsbeschwerde angegriffen. Das Bundesverfassungsgericht hat im Rahmen seiner Prüfung alle Datenschutzbeauftragten um Stellungnahme gebeten. Ich werde mich gegenüber dem Bundesverfassungsgericht im o. a. Sinne äußern.

9.1.2. EUROPOL-Konvention: Gefährdung der Länderbefugnisse von Polizei und Datenschutz

9.1.2.1. Von der grenzüberschreitenden Zusammenarbeit zum zentralen europäischen Polizeiamt

Im Zuge der europäischen Integration und des Wegfalls der Binnengrenzen wird der Ruf nach einem intensiven grenzüberschreitenden Datenaustausch der nationalen Polizeibehörden immer lauter. Die EU-Mitgliedstaaten planen zur Institutionalisierung der polizeilichen Arbeit auf europäischer Ebene eine Zentralstelle. Als erster Schritt wurde eine gemeinsame Stelle zur Bekämpfung der Drogenkriminalität (EDU) in Den Haag eingerichtet, wohin zunächst von den Mitgliedstaaten Verbindungsbeamte entsandt wurden (vgl. 16. JB, Ziff. 2.4.3.2). Inzwischen wird ein Übereinkommen vorbereitet, mit dem ein europäisches Polizeiamt (genannt EUROPOL) installiert werden soll.

EUROPOL soll eine eigene speichernde Stelle werden, die in jedem Mitgliedstaat mit einer nationalen Stelle verbunden ist. Als Aufgaben von EUROPOL sind vorgesehen

- Informationen und Erkenntnisse zu sammeln, zusammenzustellen, zu analysieren und auszuwerten,
- die nationalen Dienststellen über die sie betreffenden Informationen und die in Erfahrung gebrachten Zusammenhänge von Straftaten unverzüglich zu unterrichten,
- Ermittlungen in den Mitgliedstaaten durch die Übermittlung aller sachdienlichen Informationen an die nationalen Stellen zu unterstützen und
- eine automatisiert geführte Sammlung von Informationsbeständen zu unterhalten, die sowohl von den nationale Behörden übermittelte als auch von EUROPOL selbst eingespeicherte Daten enthalten.

Entgegen der mir noch 1993 vorliegenden Konzeption (vgl.16. JB, Ziff. 2.4.3.2), nach der allein die entsandten Verbindungsbeamten Zugriff auf ihre jeweiligen nationalen Polizeiinformationssysteme haben sollten, ist nunmehr beabsichtigt, EUROPOL eigene Speicherungs- und Informationsverarbeitungsbefugnisse einzuräumen.

Mit der Einrichtung von EUROPOL wird, so die offizielle Begründung, das Ziel verfolgt, durch Zusammenarbeit die Effizienz der zuständigen Behörden in den Bereichen der Bekämpfung des Terrorismus, des illegalen Drogenhandels und sonstiger schwerwiegender Formen der internationalen Kriminalität zu verbessern. Voraussetzungen für die Zu-

ständigkeit von EUROPOL sollen sein, daß tatsächliche Anhaltspunkte für eine kriminelle Organisationsstruktur vorliegen und von den genannten Kriminalitätsformen zwei oder mehr Mitgliedstaaten in einer Weise betroffen sind, die aufgrund des Umfangs, der Bedeutung und der Folgen ein gemeinsames Vorgehen erfordern.

Neben der Anlieferung von Daten aus polizeilicher und strafverfolgender Tätigkeit durch die Polizeibehörden des Bundes und der Länder sind EUROPOL-eigene Dateien und eine eigene Datenschutzkontrollinstanz vorgesehen.

9.1.2.2. Bedenken gegen den Konventionsentwurf

9.1.2.2.1. Länderkompetenzen

Ich habe dem Senator für Inneres und Sport und dem Senator für Justiz und Verfassung bereits im Juni 1994 zu dem Entwurf eines EUROPOL-Übereinkommens meine datenschutzrechtlichen Bedenken mitgeteilt. Vor allem sind die Länderkompetenzen und -interessen in dem Entwurf nicht in genügendem Umfang berücksichtigt. Dies gilt sowohl für die Länderpolizeien als auch für die Rechte der Landesdatenschutzbeauftragten angesichts der Tatsache, daß in großem Maße auch Daten aus den Bundesländern in bei EUROPOL geführte Dateien hineinfließen. Soweit z.B. Daten bremischer Polizeidienststellen über das Informationssystem INPOL an EUROPOL weitergeleitet werden und dort durch die angeschlossenen Mitgliedstaaten genutzt werden können, muß sichergestellt sein, daß dieser Vorgang datenschutzrechtlich überprüft werden kann. Soweit in einem solchen Verfahren auch andere Datenschutzkontrollinstanzen zuständig sind, muß es Regelungen geben, auf deren Grundlage ich diese Kollegen um Mithilfe bitten und eine Überprüfung verlangen kann.

Anfang Oktober 1994 wurde dem Bundesrat der Entwurf für einen Rechtsakt des Rates der Europäischen Union über die Ausarbeitung des Übereinkommens über die Errichtung eines Europäischen Polizeiamtes (EUROPOL) zugeleitet (Bundesrats-Drucks. 909/94). Ich habe rechtzeitig zu den Beratungen im Rechts- und Innenausschuß des Bundesrates im November 1994 gegenüber dem Senator für Inneres und Sport und dem Senator für Justiz und Verfassung meine Stellungnahme abgegeben. Darin habe ich u.a. die Streichung der Regelung des Art. 2 Abs. 3 letzter Satz verlangt, der die Übermittlungen personenbezogener Daten an Nachrichten- und Geheimdienste vorsieht. Eine solche Regelung widerspräche dem in Deutschland geltenen verfassungsrechtlichen Trennungsgebot zwischen Polizei und Nachrichtendiensten. Auch fehlt für die Erstreckung des Regelungsbereichs der EUROPOL-Konvention auf die Zusammenarbeit mit Nachrichtendiensten jede europarechtliche Ermächtigung.

Weiter habe ich darauf hingewiesen, daß EUROPOL nicht allein Zwecken der Strafverfolgung dient, sondern auch präventivpolizeiliche Daten enthält. Die im Entwurf enthaltene Verpflichtung, die erforderlichen Maßnahmen zu treffen, um der nationalen Stelle - in Deutschland ist dafür das BKA vorgesehen - den Zugang zu den entsprechenden nationalen Daten zu verschaffen, ist nach meiner Auffassung verfassungsrechtlich bedenklich: Die Mitgliedstaaten können lediglich nach Maßgabe ihres jeweiligen Rechts die Zusammenarbeit der Polizeibehörden - in Deutschland also zwischen dem BKA und den Landespolizeibehörden - regeln. Einen entsprechenden Vorschlag habe ich unterbreitet.

In den gleichen Kontext gehört mein Hinweis, daß Speicherungen im Informationssystem von EUROPOL nur durch die Stellen veranlaßt werden können, die materiell für die zugrundeliegende Aufgabe der Strafverfolgung oder Gefahrenabwehr zuständig sind. Dies sind in der Bundesrepublik in aller Regel die Polizeien der Länder, das Bundeskriminalamt nur im Rahmen seiner Aufgabe als Bundespolizeibehörde nach § 5 BKA-Gesetz. Insoweit kann seine Zuständigkeit als "nationale Stelle" nur als organisatorische Verantwortung für das Funktionieren des Systems verstanden werden, nicht jedoch als alleinige inhaltliche Verantwortung für die Zulässigkeit und Erforderlichkeit der zu speichernden Daten. Diese Prinzipien finden sich in den vom Konventionsentwurf vorgesehenen Regelungen nicht wieder.

9.1.2.2.2. EUROPOL-eigene Datenverarbeitung

Weitere Kritikpunkte: Das zentrale datenschutzrechtliche Prinzip der klaren Verantwortlichkeit für die einzelnen Phasen der Datenverarbeitung wird im Konventionsentwurf nicht ausreichend beachtet. EUROPOL soll sowohl "eigene" wie von den Mitgliedstaaten als eigene übernommene Daten in Informationssystemen speichern und hieraus abrufen dürfen, obgleich diese Daten bei den Polizeibehörden der Mitgliedstaaten z.B. gelöscht sein können. EUROPOL soll berechtigt werden, Dateien zu führen, zu denen die Mitgliedstaaten zwar Daten anliefern müssen, zu denen sie selbst aber keinen unmittelbaren Zugang hätten.

Die Gefahr eines Mißbrauchs der EUROPOL-Daten, die insbesondere auch Dritte wie z.B. Zeugen betreffen, halte ich für so groß,daß die beabsichtigte 10-%-ige Protokollierung der Abfragen nicht ausreichend erscheint. Ich habe daher empfohlen, sich für eine Protokollierung aller Abrufe einzusetzen. Um eine effiziente Datenschutzkontrolle - gerade auch bei Beschwerden Betroffener - zu ermöglichen, habe ich dafür plädiert, die Löschfrist für die Protokolldaten von sechs Monaten auf ein Jahr heraufzusetzen. Weitere Kritikpunkte betreffen die Befugnis von EUROPOL, Informationen an Stellen außerhalb der EU zu übermitteln, sowie die Ausklammerung der Verwendung der Daten aus der Datenschutzkontrolle.

9.1.2.3. Reaktion des Bundesrats

Der Bundesrat hat die Bundesregierung aufgefordert, im Zuge der Verhandlungen der EUROPOL-Konvention darauf hinzuwirken, daß

- in Bundesstaaten neben der nationalen Zentralstelle auch anderen übergeordneten Stellen der Gliedstaaten nach Maßgabe des nationalen Rechts der Zugriff auf das Informationssystem von EUROPOL über die nationale Zentralstelle eingeräumt wird und
- der unmittelbare Informationsaustausch der übergeordneten Stellen der Gliedstaaten mit den Verbindungsbeamten bei EUROPOL zugelassen wird. Die Länderpolizeien sollen sich nicht erst um eine Vermittlung durch die zuständigen Beamten des BKA bemühen müssen, um an Informationen des Europäischen Polizeiamtes zu gelangen.

Weiterhin hat der Bundesrat darauf hingewiesen, daß ein großer Teil der von deutscher Seite in das Informationssystem EUROPOL eingestellten Daten von den Länderpolizeien erhoben wird. Da nach geltender Rechtslage für die Übermittlung dieser Daten Landesrecht maßgeblich sei, sei deshalb der datenschutzrechtlichen Verantwortung der Länder Rechnung zu tragen (vgl. Bundesrats-Drucks. 909/84 (Beschluß), Pkt. 7).

Das Bundesinnenministerium hat zwar seine Bereitschaft erklärt, im Innenverhältnis den Landeskriminalämtern einen online-Zugriff über das BKA als technischem Knotenpunkt auf das EUROPOL-Informationssystem zu eröffnen. Es sträubt sich aber, einen von den Justizministern geforderten Direktzugriff der Staatsanwaltschaften zuzulassen, weil das EUROPOL-Informationssystem nicht nur Strafverfolgungsdaten, sondern auch Daten aus präventivpolizeilicher Tätigkeit enthalte; aus der Sachleitungsbefugnis der Staatsanwaltschaft für einzelne Ermittlungsverfahren könne kein Recht auf Offenlegung der gesamten polizeilichen Informationssysteme abgeleitet werden. Im übrigen steht nach Auffassung des Bundesinnenministeriums dem Wunsch nach direkten Informationsbeziehungen zwischen den Landeskriminalämtern und den Verbindungsbeamten bei EUROPOL nichts im Wege.

9.1.2.4. Weiteres Verfahren

Die Verhandlungen über die EUROPOL-Konvention konnten unter deutschem Ratsvorsitz, d.h. im zweiten Halbjahr 1994, nicht abgeschlossen werden. Sie werden im ersten Halbjahr 1995 unter französischem Vorsitz weitergeführt. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer am 26./27.09.1994 gefaßten Entschließung (vgl. u. Ziff. 20.9) gefordert, daß die Regelungen der bisherigen Entwürfe überarbeitet und so präzise gefaßt werden, daß sie dem Grundsatz der Verhältnismäßig-

keit entsprechen. Dies gelte insbesondere für die Befugnisse zur europaweiten Speicherung von Daten unbeteiligter Personen. Die deutsche Seite müsse die Verantwortung der Länder für "ihre" Daten zumindest durch eine Protokollerklärung zur Konvention klarstellen.

9.1.3. Prüfergebnisse: Überlange Speicherung in Polizeidateien und Kriminalakten

9.1.3.1. Ausonderung von Altunterlagen

Auch in diesem Jahr hat sich wieder eine ganze Reihe von Bürgern an mich gewandt und um eine Überprüfung der in polizeilichen Informationssystemen und den zugehörigen Kriminalakten gespeicherten Daten gebeten. Nicht selten kommt es nach einer solchen Überprüfung zur Löschung entweder einzelner Daten oder auch des gesamten Datensatzes sowie zur Aussonderung und Vernichtung von Kriminalakten.

So konnte ich u. a. erreichen, daß Unterlagen aus einem Gewerbezulassungsverfahren aus der Kriminalakte entfernt wurden, die in Zeiten in die Akte gelangt waren, als das Stadt- und das Polizeiamt in Bremen noch nicht organisatorisch getrennt waren.

Akzeptiert wurde auch meine Bitte auf Aussonderung einer Geburtsurkunde und eines kompletten Scheidungsurteils. Auch diese beiden Unterlagen waren schon vor Jahren an das damals noch ungeteilte Stadt- und Polizeiamt übersandt und dann in der Kriminalakte abgeheftet worden.

9.1.3.2. Löschung von ed-Daten

Einzelne Eingaben von Bürgern sind mit überdurchschnittlichem Arbeitsaufwand für meine Mitarbeiter verbunden: So war in einem Fall ein Betroffener, wie sich herausstellte, allein im Informationssystem der Bremer Polizei (ISA) dreimal als Zeuge, neunmal als Geschädigter, elfmal als Tatverdächtiger und viermal als Anzeigeerstatter gespeichert. Diesen Fall schildere ich im folgenden etwas ausführlicher, um meine Arbeitsweise ebenso wie die Vielschichtigkeit der in manchem Einzelfall auftauchenden datenschutzrechtlichen Probleme zu verdeutlichen.

Im ersten Schritt meiner Nachprüfung mußte ich feststellen, daß das Polizeipräsidium den vom Beschwerdeführer geäußerten Auskunftsanspruch nicht ausreichend erfüllt hatte. So war in der Mitteilung an den Beschwerdeführer nicht enthalten, daß er auch in der erkennungsdienstlichen Sammlung geführt wurde. Daß der Petent erkennungsdienstlich behandelt war, ergab meine INPOL-Abfrage, die das LKA Bremen als nachrichtengebende Stelle auswies. Damit war aber klar, daß Daten über den Beschwerdeführer sowohl im automatischen Fingerabdrucksystem des Bundeskriminalamtes AFIS als auch im INPOL-System beim BKA geführt wurden.

Ich hatte deshalb parallel den Bundesdatenschutzbeauftragten um Überprüfung der Speicherung der Daten des Beschwerdeführers beim Bundeskriminalamt (BKA) in INPOL gebeten. In seiner Antwort teilte mein Bonner Kollege mit, daß neben der erkennungsdienstlichen Behandlung aufgrund einer Meldung bremischer Polizeibehörden an das BKA aus dem Jahre 1984 eine Speicherung in INPOL erfolgt sei, man aber eine Löschung nur dann prüfen könne, wenn die bremische Polizei auch den Ausgang des Verfahrens melde. Dies wurde auf meine mehrfachen Bitten hin nachgeholt. Die erkennungsdienstlichen Daten wurden daraufhin in INPOL gelöscht.

9.1.3.3. Löschung nach Wegfall des Tatverdachts

Um die Frage zu beurteilen, ob die zur Person des Beschwerdeführers gespeicherten Daten in ISA zu Recht gespeichert waren oder hätten gelöscht werden müssen, bedurfte es weiterer Nachforschungen, da in mehreren der gespeicherten Ermittlungsverfahren der Verfahrensausgang bei Staatsanwaltschaft und Gericht nicht bekannt war. Ich forderte daher einen Ausdruck aus dem staatsanwaltschaftlichen Informationsystem CANASTA an und verglich diesen mit den in ISA gespeicherten Datensätzen. Zum Teil mußten zusätzlich die zugehörigen staatsanwaltschaftlichen Ermittlungsakten eingesehen werden.

In einem Fall beruhte die Speicherung als Täter auf dem anonymen Schreiben eines Dritten an die Polizei, mit dem der Beschwerdeführer u.a. des Diebstahls eines Pkw mit einem bestimmten genannten Kennzeichen verdächtigt wurde. Die staatsanwaltschaftliche Ermittlungsakte wies allerdings aus, daß der daraufhin von der Polizei beantragte Hausdurchsuchungsbefehl vom Gericht mit der Begründung abgelehnt worden war, die Polizei habe entgegen üblicher Praxis unterlassen, zunächst bei der Zulassungsstelle eine Halterabfrage zu veranlassen. Später stellte sich dann heraus, daß das fragliche Fahrzeug völlig korrekt auf den Namen des Beschwerdeführers zugelassen und nicht als gestohlen notiert war. Bei dieser Sachlage und wegen anderer fragwürdiger Anhaltspunkte in dem anonymen Schreiben war die Polizei nicht berechtigt, den aus dem Jahre 1989 stammenden Vorgang längerfristig in ISA zu speichern. Meiner Löschungsempfehlung wurde entsprochen.

9.1.3.4. Löschung und kriminalistische Prognose

Die polizeiliche Prognose einer potentiellen künftigen Tatbegehung, die zu einer Speicherung im Informationssystem geführt hat, muß im Falle einer Bürgereingabe überprüft und neu gestellt werden. Nicht nur in diesem Fall habe ich die Löschung bzw. die Löschungsprüfung insbesondere bei Verfahren angeregt, die nach § 170 Abs. 2 StPO eingestellt worden sind, d. h. in den Fällen, in denen die Ermittlungen keinen genügenden Anlaß zur Erhebung einer Anklage geboten haben.

Nach 5.1 der sog. KpS-Richtlinien ist die Aufbewahrung solange zulässig, wie sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der Polizei liegenden Aufgaben erforderlich ist. Hierbei ist das öffentliche Interesse, zu Zwecken der Strafverfolgung, Strafvollstreckung oder Gefahrenabwehr auf polizeiliche Erkenntnisse zugreifen zu können, abzuwägen mit dem durch das Grundrecht auf freie Entfaltung der Persönlichkeit geschützten Interesse des einzelnen, solchen Einwirkungen der öffentlichen Gewalt nicht ausgesetzt zu sein.

Nach der Rechtsprechung des Bundesverwaltungsgerichts ist die Anlage und Führung kriminalpolizeilicher personenbezogener Sammlungen, sei es in der Form von Dateien oder Akten, zum Zweck der Gefahrenabwehr, namentlich der vorbeugenden Straftatenbekämpfung, rechtlich nicht nur dann zulässig, wenn der Betroffene wegen Verbrechen oder Vergehen aus dem Bereich der schweren oder schwersten Kriminalität verurteilt wurde. Das BVerwG bemißt die Zulässigkeit der Aufbewahrung auch daran, ob der bei dem gegen den "Beschuldigten" gerichteten Strafverfahren festgestellte Sachverhalt nach kriminalistischer Erfahrung angesichts aller Umstände des Einzelfalls Anhaltspunkte für die Annahme bietet, daß der Betroffene künftig oder anderswo mit guten Gründen als Verdächtiger einer noch aufzuklärenden Straftat in Betracht kommt, und ob die Unterlagen die dann zu führenden Ermittlungen fördern könnten.

Eine solche Prognose wird von der Polizei zwar im Zeitpunkt der Einspeicherung gestellt, ist aber nach meiner Auffassung bei der erneuten Eingabe eines Betroffenen anhand aller dann vorliegenden Erkenntnisse neu zu stellen. Maßgeblich sind alle Umstände des jeweiligen Einzelfalls: Dazu gehören vor allem Art, Schwere und Begehungsweise der Straftaten, deren der Betroffene verdächtigt wurde, seine Persönlichkeit sowie der Zeitraum, während dessen er strafrechtlich nicht mehr in Erscheinung getreten ist. Soweit er sie darlegt, sind auch seine allgemeinen Lebensumstände, wie z.B. ein fester Wohnsitz und eine feste Arbeitsstelle, mit einzubeziehen. Eine solche Abwägung war in einzelnen der gespeicherten Fälle nicht vorgenommen worden. Insbesondere war die fast zehn Jahre dauernde Straffreiheit des Beschwerdeführers nicht ausreichend berücksichtigt worden.

9.1.3.5. Speicherdauer für "andere Personen"

Auch im Zusammenhang mit der Speicherung des Betroffenen nicht als Tatverdächtiger, sondern als Hinweisgeber, Zeuge und Anzeigeerstatter ("andere Personen") mußte ich das Polizeipräsidium bitten, seine dem Beschwerdeführer mitgeteilte Rechtsauffassung noch einmal zu überprüfen. Dort ging man davon aus, daß auch für diesen Personenkreis eine zehnjährige Speicherfrist gelte. Ich habe für eine Differenzierung der Speicherdauer plädiert je nachdem, ob ein Fall bereits aufgeklärt werden konnte oder nicht. Jedenfalls in

den durch gerichtliche Verfahren abgeschlossenen Fällen könnten Hinweisgeber, Zeugen oder Anzeigeerstatter sofort gelöscht werden. Da diese Information über den Verfahrensausgang der Polizei aber nicht immer zur Verfügung steht, haben die KpS-Richtlinien eine generalisierende Speicherfrist vorgesehen. Allerdings sieht das in ISA angewandte Löschfristenverfahren für die sogenannten "anderen Personen" keine längere Frist als fünf Jahre vor. Eine Verlängerung der Speicherfrist beim Eingang weiterer Anzeigen eines Betroffenen ist nicht vorgesehen. Deshalb sind in der Regel die Daten über sogenannte "andere Personen" nach fünf Jahren in ISA zu löschen. In diesem Sinne hat sich mittlerweile auch das Polizeipräsidium mir gegenüber geäußert.

9.1.3.6. Beginn der Speicherdauer bei Untersuchungshäftlingen

Schließlich habe ich anläßlich dieses Vorganges das Polizeipräsidium gebeten, nach Bereinigung der Datensätze das in ISA vorgemerkte Aussonderungsprüfdatum der gesamten Kriminalakte erneut zu überprüfen. In seiner Antwort hat das Polizeipräsidium sich auf einen Widerspruchsbescheid des Senators für Inneres und Sport berufen. In diesem Bescheid wird das Aussonderungsprüfdatum berechnet ab dem Datum der Entlassung des Betroffenen aus der Untersuchungshaft (U-Haft).

Ich hingegen habe die Rechtsauffassung vertreten, die Frist beginne früher, nämlich mit dem Datum der zuletzt eingetragenen Straftat. Lediglich in den Fällen, in denen auch tatsächlich eine Freiheitsstrafe verbüßt wurde, ist die Frist nach dem Datum der Entlassung aus der Anstalt zu bemessen (Nr. 5.2.1 der KpS-Richtlinie). Eine andere Auslegung würde zu einer ungerechtfertigen Ungleichbehandlung derjenigen Tatverdächtigen führen, die sich in U-Haft befunden haben. Diese Tatsache gibt aus einer Reihe von Gründen, die ich hier nicht im einzelnen wiedergebe, keinen sachlichen Grund für eine Verlängerung der Speicherfrist in ISA. Soweit es darum geht, für den Fall einer Wiederholungstat Anknüpfungspunkte für die Sachverhaltsaufklärung zu erhalten, mag es gerechtfertigt sein, bei Verbüßung einer längeren Haftstrafe die Löschung von einer Bewährung durch ein straffreies Leben nach der Entlassung abhängig zu machen und deshalb die Speicherdauer um die Zeit der verbüßten Haftstrafe zu verlängern. Diese Überlegung gilt aber für den Aufenthalt in der U-Haft nicht. Einer entsprechenden Ratio folgt auch § 46 Abs. 3 des Bundeszentralregistergesetzes (BZRG), wonach sich nur bei längeren Freiheitsstrafen die Tilgungsfrist verlängert.

Ende Oktober 1994 hat das Polizeipräsidium mitgeteilt, daß es die Daten des Beschwerdeführers, soweit er als Tatverdächtiger in ISA gespeichert war, "ohne Anerkennung einer rechtlichen Verpflichtung" gelöscht habe. Da sein Schreiben keine Auslegung der KpS-Richtlinien zur Frage der Einbeziehung der U-Haft bei der Berechnung von Speicherfristen enthält, habe ich das Polizeipräsidium um Darlegung seiner Rechtsauffassung gebeten. Eine Antwort steht noch aus.

9.2. Ausländer

9.2.1. Das Ausländerzentralregister - das neue Gesetz und die Folgen

9.2.1.1. Die Vorgeschichte

Am 1. Okt. 1994 ist das Gesetz über das Ausländerzentralregister (AZR-G) vom 2. Sept. 1994 (BGBl I S. 2265) in Kraft getreten. Dadurch erhielt dieses Register, in dem über 8 Millionen Ausländer gespeichert sind und das beim Bundesverwaltungsamt betrieben wird, erstmals eine formale Rechtsgrundlage. Eine gesetzliche Regelung haben die Datenschutzbeauftragten des Bundes und der Länder seit vielen Jahren gefordert; im AZR wurden seit mehreren Jahrzehnten Daten von Ausländern verarbeitet, ohne daß festgelegt war, wer welche Daten erheben, speichern, übermitteln, abrufen und löschen durfte. Eine Vielzahl von Behörden bediente sich z. Teil elektronisch aus diesem Register; kein betroffener Ausländer wurde über die Inhalte dieser Zentraldatei informiert und auf seine Rechte hingewiesen.

Das jetzt in Kraft getretene AZR-G erfüllt die Regelungspflicht des Gesetzgebers allerdings nicht aufgrund vorheriger sorgfältiger Prüfung und Beschränkung der bisherigen

Verwaltungspraxis. Vielmehr wird nicht nur der Status quo der Datenverarbeitung legitimiert, sondern die "Verdatung" aller nichtdeutschen Bürger sogar erweitert. Dies geschieht vor dem Hintergrund einer umfassenden Vernetzung: Schon derzeit sind ca. 7ooo Terminals an das AZR angeschlosssen. Nach dem Inkrafttreten des AZR-G wird diese Zahl voraussichtlich sprunghaft ansteigen.

Ich habe immer wieder in meinen früheren Jahresberichten auf die fehlende gesetzliche Befugnis insbesondere zum automatisierten Abruf von Daten hingewiesen. Der Senat hat zwar meine Auffassung in seiner Stellungnahme zu meinem 13. JB (siehe Bürgerschaftsdrucks. 12/1281 S. 9) bestätigt, allerdings dessenungeachtet im Herbst 1992 einen On-Line Anschluß an das AZR für die Ausländerbehörde eingerichtet.

9.2.1.2. Umfassende Registrierung - auch für Sicherheitsbehörden

Nach der Zweckbestimmung des Gesetzes sollen durch das Register die mit der Durchführung ausländerrechtlicher und asylrechtlicher Vorschriften betrauten Behörden und andere öffentliche Stellen unterstützt werden. Nach der Begründung zu § 2 des Gesetzes sollen Daten über einen Ausländer nur gespeichert werden, wenn dazu bestimmte Anlässe gegeben sind. Der dann anschließende Anlaßkatalog ist jedoch so umfassend, daß nur wenige Personen, etwa Touristen, die sich weniger als drei Monate in der BRD aufhalten und keinen Visum-Antrag stellen müssen, der Speicherung entgehen. Betroffen sind z.B. auch Personen,

- wenn sie an der Grenze zurückgewiesen oder festgenommen werden sollen,

- wenn ihr Aufenthalt für Sicherheitsbehörden interessant ist,

- wenn sie ausgeliefert oder durchgeliefert werden oder worden sind,

- wenn ihr Antrag auf deutsche Staatsangehörigkeit abgelehnt worden ist, oder

- wenn ihre Aussiedlereigenschaft nicht anerkannt worden ist.

Damit werden zahlreiche Daten "auf Vorrat" erhoben und gespeichert; dies geschieht teilweise für Zwecke, die mit ausländer- oder asylrechtlichen Verwaltungserfordernissen nichts zu tun haben, sondern polizeiliche und geheimdienstliche Motive haben. Teile dieser Datenbestände sind auch noch einmal in den Informationssystemen dieser Stellen enthalten. Damit ist das AZR auch ein Teil des Informationsverbunds der Sicherheitsbehörden.

Noch deutlicher wird diese Hilfsfunktion bei den Hinweisen zur Festnahme oder Aufenthaltsfestellung bestimmter verdächtiger Personen sowie deren Ausschreibung zur beobachtenden Fahndung, die von Polizei und Nachrichtendiensten in das AZR eingegeben werden

9.2.1.3. Besonders problematisch: Freitextfelder und Suchvermerke

Die Datensätze im AZR können Freitexte enthalten mit sog. Begründungen und betreffen Abschiebungen, Ausweisungen, Einreisebedenken oder angeordnete Einschränkungen oder Unterlassungen von politischer Betätigung. Sie stehen allen öffentlichen Stellen - nach entsprechender Begründung- zur Verfügung. Es ist aber überhaupt nicht geregelt, wie zu verfahren ist, wenn diese Begründungstexte noch nicht rechtskräftig sind oder gar im verwaltungsrechtlichen Verfahren bestritten werden. Aus meiner Sicht sind diese potentiell diskriminierenden oder ungerechtfertigten Hinweise solange zu sperren; zumindest aber ist das eingelegte Rechtsmittel zu vermerken.

Besonders kritisch zu werten sind die in § 5 AZR-G geregelten Suchvermerke. Diese Suchvermerke, sog. Merker, kann jede öffentliche Stelle, ganz gleich ob Polizei, Arbeitsamt, Sozialversicherung oder Notar, anbringen lassen. Sie bewirken, daß die suchende Stelle von dem System automatisch unterrichtet wird, welche andere Stelle aus welchem Grund den Datensatz des betreffenden Ausländer aktiviert (z.B. angefragt oder geändert) hat, und dann dort nachfragen kann, ob der Aufenthalt des Betroffenen bekannt ist.

Auch hier sind geheimdienstliche Interessen berücksichtigt: Derartige Suchvermerke können z.B. auch veranlaßt werden, wenn ein Nachrichtendienst erfahren will, wo sich ein Ausländer aufhält (Spurverfolgung), mit welchen Personen er reist oder Kontakt hat, welches Transportmittel er benutzt oder was er mit sich führt.

Über diese Daten würde der Ausländer selbst regelmäßig keine Auskunft erhalten, da sie grundsätzlich gemäß § 34 AZR-G nicht beauskunftet werden müßten. Diese Informationen stehen aber andererseits vielen angeschlossenen öffentlichen Stellen (insbesondere BGS, Polizei und Zoll) im Direktabrufverfahren zur Verfügung, denn diese Ämter sollen ja gerade die gewünschten Feststellungen treffen.

9.2.1.4. Erweiterte Hinweisfunktion

Das Register enthält in jedem Datensatz den Hinweis (Geschäftszeichen) darauf, welche Behörde welches Datum direkt eingegegeben oder konventionell durch Brief o.ä. mitgeteilt hat. Durch dieses Merkmal wird jede anfragende Stelle in die Lage versetzt, sich an diese Behörden zu wenden und um Übermittlung weiterer Daten (Hintergrunddaten) zu ersuchen. Damit ist das AZR nicht nur selbst ein umfassendes Auskunftssystem, sondern darüber hinaus ein Hinweissystem, das den Rückgriff auf eine Vielzahl weiterer Akten und Unterlagen ermöglicht.

9.2.1.5. Kritik und Konsequenzen

Die Datenschutzbeauftragten haben ihre Kritik, die sie auch im Gesetzgebungsverfahren zum AZR-G detailliert vorgetragen und begründet haben, in einer Entschließung ihrer Konferenz zusammengefaßt (vgl. u. Ziff. 20.5). Kernpunkt dieser Bedenken ist die Erweiterung eines Systems zur Unterstützung der Ausländerbehörden zu einem Informationsverbund auch der Sicherheitsbehörden und Nachrichtendienste, also der Verstoß gegen das Gebot der Zweckbindung. Die Einwände der Datenschutzbeauftragten sind jedoch weitestgehend unberücksichtigt geblieben.

Kleinere Korrekturen sind jetzt nur noch auf der untergesetzlichen Ebene möglich, etwa bei der Regelung der Einspeicherungsbefugnis der Nachrichtendienste, die durch eine "Festlegung" des Bundesinnenministeriums erfolgen soll.

Im Land Bremen sind Direktabrufeinrichtungen bei den Ausländerbehörden und Polizeibehörden in Bremen und Bremerhaven sowie bei der zentralen Aufnahmeeinrichtung für Asylbewerber vorhanden oder geplant. Die Datenkommunikation dieser Stellen mit dem AZR werde ich im nächsten Berichtszeitraum prüfen.

9.2.2. Erkennungsdienstliche Behandlung aller Bürgerkriegsflüchtlinge?

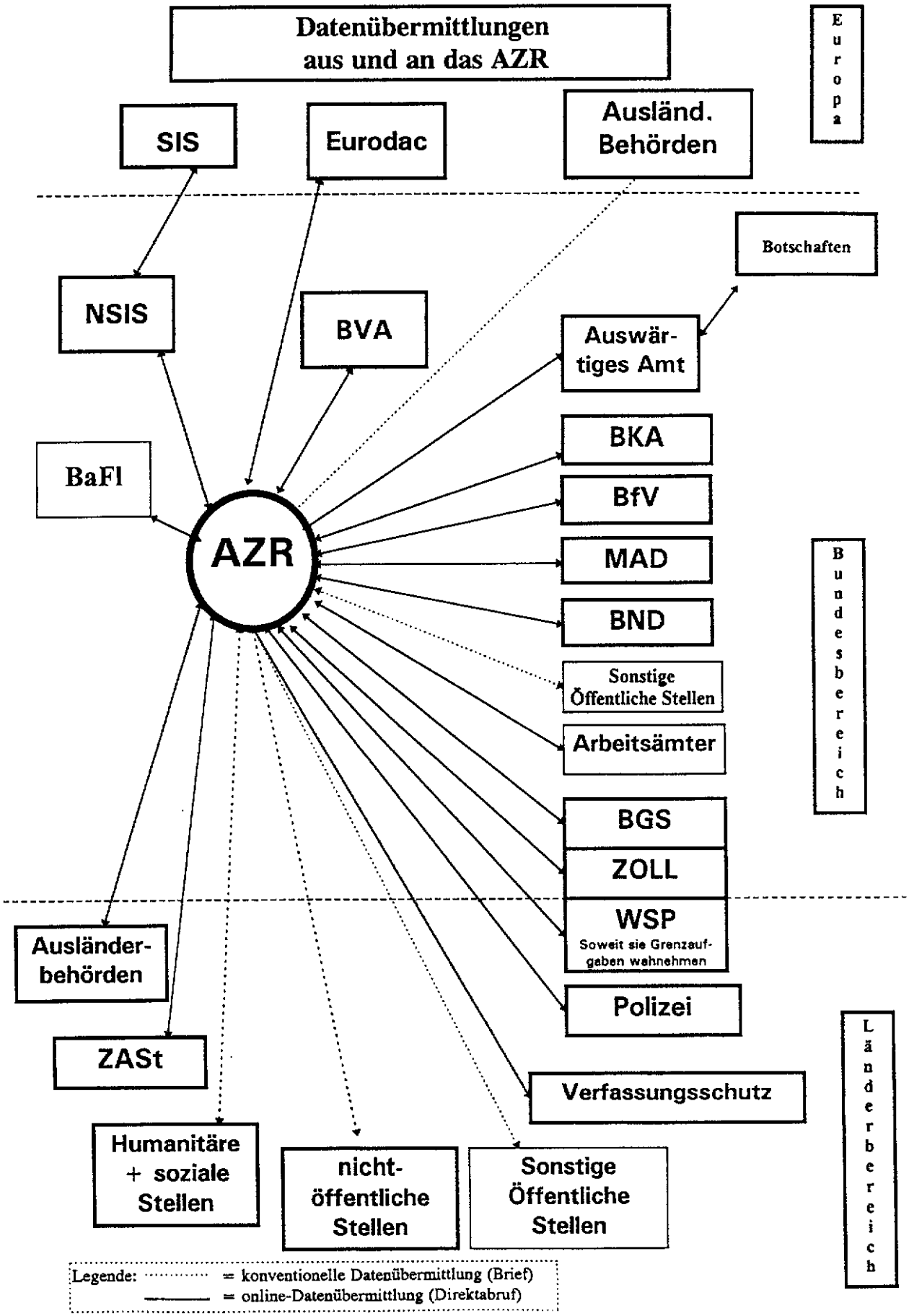
Durch eine Vorlage für die Konferenz der Innenminister und -senatoren der Länder (IMK) vom 15. April 1994 erhielt ich von dem Vorschlag einer Vorbereitungsgruppe Kenntnis, die Bundesregierung zu einer Gesetzesänderung mit dem Ziel aufzufordern, künftig für alle Bürgerkriegsflüchtlinge, die nach dem Ausländergesetz und nach internationalen Abkommen einen besonderen Schutzstatus besitzen, die gleichen Regelungen wie für Asylbewerber anzuwenden.

Dies würde vor allem die erkennungsdienstliche Erfassung aller Bürgerkriegsflüchtlinge bedeuten. Im allgemeinen Ausländerrecht (vgl. § 41 Ausländergesetz) ist diese Maßnahme nur zulässig, wenn Personen keine ausreichenden oder nur offensichtlich gefälschte oder verfälschte Personaldokumente vorlegen können. Die pauschale Erweiterung auf Bürgerkriegsflüchtlinge stellte aus meiner Sicht eine ungerechtfertigte Kriminalisierung dieser ohnehin von schwierigsten Lebensumständen betroffenen Menschen dar.

Diese Pläne lösten verständlicherweise ein starkes Medienecho aus. Kritik gab es auch in Bonner Politikerkreisen. Ich habe meine verfassungsrechtlichen Bedenken mehrmals sowohl gegenüber dem Innensenator als auch öffentlich geäußert.

Die Innenministerkonferenz hat zwar auf ihrer Sitzung am 6. Mai 1994 wie vorgeschlagen beschlossen, allerdings sind bisher keine Gesetzesinitiativen in dieser Richtung bekannt.

Skizze: Datenflüsse nach dem AZR-G:



Bestandteil des IMK-Beschlusses war auch die Aufforderung an die Ausländerbehörden, bis zu einer gesetzlichen Neuregelung bei Bürgerkriegsflüchtlingen jedenfalls den § 41 AuslG (s.o.) "konsequent" anzuwenden, was im Kontext des gesamten Entschließungstextes als Aufforderung zur Durchführung von mehr ed-Behandlungen als bisher verstanden werden konnte. Der Senator für Inneres und Sport hat mit Schreiben vom 12. Juli 1994 an die Ausländerbehörden in Bremen und Bremerhaven diese Bitte weitergegeben.

9.2.3. Fall: Ausländerbehandlung trotz deutscher Staatsangehörigkeit

9.2.3.1. Post vom Ausländeramt nach Einbürgerung

Ist das Ausländeramt auch für Deutsche zuständig? Dieses mußte man annehmen, als ich Mitte 1994 durch eine Ausländerselbsthilfeeinrichtung darüber informiert wurde, daß mehrere eingebürgerte deutsche Staatsangehörige von der Ausländerbehörde Post bekommen hatten. Sie waren darauf hingewiesen worden, daß sie einer Aufenthaltsgenehmigung bedürften und deshalb umgehend während der Geschäftsstunden dort vorzusprechen hätten. Ähnliche Aufforderungen verschickte das Arbeitsamt wegen angeblich erforderlicher Arbeitserlaubnisse. Diese behördlichen Aktivitäten führten bei den Betroffenen zur Verunsicherung und zu den Fragen, ob sie Deutsche "zweiter Klasse" wären, die immer noch vom Ausländeramt bzw. Arbeitsamt überwacht werden, und ob die Behörden ihre Daten nicht bereinigen würden.

Bei meiner Überprüfung stellte ich fest, daß die Ausländerbehörde trotz einer mehrere Jahre zurückliegenden Einbürgerung der Betroffenen von der Meldebehörde unterrichtet worden war, wie das für Ausländer in § 76 Abs. 5 AuslG i.V.m. § 2 Abs. 1 Ausländerdatenübermittlungsverordnung vorgesehen ist. Die Meldebehörde hatte übersehen, daß eine Mitteilung für deutsche Staatsangehörige, auch wenn sie früher eine andere Staatsangehörigkeit hatten, unzulässig ist. Diese routinemäßige Unterrichtung hatte das Ausländeramt ohne eigene Überprüfung zum Anlaß genommen, die o.a. Aufforderungen zu versenden.

Weiter stellte ich fest, daß im Ausländeramt eine sog. B-Kartei besteht, in der eingebürgerte, ausgereiste, fortgezogene oder verstorbene Ausländer geführt werden, und daß auch die Ausländerakte archiviert worden war. Diese Vorgänge, aus denen sich die Einbürgerung ergeben hätte, waren aber nicht bei der Bearbeitung beigezogen worden. Vielmehr wurde eine sog. Prüfakte angelegt, in der die von der Meldebehörde mitgeteilten Fälle "zwischengelagert" wurden.

In den von mir überprüften Fällen wurden die Vorgänge, d.h. die Mitteilung der Meldebehörde und die Durchschriften der Aufforderungsschreiben, nach Intervention der jetzigen deutschen Staatsbürger vernichtet.

9.2.3.2. Aktenführung nach Einbürgerung

Generelle rechtliche Einwände bestehen gegen das Archivierungsverfahren, d.h. das Abstellen der Karteikarte der eingebürgerten Ausländer in der B-Datei und die Ablage der Ausländerakte im Archiv. Nach § 6 Ausländerdateienverordnung sind die Daten zu löschen, wenn ein bisheriger Ausländer die Rechtsstellung eines Deutschen erworben hat. Die rechtliche Gleichstellung muß konsequenterweise auch dazu führen, daß die Archivierung der Ausländerakte und die Aufbewahrung der Karteikarte unzulässig ist, da die Ausländerbehörde sowohl nach dem Ausländergesetz als auch nach dem Asylverfahrensgesetz keinerlei Zuständigkeiten mehr hat.

Ich habe das Ausländeramt aufgefordert, die betr. Karteikarten aus der B-Datei zu entfernen und zu vernichten und mit dem Staatsarchiv zu regeln, ob die auszusondernden Ausländerakten übernommen werden oder vernichtet werden können.

In einem der vorliegenden Fälle bewahrheitete sich die alte Behördenerfahrung, daß Akten, solange sie bestehen, immer noch genutzt werden. In einer Akte war nach meinem letzten Einblick noch ein Dokument nachgeheftet worden, nämlich ein Bußgeldbescheid. Bei Ausländern sind solche Bescheide nach § 76 Abs. 2 Ausländergesetz mitteilungspflichtig. Die absendende Staatsanwaltschaft hatte sich ohne weitere Überprüfung ledig-

lich an dem ausländisch klingenden Namen orientiert. Aber auch die Ausländerbehörde schickte nicht etwa diese Mitteilung zurück, sondern heftete sie routinemäßig ab.

Die Ausländerbehörde hat umgehend reagiert und den Vorgang sofort vernichtet. Sie hat mir auch zugesagt, die Archivierungsvorschriften aufgrund der neuen Rechtslage zu überprüfen und mich zu beteiligen.

Bei der Staatsanwaltschaft konnte der Vorgang noch nicht geprüft werden, weil die Akte noch nicht verfügbar war.

9.2.4. ASYL-CARD

9.2.4.1. Das Projekt

Im Dezember 1994 erhielt ich von dem Protokoll einer Bund/Länder-Arbeitsgruppe Kenntnis, die sich mit der Harmonisierung der Verwaltungsabläufe im Asylverfahren befaßt hat. Hinter dieser harmlosen Überschrift verstecken sich Überlegungen für eine umfassende Überwachung von Asylbewerbern, die in dem Vorschlag zur Einführung einer "Asyl-CARD" gipfelten. Zur Prüfung dieses Vorschlags wurde eine sog. "Machbarkeitsstudie" angeregt.

Nach den Vorschlägen dieser Arbeitsgruppe soll jeder Asylbewerber eine sog. Smart-Card (prozessorgestütze Chipkarte) erhalten. Diese Asyl-CARD wäre bundesweit und evtl. später in anderen europäischen Ländern einsetzbar und könnte folgende Funktionen haben:

- Identifizierung (u.a. Lichtbild und elektronische Fingerabdrücke)
- Zutrittskontrollfunktionen (zu den zentralen Aufnahmeeinrichtungen)
- Aufenthaltskontrolle (Speicherung des Kontaktes mit einer Behörde)
- Verfahrensdaten (Antrag, Anhörungen usw.)
- Empfang von Sachleistungen (z.B. Essenempfang in Aufnahmeeinrichtungen)
- Empfang von Unterstützungsleistungen
- Arbeitserlaubnisse
- Leistungen von Dritten (z.B. Abrechnungen privater Unterkunftsbetreiber)

Folgende Zwecke der ASYL-Card nennt das Papier der Arbeitsgruppe:

- Reduzierung des Verwaltungsaufwandes
- Reduzierung der Datenfehlerquote
- Dynamische Datenhaltung und -auswertung
- Ständig aktuelle Daten bundesweit
- Aktuelle, d.h. aussagekräftige Statistiken
- Reduzierung des mißbräuchlichen Leistungsempfangs

Aus Sicht des Bundesamtes für die Anerkennung ausländischer Flüchtlinge könnte der Einsatz einer ASYL-CARD wie folgt gestaltet werden:

Nach der erkennungsdienstlichen Behandlung und der Rückmeldung des Bundeskriminalamtes, daß keine Doppelidentität vorliegt, wird dem Asylbewerber die ASYL-CARD ausgehändigt, die er bis zum Abschluß des Verfahrens (Anerkennung oder Ausreise) bei sich zu führen hat. Sie dient ihm als Ausweis und als Legitimation für die Inanspruchnahme sämtlicher ihm im Verlaufe seines Asylverfahrens zu gewährenden Leistungen. Der auf der Karte enthaltene Chip räumt den beteiligten Behörden die Möglichkeit ein, sowohl Identifizierungs- und Verfahrensdaten als auch Leistungsdaten zu speichern. Diese Angaben können bei Bedarf durch individuelle Fensterlösungen für die einzelnen Behör-

den lesbar gemacht werden. Die Ausgabe einer Ersatzkarte erfolgt erst nach erneuter erkennungsdienstlicher Behandlung.

9.2.4.2. Die Reaktionen

Ich habe mich ebenso wie eine Reihe meiner Kollegen umgehend gegen diese Pläne gewandt. Gegenüber dem Innensenator sowie in Presseerklärungen und Interviews habe ich deutlich herausgestellt, diese neue Zwangschipkarte würde es ermöglichen, über die Asylbewerber ein so umfassendes Persönlichkeitsbild herzustellen, daß dies mit dem Grundrecht auf informationelle Selbstbestimmung, das auch Asylbewerber beanspruchen können, nicht vereinbar wäre. Die Überlegungen zur Einführung dieses Kartensystems beruhen auf Defiziten des Asylverfahrens, die anders abgestellt werden sollten als mit datenschutzrechtlich problematischen Verfahren.

Der Senator für Inneres und Sport hat gegenüber Medienvertretern ebenfalls seine erheblichen - auf das Datenschutzrecht begründeten - Bedenken zur Asyl-CARD geäußert. Kritische Stimmen gab es auch aus dem Bundestag. Ich hoffe, daß dieses Projekt nicht weiterverfolgt wird.

9.2.5. Verfassungsschutzüberprüfung bei Einbürgerung

Wenn ein Ausländer nach § 8 Reichs- und Staatsangehörigkeitsgesetz deutscher Staatsbürger werden will, so wird er in Bremen durch den Verfassungsschutz überprüft. Diese "Regelanfrage" stellt die Einbürgerungsstelle beim Senator für Inneres und Sport in den Fällen, in denen die Verwaltung einen Ermessensspielraum bei der Einbürgerungsentscheidung hat. Nach dem Staatsangehörigkeitsrecht ist Voraussetzung für eine Einbürgerung, daß über den Einbürgerungsbewerber keine Anhaltspunkte vorliegen, daß er die öffentliche Sicherheit oder Ordnung im Sinne von § 46 Nr. 1 Ausländergesetz gefährden könnte.

Doch ist eine Überprüfung durch den Verfassungsschutz durch das Staatsangehörigkeitsgesetz selbst nicht vorgeschrieben und auch im Verfassungsschutzgesetz nicht angesprochen; vielmehr beruht sie auf Verwaltungsvorschriften und Erlassen des Bundesinnenministeriums.

Vor allem aber halte ich dieses Anfrageverfahren zumindest seit 1990 deshalb für überflüssig, weil ja § 76 Abs. 2 Ausländergesetz Polizei, Staatsanwaltschaft und Verfassungsschutz gerade verpflichtet, Daten, die eine Ausweisung rechtfertigen, **an die Ausländerbehörde** zu übermitteln. Eine nochmalige Anfrage bei den genannten Stellen einschließlich des Verfassungsschutzes stellt dementsprechend eine Doppelerhebung dar.

Ich plädiere dafür, die bremische Ermittlungspraxis in Einbürgerungsverfahren auf Notwendigkeit und Verhältnismäßigkeit hin zu überprüfen. Nach meinen Informationen herrscht in einigen anderen Bundesländern eine liberalere Verfahrensweise. Über dieses Thema bin ich mit dem Senator für Inneres und Sport im Gespräch.

9.3. Straßenverkehr

9.3.1. Verwertung von Strafurteilen trotz Löschung im Verkehrszentralregister

Nach wie vor ist ungeklärt, wie lange Führerscheinakten aufbewahrt und insbesondere inwieweit alte Vorgänge über strafrechtliche Verurteilungen, die sowohl im Bundeszentralregister als auch im Verkehrszentralregister gelöscht sind, z.B. bei Neuanträgen auf Erteilung eines Führerscheins herangezogen und verwertet werden.

9.3.1.1. Der erste Anlauf zur Klärung des Problems

In meinem 14. Jahresbericht vom 31.03.1992 (Ziff. 2.2.4.3) hatte ich dargelegt, daß der Senator für Inneres und Sport die Führerscheinstellen in Bremen und Bremerhaven anweisen wollte, nach Erteilung der Fahrerlaubnisse und Eintragung in die Führerscheinkartei die Führerscheinakten zu vernichten. Lediglich in den Verfahren, in denen Anträge auf Erteilung einer Fahrerlaubnis insbesondere wegen Eintragungen in das Straßenverkehrs-

zentralregister abgelehnt worden sind, sollten die Akten bis zur Tilgung dieser Eintragungen aus dem Verkehrszentralregister (z. T. fünf oder zehn Jahre) aufbewahrt werden.

In seiner Stellungnahme zu meinem 14. Jahresbericht hatte der Senat hierzu dargelegt, daß Fahrerlaubnisakten über den Zeitpunkt der Beendigung des Verwaltungsverfahrens hinaus nicht aufbewahrt würden. Besonderheiten ergäben sich bei Akten, die aufgrund eines Antrags auf Erteilung einer Fahrerlaubnis zur Fahrgastbeförderung angelegt wurden. Wegen des Nachweises der gesundheitlichen Eignung und der Ortskunde seien bislang längere Aufbewahrungsfristen für diese Unterlagen geboten gewesen. Da der Nachweis jedoch auch anders geführt werden könne, würde die Verwaltungpraxis entsprechend geändert. Aufgrund dieser eindeutigen Erklärung bin ich davon ausgegangen, daß diese datenschutzgerechte Verfahrensweise auch tatsächlich gehandhabt wird.

9.3.1.2. Neue Eingaben

Einige Monate später wandten sich mehrere Beschwerdeführer gegen die Praxis der Führerscheinstelle in Bremerhaven, wonach 20 bis 30 Jahre zurückliegende strafrechtliche Verurteilungen im Zusammenhang mit dem Straßenverkehr bei späteren Anträgen auf Neuerteilung einer Fahrerlaubns herangezogen und berücksichtigt worden waren.

Ich habe mich aufgrund dessen erneut an den Senator für Inneres und Sport gewandt und auf die Diskrepanz zwischen der von ihm erklärten datenschutzgerechten Verfahrensänderung und der praktischen Umsetzung hingewiesen. Meine Auffassung von der derzeitigen Rechtslage habe ich wie folgt begründet:

Die Vorschrift des § 51 Abs. 1 Bundeszentralregistergesetz (BZRG) regelt, daß die Tat und die Verurteilung dem Betroffenen im Rechtsverkehr nicht mehr vorgehalten und nicht zu seinem Nachteil verwertet werden dürfen, wenn die Eintragung über eine Verurteilung im Register getilgt worden ist. Dieses Verwertungsverbot gilt jedoch nur eingeschränkt nach § 52 Abs. 2 BZRG, wonach eine frühere Tat in einem Verfahren berücksichtigt werden darf, das die Erteilung oder Entziehung einer Fahrerlaubnis zum Gegenstand hat, wenn die Verurteilung wegen dieser Tat in das Verkehrszentralregister einzutragen war.

Diese Rechtsvorschrift ist unter Berücksichtigung des Volkszählungsurteils des Bundesverfassungsgerichts vom 15. Dezember 1993 als nicht mehr verhältnismäßig anzusehen. Insbesondere kollidiert diese Vorschrift mit dem Sinn, der den Tilgungsvorschriften zugrundeliegt, wonach die Betroffenen nach Tilgung der Eintragungen als "rehabilitiert" gelten sollten. Aus diesem Grunde war in dem Referentenentwurf des Bundesministers der Justiz zur Änderung des Bundeszentralregistergesetzes vom 01.07.1989 vorgesehen, diese Vorschrift dahingehend zu fassen, daß eine frühere Tat in einem Verfahren zur Erteilung oder Entziehung einer Fahrerlaubnis nur berücksichtigt werden darf, solange die Verurteilung wegen dieser Tat im Verkehrszentralregister eingetragen ist. Begründet wurde dieser Vorschlag damit, daß die derzeitige Regelung ohne zwingende Notwendigkeit die zeitlich unbegrenzte Berücksichtigung einer solchen Tat ermöglicht. Die beabsichtigte Neuregelung sollte gewährleisten, daß getilgte Eintragungen auch im Straßenverkehrsbereich nicht mehr verwertet werden.

Der Senator für Inneres und Sport vertritt inzwischen die Auffassung, nur eine sorgfältige Abwägung aller Gesichtspunkte neben der Tat selbst werde der einschneidenden Wirkung eines Entzugs oder einer Versagung der Erteilung einer Fahrerlaubnis gerecht. Die Regelung des § 52 Abs. 2 BZRG werde daher aus der Erfahrung der verkehrsrechtlichen Praxis als sachgerecht angesehen.

9.3.1.3. Konsequenzen für Gesetzgebung und Verwaltungspraxis

Ich halte es angesichts dieser Rechtsauffassung für erforderlich, daß die vom Bund bereits vor Jahren geplante Gesetzesänderung (s.o.) möglichst bald in der neuen Legislaturperiode in Angriff genommen wird.

In Bremen sollte unabhängig davon eine Regelung über die Aufbewahrung von Führerscheinakten in den Fällen erlassen werden, in denen die Erteilung aufgrund von Einträgen im Verkehrszentralregister abgelehnt worden ist. Die Vernichtung sollte vorgenommen

werden, sobald die strafrechtlichen Verurteilungen aus dem Verkehrszentralregister gelöscht sind.

Meine Auffassung wird gestützt von einem Beschluß des Bundesverwaltungsgerichts vom 18.03.94 (Az. 11 B 76.93), das sinngemäß entschieden hat, daß ein in der Führerscheinkartei eingetragener lange zurückliegender Fahrerlaubnisentzug (aus dem Jahr 1965) für eine Prognose über das künftige Fahrverhalten des Klägers nicht mehr tauglich erscheint.

9.3.2. Abbildung von Beifahrern auf Radarfotos

9.3.2.1. Konsequenzen der Aufnahmetechnik

Beschwerdeführer haben sich dagegen gewandt, daß auf dem Radarfoto der Polizei als Beweismittel neben dem Fahrer als Verursacher von Verkehrsordnungswidrigkeiten auch die Beifahrer auf dem Vordersitz mit abgebildet worden sind. Ich habe dem Stadtamt Bremen mitgeteilt, daß gegen diese Praxis Bedenken bestehen, weil Beifahrer nicht automatisch Beteiligte im Rahmen eines Verkehrsordnungswidrigkeitenverfahrens sind. Ich habe angeregt zu prüfen, wie die Gesichter von unbeteiligten Beifahrern auf den zu den Akten genommenen Fotos geschwärzt oder in anderer Weise unkenntlich gemacht werden können bzw. ob ggf. der entsprechende Teil des Frontfotos abgetrennt und vernichtet werden kann.

Nach Angaben des Stadtamtes beruht die derzeitige Praxis auf der von der Polizei angewandten Aufnahmetechnik. Da die eventuelle zeugenschaftliche Stellung von Bei-/Mitfahrern nicht dazu berechtige, von ihnen Bildaufnahmen zu fertigen, müsse die bildtechnische Erfassung bzw. Verarbeitung bereits darauf Rücksicht nehmen. Ob die Aufnahmetechnik entsprechend geändert werden könne, sei bisher ungeklärt. Derzeit jedenfalls seien die von mir vorgeschlagenen Maßnahmen wegen der Vielzahl der Vorgänge und der jeweils erforderlichen Einzelprüfung nicht zumutbar.

9.3.2.2. Offenbarung gegenüber dem Halter

Die Behörde hat außerdem darauf hingewiesen, daß Radar-Fotos, die als Frontalaufnahmen bei Geschwindigkeitsüberschreitungen gefertigt wurden, in Bremen nicht mit dem Anhörbogen an den Fahrzeughalter versandt würden. Der Halter werde lediglich durch einen entsprechenden Aufdruck im Anhörbogen auf das vorliegende Frontfoto als Beweismittel und auf die sachbearbeitende Dienststelle hingewiesen und bekomme in jedem Fall nur eine Ausschnittvergrößerung zu sehen, auf dem lediglich er selbst und das Fahrzeugkennzeichen zu erkennen seien.

Erst wenn die Verwarnung nicht akzeptiert werde oder der Betroffene Einspruch gegen den Bußgeldbescheid einlege, werde entweder ein Positivabzug der Ausschnittvergrößerung oder ggf. auch ein Abzug von der Totalaufnahme (mit den Einblendungen der Meßdaten) zur Akte genommen. Diese Praxis der Polizei und die Berufung auf die technischen Sachzwänge sind für mich nach wie vor nicht befriegend.

Im übrigen werden die Negativ-Filme nach Angaben der Verkehrsbereitschaft des Polizeipräsidiums fünf Jahre aufbewahrt. Diese Aufbewahrungsfrist halte ich nicht für notwendig, weil in den meisten Fällen kein Einspruch erfolgt und in den Einspruchsfällen ein Positivabzug angefertigt und zur Akte genommen wird. Ich beabsichtige, diese Praxis demnächst zu überprüfen.

9.4. Melde- und Personenstandswesen

9.4.1. Wahlkampf mit Wählerdaten

Anläßlich der Wahlen zum Europäischen Parlament und zum Deutschen Bundestag im vergangenen Jahr überprüfte ich bei den Meldebehörden in Bremen und Bremerhaven, ob im Vorfeld der Wahlen Daten aus dem Melderegister an die politischen Parteien übermittelt und ob dabei die melderechtlichen Vorschriften eingehalten wurden.

Die Prüfung ergab, daß vor den Wahlen zum Europäischen Parlament keine Meldedaten an die Parteien übermittelt wurden.

Vor der Wahl zum Deutschen Bundestag wurden dagegen auf Anfrage einer Partei von der Meldebehörde Bremerhaven Meldedaten übermittelt, und zwar auf Adreßaufklebern Namen, Vornamen, akademische Grade und Anschriften von Einwohnern mit deutscher Staatsangehörigkeit, die zwischen dem 01.01.1972 und dem 31.10.1976 sowie dem 01.01.1929 und dem 31.12.1919 geboren wurden.

Bei dieser Datenübermittlung war ein Verstoß gegen die Bestimmungen des Melderechts festzustellen. Unberücksichtigt blieb nämlich, daß Personen, die nach dem 16. 10. 1976 geboren wurden, zur Bundestagswahl nicht wahlberechtigt waren und ihre Daten deshalb nach den melderechtlichen Vorschriften nicht hätten übermittelt werden dürfen. Die Daten wurden in chronologischer Reihenfolge nach dem Geburtsdatum aufbereitet und übermittelt; dies verstößt ebenfalls gegen das Melderecht, das eine derartige Sortierung des Datenmaterials nicht zuläßt. Ich habe den Datenschutzverstoß gegenüber der Meldebehörde gerügt und verlangt, daß bei künftigen Wahlen unzulässige Datenübermittlungen dieser Art unterbleiben. Außerdem ließ ich mir bestätigen, daß die Partei die Adreßaufkleber zweckentsprechend verwandt hat und eine weitergehende Speicherung nicht vorgenommen wurde.

Aufgrund verschiedener Gesetzesänderungen (z.B. Melderechtsrahmengesetz, Wehrpflichtgesetz) ist es erforderlich, in Kürze das Bremische Meldegesetz zu ändern. Bei dieser Gelegenheit könnte auch die Übermittlung der Meldedaten an politische Parteien und Wählergruppen neu überdacht werden. Zwar sieht das Bremische Meldegesetz seit langem schon ein Widerspruchsrecht des Betroffenen gegen eine derartige Datenübermittlung und einen amtlichen Hinweis darauf, etwa in den Amtlichen Bekanntmachungen in den Tageszeitungen, vor, doch geht dieses Recht weitgehend ins Leere, da es nur wenige kennen und der amtliche Hinweis meist überlesen wird. Die Information der Bürger über ihre melderechtlichen Ansprüche sollte daher verbessert werden

Bei Gelegenheit dieser Änderung sollten auch die unterschiedlichen Fristen des Melderechts denjenigen des Wahlrechts angeglichen werden. Eingefügt werden muß außerdem die neue Regelung des Melderechtsrahmengesetzes, wonach die Parteien und Wählergruppen die Daten spätestens einen Monat nach der Wahl zu löschen haben.

9.4.2. Meldesperren und Wählerverzeichnis

9.4.2.1. Die Rechtslage

Das Melderecht enthält verschiedene Auskunfts- und Übermittlungssperren zum Schutz des meldepflichtigen Einwohners, die entweder auf Antrag oder von Amts wegen im Melderegister eingetragen werden. Die Sperren beziehen sich ausschließlich auf die Datenweitergabe an Private; innerhalb des öffentlichen Bereichs entfalten sie keine Wirkung; die Daten werden hier -allerdings mit Sperrvermerk- weitergegeben.

Für die Führung des auf Öffentlichkeit und allgemeine Zugänglichkeit angelegten Wählerverzeichnisses wirft dies einige Probleme auf. Einwohner, die auf die Sperrwirkung des Melderegisters vertrauen, müssen erleben, daß die melderechtlichen Sperren im Wahlrecht keine oder nur eine geringe Auswirkung haben.

Zur Führung des Wählerverzeichnisses dürfen die Meldebehörden den Wahlämtern gem. § 16 Bremische Meldedatenübermittlungsverordnung (MeldDÜV) unter anderem Namen, Geburtsdaten, Anschriften, Hinweise zur Staatsangehörigkeit, Zuzugs- und Fortzugsdaten sowie Wahlrechtsausschlußgründe übermitteln. Bei der Übermittlung der Daten sind die Verfahrens- und Sicherungsvorschriften der §§ 2, 3 sowie 18 und 20 MeldDÜV zu beachten. Nach § 18 Abs. 1 MeldDÜV haben die Meldebehörden beim Bestehen einer Auskunftssperre nach § 32 Abs. 5 (Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange) oder § 32 Abs. 7 Nr. 2 (Wahrung des Adoptionsgeheimnisses) Bremisches Meldegesetz (BremMeldG) einen Hinweis auf das Vorliegen der Sperre zu erteilen, womit die Durchbrechung der Auskunftssperre verhindert werden soll.

9.4.2.2. Praxis: Geheimadressen im öffentlichen Wählerverzeichnis

Im Zusammenhang mit den Wahlen zum Europäischen Parlament 1994 stellte ich bei den Meldebehörden in Bremen und Bremerhaven fest, daß der nach § 18 Abs. 1 MeldDÜV von den Meldebehörden zu erteilende Hinweis auf das Vorliegen einer Auskunftssperre an die Wahlämter nicht erteilt wurde. Dies führte dazu, daß die Wählerverzeichnisse ohne diese Hinweise geführt wurden und bei der öffentlichen Auslegung der Sperrvermerk nicht beachtet werden konnte.

Die Nichterteilung des Hinweises wurde damit begründet, daß nach einer Dienstanweisung des Innensenators die melderechtlichen zugunsten der wahlrechtlichen Vorschriften zurückzutreten hätten. Da die wahlrechtlichen Vorschriften die Auslegung des vollständigen Wählerverzeichnisses erfordern würden, sei der Hinweis auf das Vorliegen der Sperre nicht notwendig. Unberücksichtigt bleibt bei dieser Betrachtung jedoch, daß mit der Durchbrechung der melderechtlichen Auskunftssperre eine Gefährdung hochrangiger Rechtsgüter der Betroffenen einhergeht.

Ich forderte den Senator für Inneres und Sport auf, dafür zu sorgen, daß die Meldebehörden künftig den Hinweis, zu dem sie nach §18 Abs.1 MeldDÜV verpflichtet sind, an die Wahlämter erteilen und daß diese die melderechtliche Auskunftssperre dann beachten.

In Bremerhaven wurde bereits im Zusammenhang mit der Wahl zum Deutschen Bundestag das Übermittlungsverfahren teilweise geändert. Von der Meldebehörde wurden die nach § 18 Abs. 1 MeldDÜV erforderlichen Hinweise übermittelt, so daß sie bei der Führung und der Auslegung des Wählerverzeichnisses berücksichtigt werden konnten. In Bremen wurden die Hinweise auch bei der Bundestagswahl nicht erteilt.

9.4.2.3. Vorschlag: Herausnahme der gesperrten Anschriften

Die Übermittlung des Sperrhinweises an die Wahlämter kann allerdings nur bewirken, daß das Wahlamt von der Sperre erfährt und entsprechend handelt. Offen bleibt jedoch, wie in derartigen Fällen bei der Auslegung des Wählerverzeichnisses, d. h. der Übermittlung an andere Bürger, verfahren werden soll.

Nach meiner Auffassung sollten wahlberechtigte Personen, bei denen eine melderechtliche Auskunftssperre vorliegt, bei der öffentlichen Auslegung des Wählerverzeichnisses ausgespart werden, d. h. weder am Bildschirm angezeigt noch listenmäßig ausgedruckt werden. Die Wahlämter würden so den melderechtlichen Sperrhinweis beachten, ohne daß der wahlberechtigte Bürger im Wählerbestand gelöscht und von der Wahlteilnahme ausgeschlossen wäre. Die Sicherung persönlichkeitsschützender Rechtsgüter sollte höher bewertet werden als der Anspruch der Allgemeinheit, durch die öffentliche Auslegung des Wählerverzeichnisses die Wahlrechte der Bürgerinnen und Bürger und die Vollständigkeit des Verzeichnisses prüfen und evtl. korrigieren zu können. Sowohl das Demokratieprinzip als auch die Möglichkeit einer öffentlichen Kontrolle des Wahlverfahrens werden durch die Nichtbekanntgabe von Daten einzelner weniger Personen im für Einsichtszwekke kaum genutzten Wählerverzeichnis in ihrer Substanz nicht beeinträchtigt.

Meiner Auffassung entsprechend habe ich dem Senator für Inneres und Sport die Änderung der die Auslegung des Wählerverzeichnisses betreffenden wahlrechtlichen Vorschriften des Landes empfohlen. Zugleich bat ich ihn darum, soweit bundesrechtliche Vorschriften betroffen sind, meine Auffassung an den Bundesminister des Innern heranzutragen.

Der Senator für Inneres und Sport teilte mir daraufhin mit, daß im Bereich des Wahlrechts auf eine für die Wahlorganisation größtmögliche Übereinstimmung zwischen landes- und bundesrechtlichen Regelungen geachtet werden müsse. Bremen selbst könne nur Landesrecht, nicht aber das Wahlrecht des Bundes ändern. Derzeit stünden auf Bund-/Länderebene Erörterungen bevor, die möglicherweise zu einem bundesweiten Verzicht auf die öffentliche Auslegung des Wählerverzeichnisses führen. Für den Fall, daß im Bund auf die öffentliche Auslegung nicht verzichtet werde, erklärte sich der Senator für Inneres und Sport zu eigenständigen Überlegungen für das Land Bremen bereit. Dabei werde er zu einer Lösung tendieren, nach der Personen, für die im Melderegister eine

Auskunftssperre nach § 32 Abs. 5 oder Abs. 7 Nr. 2 BremMeldG besteht, im öffentlich zugänglichen Wählerverzeichnis nicht mehr angezeigt bzw. ausgedruckt werden. Diese Lösung wäre auch mit Regelungen anderer Bundesländer vergleichbar.

Die Erörterungen auf Bund-/Länderebene waren bis Ende Januar 1995 noch nicht abgeschlossen; ein bundesweit abgestimmtes Ergebnis ist nicht in Sicht. Spätestens nach der Bürgerschaftswahl 1995 sollte deshalb eine entsprechende landesspezifische Neuregelung angegangen werden.

10. Justiz

10.1. Strafakten als multifunktionale Informationsquelle

10.1.1. Der Entwurf des Bundesrates für ein Strafverfahrensänderungsgesetz 1994 (StVÄG 1994)

Seit Jahren werden die staatsanwaltschaftlichen Verfahrensregister ohne Rechtsgrundlage nur aufgrund der Beanspruchung des verfassungsrechtlichen "Übergangsbonus" betrieben. Nachdem absehbar war, daß der Bundesgesetzgeber auch in der Ende 1994 abgelaufenen Legislaturperiode nicht in der Lage sein würde, entsprechende gesetzliche Regelungen in Kraft zu setzen, hatte sich eine Arbeitsgruppe der Justizminister und -senatoren der Länder zusammengefunden, um einen Länderentwurf für ein StVÄG zu erarbeiten. Das Arbeitsergebnis dieser Gruppe war allerdings weniger durch präzise Normen als durch weite Generalklauseln gekennzeichnet.

Der Senator für Justiz und Verfassung hat sich eine ganze Reihe auch von mir ihm vorgetragener datenschutzrechtlicher Verbesserungen zu eigen gemacht und diese in Form von Änderungsanträgen im Rechtsausschuß des Bundesrates eingebracht. Leider wurden diese Anträge ganz überwiegend nicht angenommen. Deshalb ist es bedauerlich, daß Bremen in der Schlußabstimmung im Oktober 1994 dennoch dem Gesetzentwurf (BR-Drs. 620/94) zugestimmt hat.

10.1.2 Die Datenschutzkritik

Der StVÄG-Länderentwurf erhebt den Anspruch, den Schutz der Daten am Strafprozeß beteiligter Bürger sicherzustellen. Dieser Zweck wird aber völlig verfehlt. Mit zahlreichen generalklauselartigen Formulierungen sollen in großem Umfang die Informationsverarbeitung im Strafverfahren und die Datenübermittlungen an eine Vielzahl von Stellen ermöglicht werden. Zweckbindungsgebote fehlen weitgehend ebenso wie Nutzungsbeschränkungen bzw. Verwertungsverbote für die Datenempfänger oder verbindliche Lösch- bzw. Aussonderungsprüffristen.

Präzise Verarbeitungsnormen sind jedoch gerade in diesem Bereich umso notwendiger, als es sich bei den von den Strafverfolgungsbehörden verarbeiteten Daten oft um hochsensible und höchstpersönliche Daten von Opfern, Tätern und Zeugen handelt. Zu nennen sind beispielsweise intime medizinische und psychologische Gutachten in Vergewaltigungsprozessen, belastende Zeugenaussagen im Bereich der organisierten Kriminalität oder vertrauliche Abhörprotokolle von Telefonüberwachungsmaßnahmen. Der Entwurf läßt wichtige, seit Jahren erhobene Forderungen der Datenschutzbeauftragten des Bundes und der Länder unberücksichtigt.

Vor allem wird nicht ausreichend zwischen den verschiedenen Funktionen staatsanwaltschaftlicher Informationssysteme differenziert. Zu unterscheiden ist zwischen Aktennachweissystemen (zentrale Namensdateien), die zur Vorgangsverwaltung dienen und Systemen, die der Sachbearbeitung dienen (z.B. Schreiben von Ladungen oder Anklagen). Die ersteren brauchen nur Angaben zu enthalten, die zum Auffinden der Akten und zur Information über den Verfahrensstand sowie zur Fristenkontrolle erforderlich sind. Diese Daten sind entsprechend dem Verfahrensstand laufend zu aktualisieren und nur so lange zu speichern, wie auch die zugehörigen Akten aufbewahrt werden dürfen. Die automatisierten Aktennachweissysteme sollten und könnten deshalb auch für eine wirksame Kontrolle der Aufbewahrungsfristen genutzt werden.

Wenn der Entwurf scheinbar präzisierend vorsieht, daß solche Vorschriften des Bundes und Landes zu beachten sind, die die Verwendung personenbezogener Informationen für Zwecke des Strafverfahrens besonders regeln, so geht diese Verweisung ins Leere, da derartige landesrechtliche Vorschriften weder existieren noch zu erwarten ist, daß der Landesgesetzgeber für die Vielzahl an Verwendungsmöglichkeiten detaillierte Normen erlassen wird.

Zu kritisieren ist weiter die undifferenzierte Ermächtigung aller öffentlichen Stellen zur Weitergabe von Informationen an die Staatsanwaltschaft. Sie ist auch insoweit systemwidrig, als Übermittlungsbefugnisse üblicherweise im Recht der übermittelnden und nicht im Recht der datenempfangenden Stelle geregelt werden.

Zu weitgehend sind die Auskunfts- und Akteneinsichtsrechte dritter Stellen wie z.B. Versicherungen. Ein Nachweis von der anfordernden Stelle, wofür sie die Akten benötigt, wird nicht vorgeschrieben. Dem Prinzip, daß Akteneinsicht und -übersendung nicht in Betracht kommen, wenn eine Auskunft aus den Unterlagen ausreicht, wird nicht Rechnung getragen. Ein "berechtigtes Interesse", wozu auch wirtschaftliche und publizistische Interessen zählen, soll für die Aktenanforderung ausreichen. Zu differenzieren ist zwischen Personen, die unmittelbar von der Durchführung eines Strafverfahrens betroffen sind wie z.B. Beschuldigte, Zeugen oder Opfer; ihre Informationsinteressen sind wesentlich gewichtiger als die sonstiger Personen und Stellen.

Die Konferenz der Datenschutzbeauftragten zog in einem Beschluß im September 1994 das Fazit, der Entwurf werde "datenschutzrechtlichen Anforderungen in keiner Weise gerecht" (vgl. u. Ziff. 20.2). Auch das Oberlandesgericht Frankfurt hat in seinem Beschluß vom 19.05.1994 (Az.: 3 VAs 31/94) klar gemacht, daß der Gesetzentwurf unter datenschutzrechtlichen Gesichtspunkten noch überarbeitet werden muß. Die Bundesregierung hat inzwischen beschlossen, zum Länderentwurf keine detaillierte Stellungnahme vorzulegen, sondern einen eigenen Entwurf ins Gesetzgebungsverfahren zu bringen. Ich erwarte, daß bereits dieser Text und ggf. die Beratungen im Bundestag zu verfassungsgemäßen Regelungen führen.

10.2. Bundesweites staatsanwaltschaftliches Informationssystem

10.2.1. Ziele des neuen Bundes-SISY

Auch wenn nach wie vor offen ist, wann es zu den verfassungsrechtlich gebotenen Normen für die Datenverarbeitung im Strafverfahren kommen wird (vgl. ausf. dazu Ziff. 10.1), eine Vorabregelung wurde in dem unter 9.1.1. dargestellten und kritisierten Verbrechensbekämpfungsgesetz bereits untergebracht: Art. 4 Nr. 12 sieht den Aufbau eines bundesweiten staatsanwaltschaftlichen Informationssystems (sogenanntes Bundes-SISY) vor.

Die Datei dient der zentralen Speicherung aller im Bundesgebiet anhängigen Ermittlungs- und Strafverfahren. Die Datenbank soll beim Generalbundesanwalt - Dienststelle Bundeszentralregister - geführt werden. Aufnahme in die Datei sollen die Daten aller Beschuldigten in einem Ermittlungs- und Strafverfahren finden. Die Daten sollen auch in den Fällen, in denen es zu keiner Verurteilung der Betroffenen kommt, über den Abschluß des Verfahrens hinaus gespeichert bleiben. Die bisherige zentrale Registrierung beim Bundeszentralregister ist auf rechtskräftige Verurteilungen beschränkt.

10.2.2. Fehlende Differenzierung bei der bundesweiten Speicherung

Gegen eine solche bundesweite Strafdatenbank habe ich zusammen mit anderen Datenschutzbeauftragten des Bundes und der Länder erhebliche Bedenken geltend gemacht (vgl. Konferenzbeschluß vom 09./10.03.1994, Ziff. 20.2). Länderübergreifende automatisierte Informationssysteme dürften allenfalls für solche Vorgänge errichtet werden, bei denen bestimmte Tatsachen die Prognose begründen, daß auf die erfaßten Daten zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben erneut zugegriffen werden muß. Eine solche negative Prognose wird in der Regel dann nicht gerechtfertigt sein, wenn das zugrundeliegende Verfahren mit einer Einstellung nach § 170 Abs. 2 StPO oder einem rechtskräf-

tigen Freispruch abgeschlossen worden ist, sofern nicht auch nach Abschluß des Verfahrens noch tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte eine strafbare Handlung begangen hat. Eine Bereitstellung von Daten zu Zwecken der Strafverfolgung wird ferner grundsätzlich dann nicht in Betracht kommen, wenn die Ermittlungen konkrete Anhaltspunkte dafür bieten, daß der Beschuldigte nicht erneut strafbare Handlungen begehen wird. Dies kann z. B. bei Fahrlässigkeitstaten der Fall sein.

Eine solche Differenzierung ist aber mit den durch das Verbrechensbekämpfungsgesetz verbundenen Änderungen der StPO nicht vorgesehen. Die bereits in früheren Jahren wiederholt von der Konferenz der Datenschutzbeauftragten vorgetragenen Anforderungen und Anregungen für Regelungen der Informationsverarbeitung im Strafverfahren, namentlich die Beschlüsse der Konferenz vom 28./29.09.1991 ("Mindestanforderungen für den Datenschutz bei den zentralen Namensdateien der Staatsanwaltschaften"), vom 24./25.11.1986 ("Überlegungen zu Regelungen der Informationsverarbeitung im Strafverfahren") und vom 05./06.04.1989 ("Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts vom 03.11.1988") wurden nicht berücksichtigt.

10.2.3. Risiken des neuen Bundesregisters

Da ja in den Ländern auch weiterhin eigene staatsanwaltschaftliche Datenverarbeitungs- und Nachweissysteme geführt werden, lassen die Regelungen zum Bundes-SISY insoweit ein zwischen Bund und Ländern abgestimmtes Gesamtkonzept vermissen. Auch wurde es unterlassen zu prüfen, ob die in den polizeilichen Informationssystemen des Bundes und der Länder vorhandenen Daten nicht eine ausreichende Informationsgrundlage geboten hätten, um die vom Bundes-SISY angestrebten Zwecke zu erreichen. Die Zentralisierung der Verfahrensregister und der damit verbundene massive Eingriff in die Rechte der Betroffenen steht in einem deutlichen Mißverhältnis zu den Nutzungsinteressen der Strafverfolgungsbehörden. Für den Zweck, mehrere gegen eine bestimmte Person anhängige Ermittlungsverfahren zusammenzuführen und die erforderlichen Informationen zur Verfügung zu stellen, um parallele Ermittlungen in mehreren Verfahren und die Durchführung mehrerer Hauptverhandlungen zu vermeiden, hätte es nicht eines neuen gigantischen Bundesregisters bedurft.

Die Risiken einer bundesweiten Datei auch und gerade für "unbescholtene" oder nur gering belastete Bürger zeigt sich insbesondere bei unbegründeten Strafanzeigen (vgl. hierzu den unter Ziff. 9.1.3 geschilderten Fall einer anonymen Anzeige), bei Fahrlässigkeitsdelikten ohne überörtliche Bedeutung und bei der vorgesehenen zweijährigen Weiterspeicherung von Daten über Freisprüche und Einstellungen ohne Restverdacht. Der Bürger bleibt also trotz rechtskräftigen Freispruchs im Computer! Aber auch wenn das Strafverfahren eingestellt wird oder die Staatsanwaltschaft entscheidet, daß der ursprünglich Beschuldigte als Täter nicht in Betracht kommt oder sein Verhalten gar nicht strafbar war, ist kein überwiegendes Allgemeininteresse zu erkennen, das eine jahrelange bundesweite Verfügbarkeit rechtfertigen würde.

Ich habe meine Bedenken gegenüber den Regelungen zur Einführung eines Bundes-SISY dem Senator für Justiz und Verfassung mehrfach vorgetragen.

10.3. Sijus-Straf - Rechnernetz und Datenkommunikation für Staatsanwälte

10.3.1. Systembeschreibung

Bei der Staatsanwaltschaft Bremen und Bremerhaven sollte bis zum Jahreswechsel 1994/95 flächendeckend das ADV-Verfahren Sijus-Straf eingeführt werden. Das Verfahren Sijus-Straf ist ein Softwarepaket zur Unterstützung der Automation des Geschäftsstellenbetriebes und der Kanzleitätigkeiten bei den Staatsanwaltschaften. Mit Hilfe von Sijus-Straf können u.a.folgende Arbeiten automatisiert werden:

- Verfahrens- und Registerführung,
- Führen und Auswertungen der Zentralen Namensdatei,
- Aktenführung, Aktenkontrolle und Erstellen von Kontrollübersichten,

- Wiedervorlage,
- Fristen- und Terminalverwaltung,
- Zählkartenbearbeitung,
- Aufgaben der Registratur,
- statistische Erhebungen und Auswertungen,
- Auflistung und Auswahl (z.B. von Geschädigten, gesetzlichen Vertretern, Beschuldigten und Beteiligten),
- Textbe- und -verarbeitung, d. h. das Erstellen aller Schreiben, Fertigen von Anklageschriften und das Erstellen von Formschreiben, wie z.B. Ladungen,
- Aufgaben der Behördenleitung und des individuellen Geschäftsbetriebes.

Eine Besonderheit in Bremen ist die Anbindung der Staatsanwaltschaft Bremerhaven an die Staatsanwaltschaft Bremen über eine Standleitung. Auf diese Weise verfügen alle Staatsanwaltschaften im Lande über die gleichen, zentral geführten Dateien.

Weiter soll ein leitungsübermittelter Datenaustausch mit anderen Behörden und zentralen Registerbehörden stattfinden. So sind vorgesehen Schnittstellen mit

- Informationssystemen der Polizei. Die jetzt bestehende Schnittstelle mit ISA/CANASTA soll integriert werden; es ist aber langfristig geplant, einen weiterreichenden Datenaustausch mit der Polizei technisch vorzubereiten, um den Austausch von Schriftstücken und Daten zu ermöglichen,
- den Datenbanken der Einwohnermeldebehörden in Bremen und Bremerhaven, um der Eingangsstelle einen Abgleich der Meldedaten mit DEMOS zu ermöglichen und ggf. die Anschriften zu aktualisieren,
- dem Bundeszentralregister zur Einspeicherung und zum Abruf von Verfahrensdaten in das Bundeszentralregister,
- der Datenbank beim Kraftfahrbundesamt, wobei der Datenaustausch über DATEX-P laufen soll,
- automatisierten Informationssystemen in den Justizvollzugsanstalten; ein solcher Anschluß soll allerdings erst später realisiert werden. Gleiches gilt für den Anschluß an
- vernetzte Informationssysteme der Strafgerichte.

10.3.2. Beteiligung des Landesbeauftragten für den Datenschutz

Vor der endgültigen Entscheidung über die Einführung des Sijus-Straf-Verfahrens wurde es in einem Testbetrieb ab dem 01. Oktober 1993 von der Abteilung V auf die Tauglichkeit für den Einsatz bei der Staatsanwaltschaft Bremen getestet. Im Juli 1994 erhielt ich den ADV-Antrag zum flächendeckenden Einsatz des Verfahrens Sijus-Straf. Nach Studium der angeforderten Verfahrensunterlagen und Durchführung zweier Besprechungstermine im Hause der Staatsanwaltschaft in Bremen, bei der ich auch partiell Funktionsweisen des System vorgeführt bekam, habe ich im September 1994 eine datenschutzrechtliche Stellungnahme gegenüber dem Senator für Justiz und Verfassung und der federführenden Staatsanwaltschaft in Bremen abgegeben. Darin habe ich auf folgendes hingewiesen:

10.3.3. Datenschutzrechtliche und technische Bewertung

Mit SIJUS-Straf will die Staatsanwaltschaft ein nach vielen Seiten offenes und für die eigene Arbeit multifunktional einsetzbares Informationssystem aufbauen in der Hoffnung, auf diese Art und Weise die eigene Arbeit zu effektivieren und so zu kürzeren Bearbeitungszeiten zu gelangen. Nach wie vor fehlt aber die erforderliche gesetzliche Absicherung der Datenverarbeitung im Ermittlungsverfahren (vgl. o. Ziff. 10.1). Weit über die Anwendungen in anderen Bundesländern hinaus und ohne auf die Vorgaben des Bundesgesetzgebers zu warten, soll in Bremen ein allein nach den Funktionsinteressen der Staatsanwaltschaft zugeschnittenes Informationssystem in Betrieb gehen.

Anders als beim bisherigen System CANASTA kann für das Verfahren Sijus-Straf nicht der verfassungsrechtliche "Übergangsbonus" reklamiert werden, wonach für eine befristete Zeit Eingriffe in das Recht auf informationelle Selbstbestimmung durch den Bürger hinzunehmen sind, bis der Gesetzgeber eine gesetzliche Regelung getroffen hat. Denn das Verfahren Sijus-Straf erhält nicht den Status quo, sondern erweitert die Möglichkeiten der Datenverarbeitung und -nutzung und damit das Risiko unzulässiger Eingriffe in das Recht auf informationelle Selbstbestimmung.

Ungeachtet dieses prinzipiellen Einwands fehlender gesetzlicher Absicherung habe ich das System unter Gesichtspunkten der Datensicherung begutachtet und eine Fülle von Anforderungen u.a. zum Zugriffsschutz, zur Datenfernübertragung, zur Protokollierung und zur Fernwartung formuliert. In meiner Stellungnahme habe ich abschließend zum Ausdruck gebracht, daß ich erwarte, daß Sijus-Straf nicht in Betrieb geht, bevor die von mir angesprochenen Punkte geklärt sind und das Datenschutzkonzept mit mir abgestimmt worden ist. Eine Stellungnahme des Senators für Justiz und Verfassung ist mir kurz vor Redaktionsschluß dieses Berichts zugegangen und wird zur Zeit geprüft.

10.4. Bilanz: Prüfung der Justizvollzugsanstalt Oslebshausen

10.4.1. Konsequenzen der Beanstandung

Nach einer Datenschutzprüfung habe ich im Oktober 1993 verschiedene Formen der Datenverarbeitung im Strafvollzug in der Justizvollzugsanstalt Oslebshausen gegenüber dem Senator für Justiz und Verfassung beanstandet und, wie in § 29 Abs. 3 BrDSG vorgesehen, damit Vorschläge zur Beseitung der Mängel verbunden und eine ganze Reihe von Maßnahmen zur sonstigen Verbesserung des Datenschutzes vorgeschlagen (vgl. 16. Jahresbericht,Ziff. 6.1).

1994 stand ganz im Zeichen der Abarbeitung dieser datenschutzrechtlichen Vorschläge und Anregungen. Dazu war es erforderlich, eine Vielzahl von Gesprächen mit Vertretern der senatorischen Dienststelle, dem Justizvollzugsamt und Anstaltsleitern zu führen. Zusammenfassend ist festzustellen, daß bis auf ganz wenige noch klärungsbedürftige Punkte meinen Vorschlägen und Anregungen zur Verbesserung des Datenschutzes gefolgt wurde. Positiv zu bewerten ist dabei insbesondere, daß nicht nur Lösungen für die geprüfte Justizvollzugsanstalt Oslebshausen, sondern auch für alle anderen Vollzugsanstalten im Lande Bremen getroffen wurden.

10.4.2. Der erste Schritt: Neue Allgemeinverfügung

In einem ersten Schritt wurden konkrete Maßnahmen ergriffen, um zu verhindern, daß weiterhin wie berichtet amtliche Schriftstücke und Aktenteile aus dem Bereich des Strafvollzugs in die Hände von Gefangenen geraten oder in der Öffentlichkeit auftauchen. Einen großen Teil trägt hierzu die Einführung der automatisierten Datenverarbeitung, d.h.des Verfahrens ADIV (vgl. u. Ziff. 10.4.7) bei, weil dieses Verfahren zum einen die erforderlichen Informationen den einzelnen Bereichen in der JVA in papierloser Form zur Verfügung stellt, zum anderen den einzelnen Anstaltsbereichen nicht - wie bisher häufig praktiziert - im Durchschlagverfahren möglichst viele Informationen, sondern gezielt nur die speziell benötigte Auswahl der Daten zukommen läßt.

Parallel dazu hat der Senator für Justiz und Verfassung nach Vorlage in der Deputation für Justiz und Verfassung im März 1994 eine Allgemeinverfügung (AV) erlassen. Die Allgemeinverfügung betrifft die Verwahrung von Schriftgut mit personenbezogenen Daten und verlangt die sichere Aufbewahrung von Schriftstücken, regelt die Herausgabe und Rücknahme von Gefangenenpersonalakten, trifft Vorgaben zur Archivierung des Schriftgutes wie auch zur Führung der Archive und trifft Regelungen zur Vervielfältigung und Vernichtung von Schriftgut. Sie enthält weiter besondere Vorschriften für den ärztlichen Bereich, für die Reinigung der Diensträume durch Gefangene sowie für die Auskunftserteilung über Gefangene, deren Angehörige und sonstige Kontaktpersonen.

Auch wenn ich mich u.a. nicht mit der Forderung durchsetzen konnte, wegen der Sensibilität der dort aufbewahrten Unterlagen keine Reinigung der Vollzugsgeschäftsstelle

durch Gefangene vornehmen zu lassen, sind die getroffenen Regelungen insgesamt als positiv zu bewerten. Meine Vorschläge wurden dabei fast alle übernommen.

10.4.3. Archivierung inaktueller Unterlagen

Da nach Aussage der Anstaltsleitung bei den Beschäftigten zum Teil erhebliche Unsicherheit darüber besteht, welche Schriftstücke aufbewahrt und später archiviert werden müssen und welche der Vernichtung zugeführt werden können, hat der Justizsenator bereits in seiner Vorlage für die Justizdeputation ausgeführt, daß der Erlaß einer Allgemeinverfügung allein nicht ausreichend ist, vielmehr müsse den Mitarbeitern im Justizvollzug der Sinn und die Praktikabilität der Allgemeinverfügung durch Dienstbesprechungen und Fortbildungsveranstaltungen vermittelt werden. Leider wurde damit 1994 noch nicht begonnen.

Dabei sieht die Allgemeinverfügung vor, daß die Standorte der Archive, deren Sicherung sowie der Zugang zum Archiv (personell und technisch) festzulegen sind. Weiter ist für jedes Archiv ein verantwortlicher Bediensteter durch den Anstaltsleiter zu benennen. Die Mindestanforderungen der Verwaltung und Vernichtung des Archivgutes sind festzulegen. Sie betreffen die Art der ordnungsgemäßen Lagerung des Schriftgutes, den Nachweis des Archivgutes in Übersichten, die Ausgabe von Archivgut, die Auskünfte aus archivierten Unterlagen, die Fristenfestlegung und -verfolgung und Vernichtung von Archivgut bzw. die Abgabe an das Staatsarchiv. Wie ich im November 1994 feststellte, war auch mit der Umsetzung wenigstens dieser Regelungen noch nicht begonnen worden.

10.4.4. Neue Aktenfunde

Wie dringlich die rasche Realisierung der neuen Regelungen ist, zeigt ein neuer Vorfall. Ein Gefangener sandte mir in der JVA "abgezweigte" Protokolle über 72 anstaltsinterne Konferenzen aus den Jahren 1978 und 1979 zu.

Die Unterlagen enthielten u.a. Berichte über Vorstrafen, Lebensgeschichten und -verhältnisse sowie Heilbehandlungen und Entziehungskuren früherer Häftlinge. Diese brisanten Unterlagen hätten längst archiviert oder vernichtet werden können, wenn die o.a. Richtlinie praktiziert worden wäre.

Ich habe mich daher sofort an die Anstaltsleitung der JVA Oslebshausen gewandt und dabei auch auf die möglichen Folgen für einzelne Betroffene und deren möglicherweise abgeschlossene Resozialisierung hingewiesen. Neben der Suche nach der Schwachstelle im konkreten Fall geht es nach wie vor um eine deutliche Verbesserung der Aktensicherheit und damit um die konsequente Umsetzung der neuen Anweisungen.

Mir wurde aber zugesichert, daß das Justizvollzugsamt diesen Bereich nunmehr zügig in Angriff nehmen und Archivregelungen für alle Vollzugsanstalten erarbeiten wolle. Nach letzten Informationen im Januar 1995 befindet sich ein solcher Entwurf in der ressortinternen Abstimmung und soll mir dann zur Stellungnahme zugeleitet werden.

10.4.5. Weitere Maßnahmen

Nach der Sommerpause 1994 konnten in mehreren Besprechungen auch die übrigen in meinem Prüfbericht enthaltenen Punkte mit den Verantwortlichen in Justizressort und Haftanstalten abgearbeitet werden. Dazu Beispiele: Vom Justizvollzugsamt wurde eine Allgemeinverfügung zur Anwendung der Vollzugsgeschäftsordnung (VGO) erarbeitet. Hierin werden personelle und organisatorische Maßnahmen zur Umsetzung des ADIV-Verfahrens getroffen. Die Herausgabe und der Rücklauf von Gefangenenpersonalakten aus der und in die Vollzugsgeschäftsstelle wurden neu geregelt. Die Datenverarbeitung im ärztlichen Dienst wurde ebenso neu organisiert wie in die in der Abteilung für kranke Gefangene. Auch die Besucherabwicklung wird 1995 datenschutzfreundlich umgestaltet. Sogar mein Vorschlag, den Gefangenen für Briefe und andere persönliche Unterlagen verschließbare Behälter in den Zellen zu überlassen, wurde realisiert.

10.4.6. Abschluß in Sicht

Die erzielten Ergebnisse sind der Justizdeputation am 27. Januar 1995 vorgestellt worden, ein ganz wesentlicher Teil der Arbeit ist damit erledigt. Hinsichtlich der wenigen noch ausstehenden Arbeitsaufträge habe ich die Hoffnung, daß auch sie noch vor der Sommerpause 1995 von der Justizverwaltung erledigt werden können.

10.4.7. ADV in den Vollzugsgeschäftsstellen (ADIV)

10.4.7.1. Systemkonfiguration

Ende 1993 und im Berichtsjahr ist die Installation und Inbetriebnahme des ADV-Verfahrens im Strafvollzug "ADIV", insbesondere in der Justizvollzugsanstalt Oslebshausen, vorangeschritten.

Der Schwerpunkt der Automatisierung liegt im Bereich der Vollzugsgeschäftsstelle. Der Leiter der Vollzugsgeschäftsstelle, sein Vertreter und die Sachbearbeiter haben die weitestgehenden Benutzerrechte, andere Leitungskräfte auf der Anstalts-, Schicht-, Abteilungs-, Verwaltungs- und Gruppenleiterebene erhalten überwiegend nur lesenden Zugriff auf die für ihre Arbeit erforderlichen Daten.

Daneben wird in der Abteilung für kranke Gefangene ein separater, mit keiner Verbindung nach außen versehener Rechner mit zwei Terminals und Drucker installiert. Ebenfalls Anfang 1995 soll die Pforte der Abteilung am Fuchsberg ein Terminal mit Nutzungsrechten u.a. für die Registrierung von Ausgang und Urlaub erhalten. Der Anschluß weiterer Organisationseinheiten wird 1995 je nach Fertigstellung der jeweiligen Programmteile erfolgen.

10.4.7.2. Maßgeschneidertes Datenschutzkonzept

Es liegt auf der Hand, daß der Einsatz eines solchen komplexen vernetzten Systems eines umfassenden Datenschutzkonzepts bedarf. Dies wird auch vom Justizvollzugsamt Bremen so gesehen, das u. a. mir gegenüber auf folgende Entwicklung hingewiesen hat: "Es hat eine starke Dezentralisierung von Vollzugsaufgaben und eine außergewöhnliche Steigerung des Informationsbedarfs über Insassen innerhalb der Vollzugsanstalten stattgefunden. Dieser Informationsbedarf wird in vielen Fällen zu häufig durch die Mitnahme der kompletten Gefangenenpersonalakte aus den Vollzugsgeschäftsstellen befriedigt; auch dort, wo zur Aufgabenerfüllung nur ein Bruchteil der in ihnen enthaltenen Informationen benötigt wird. Dabei muß betont werden, daß der Begriff "gläserner Mensch" selten so gerechtfertigt ist, wie in der Darstellung manches Insassen in seiner Personalakte. Psychologische Gutachten, Vorgeschichte, soziales Umfeld, Suchtverhalten und -folgen, Kenntlichmachung von Bezugspersonen usw. bilden Datensammlungen in einer Konzentration, die ein Höchstmaß an Datensicherheit erfordert."

Angesichts dieser zutreffenden Einschätzung gab es bei den betroffenen Verantwortlichen große Bereitschaft, parallel mit der Inbetriebnahme des Verfahrens datenschutzrechtliche Standards umzusetzen. In enger Abstimmung mit mir wurde binnen kurzer Zeit für das ADIV-Verfahren ein "maßgeschneidertes" Datenschutzkonzept mit zahlreichen Sicherungsmaßnahmen entwickelt, Ergebnis einer insgesamt gelungenen Kooperation. Ziel war es dabei, neben der Steigerung der administrativen Leistungsfähigkeit die Kontrolle der Verarbeitung personenbezogener Daten der Gefangenen sicherzustellen.

Das Datenschutzkonzept, auf dessen Einzelheiten ich in an dieser Stelle nicht eingehe, wird jeweils mit Inbetriebnahme weiterer Ausbaustufen fortgeschrieben. Die jeweiligen Nutzerrechte der neuen Verfahrensbeteiligten werden in den Verfahrensdokumentationen explizit festgelegt.

Der entscheidende Vorteil der Einführung von ADIV liegt in der erheblichen Reduzierung des anstaltsinternen Datenaustausches.

11. Bildung und Wissenschaft

11.1. Schülerbefragung in Bremerhaven

11.1.1. Die Befragung

Aufgrund einer Eingabe erfuhr ich, daß die Heinrich-Heine-Schule in Bremerhaven bei einem großen Teil ihrer Schüler der 5.-10. Jahrgangsstufe eine Fragebogenerhebung durchgeführt hatte, ohne daß hierfür die Einwilligung der Erziehungsberechtigten eingeholt worden war. Erfragt wurden mit einem 13-seitigen Fragebogen Angaben sowohl zu den häuslichen Lebens- und Lernbedingungen wie auch zu den Gewohnheiten und Ansichten der betroffenen Schüler.

Die Klassenlehrer hatten die Fragebögen in ihren Klassen ausgeteilt, im Unterricht ausfüllen lassen, wieder eingesammelt und schließlich dem Psychologen der Schule zur weiteren Bearbeitung übergeben. Dieser sollte das Datenmaterial aufbereiten und auswerten und die Ergebnisse im Rahmen einer schulinternen Lehrerfortbildung verwenden. Insgesamt waren 242 Fragebögen ausgeteilt und wieder eingesammelt worden. Die betroffenen Eltern, der Elternbeirat der Schule und auch ich waren über die Erhebung nicht unterrichtet worden.

Mit der Schülerbefragung wollte die Schule ihre Schüler besser verstehen lernen. Trotz dieser positiven, pädagogischen Zielen verpflichteten Motivation entsprach die Schülerbefragung nicht den datenschutzrechtlichen Erfordernissen.

11.1.2. Die Rechtslage

§ 13 des Gesetzes zum Datenschutz im Schulwesen (BrSchDSG), der die Befugnis zu Erhebungen, Untersuchungen und wissenschaftlicher Forschung im Schulbereich betrifft, konnte in diesem Fall als Rechtsgrundlage nicht herangezogen werden; es handelte sich weder um eine Erhebung bzw. Untersuchung zur Erfüllung von Aufgaben der Schulbehörde noch um wissenschaftliche Forschung. Die Zulässigkeit der Schülerbefragung mußte vielmehr nach den Regelungen beurteilt werden, die für die Datenverarbeitung der Schulen gelten(§§ 1 - 12 BrSchDSG). Diese Bestimmungen erlauben öffentlichen Schulen die Verarbeitung von Schüler-, Lehrer- und Elterndaten nur insoweit, als dieses zur Erfüllung des Unterrichts- und Erziehungsauftrages der Schule und zur Wahrnehmung ihrer gesetzlichen Mitwirkungsrechte erforderlich ist.

Der in § 2 BrSchDSG festgelegte Umfang der Datenverarbeitung war bei der Erhebung der Heinrich-Heine-Schule erheblich überschritten worden. Von den betroffenen Schülerinnen und Schülern waren Angaben erhoben worden, die bis in ihre intimsten Lebensbereiche hineinreichten. Zum Teil wurde sogar in bestehende Schutzrechte (Adoptionsgeheimnis) eingegriffen. Auch die Bestimmungen des § 4 BrSchDSG, die die Einwilligung und Unterrichtung der Betroffenen, in diesem Fall der Erziehungsberechtigten, sowie die eventuelle Ersetzung der Einwilligung durch den Schulleiter im Einzelfall verlangen und die ausnahmsweise freiwillige Datenerhebung über den in § 2 BrSchDSG genannten Katalog hinaus regeln, waren von der Heinrich-Heine-Schule nicht eingehalten worden. Es mußte leider festgestellt werden, daß die von der Heinrich-Heine-Schule durchgeführte nicht anonyme Erhebungsaktion weder durch eine gesetzliche Erlaubnisnorm noch durch eine Einwilligungserklärung der Betroffenen gerechtfertigt werden konnte.

11.1.3. Die Konsequenzen

Der von mir festgestellte Datenschutzverstoß veranlaßte mich, gegenüber dem Magistrat der Stadt Bremerhaven eine Beanstandung gem. § 29 Abs.1 Nr.2 BrDSG auszusprechen. Zugleich forderte ich die Vernichtung aller von den Schülern ausgefüllten Fragebögen und die Löschung aller sonstigen Daten, die bei der Durchführung der Erhebung bzw. im Hinblick auf die geplante Auswertung der erhobenen Daten evtl. schon entstanden waren.

Zur Verbesserung des Datenschutzes an der Heinrich-Heine-Schule und generell im Schulbereich gab ich darüber hinaus gem. § 29 Abs. 3 BrDSG einige Empfehlungen. U.a. empfahl ich, da der Schulpsychologe stark in das Lehrerkollegium der Schule eingebettet

war und er nach den Bestimmungen des Schulverwaltungsgesetzes eigenständige schweigepflichtige Aufgaben zu erfüllen hat, einige organisatorische Veränderungen hinsichtlich des Aufgaben- und Tätigkeitsbereiches des Schulpsychologen. Des weiteren regte ich eine Überprüfung des gesamten Bereiches der Schuluntersuchungen und der Schulbegleitforschung auf Einhaltung datenschutzrechtlicher Vorgaben an.

Der Magistrat und auch der Senator für Bildung und Wissenschaft teilten mir daraufhin mit, daß sie meine Bewertung der Angelegenheit teilten. Die an der Heinrich-Heine-Schule vorhandenen Unterlagen über die Schülerbefragung wurden vernichtet. In Schulleiterdienstbesprechungen wurde unter meiner Beteiligung über den Datenschutz im Schulwesen referiert und diskutiert. Geprüft wird noch, inwieweit eine andere organisatorische Zuordnung des der Schule zugewiesenen Psychologen zur Absicherung seiner Schweigepflicht möglich ist.

Dieser Vorgang verstärkte die Bemühungen, das Merkblatt zum Datenschutz bei Erhebungen, Untersuchungen und Forschungsvorhaben an öffentlichen Schulen im Lande Bremen fertigzustellen und zu veröffentlichen (vgl. Ziffer 19).

11.2. Erhebungen, Untersuchungen und Forschungsvorhaben an öffentlichen Schulen im Lande Bremen

Ich habe im Berichtsjahr das von mir im letzten Jahresbericht (Ziffer 7.1) angekündigte Merkblatt zum Datenschutz bei Erhebungen, Untersuchungen und Forschungsvorhaben an öffentlichen Schulen im Lande Bremen fertiggestellt. Dieses Merkblatt enthält ausführliche Informationen über die Anwendbarkeit des § 13 BrSchDSG, die Beachtung des Grundsatzes der Einwilligung einschl. der dabei zu berücksichtigenden Formvorschriften, den Grundsatz der frühzeitigen Trennung erhobener personenbezogener Daten vom nichtpersonenbezogenen Datenmaterial sowie das Prinzip der strikten Zweckbindung. Außerdem wird in ihm auf die Unterrichtungsverpflichtung gegenüber dem Eltern- und dem Schülerbeirat, bei Einbeziehung mehrerer Schulen gegenüber den zuständigen Gesamtvertretungen, und meiner Behörde sowie auf den Genehmigungsvorbehalt des Senators für Bildung und Wissenschaft bei wissenschaftlicher Forschung aufmerksam gemacht. Ferner enthält es Hinweise zur Einhaltung der Bestimmungen über die Sicherung der Daten, das Datengeheimnis und über die Erstellung der Dateibeschreibung und des Geräteverzeichnisses (vgl. u. Ziff. 19).

Ich gehe davon aus, daß nach der erfolgten Abstimmung des Textes der Senator für Bildung und Wissenschaft das Merkblatt sowohl den zuständigen parlamentarischen Gremien zur Kenntnis gibt als es auch bei den Betroffenen, d.h. Schulleitungen, Forschern, Elterngremien etc. verteilt.

Für die Durchführung des Genehmigungsverfahrens beim Senator für Bildung und Wissenschaft nach § 13 Abs.7 BrSchDSG -die senatorische Dienststelle ist Genehmigungsbehörde für die Datenverarbeitung zum Zwecke wissenschaftlicher Forschung an Schulen- habe ich eine außerdem eine "Checkliste" erstellt, die die datenschutzrechtlichen Anforderungen enthält, die die Forscher bei ihren Vorhaben zu beachten und der Genehmigungsbehörde darzulegen haben. Diese Checkliste wurde von der senatorischen Behörde nochmals bearbeitet und soll bei künftigen Genehmigungsverfahren zur Beschleunigung der datenschutzrechtlichen Beurteilung beitragen.

11.3. Datenschutz bei Forschungsprojekten

11.3.1. Merkblatt als Handlungshilfe

Die mißglückte Schülerbefragung an der Heinrich-Heine-Schule in Bremerhaven (vgl. o. Ziff. 11.1) ist ein erneutes Beispiel für die verbreitete Unsicherheit von Forschern und sonstigen Projektverantwortlichen beim Umgang mit den einschlägigen datenschutzrechtlichen Spezialvorschriften. Für Erhebungen an Schulen habe ich eine spezielle Handlungsanleitung erarbeitet (s.o. Ziff. 11.2). Darüber hinaus lege ich großen Wert darauf, generell bei bei forschenden Personen und Institutionen mehr Handlungssicherheit herzustellen. Dazu habe ich die wichtigsten zu beachtenden Punkte in einem weiteren Merkblatt

zusammengestellt, das bei mir bezogen werden kann und dessen Inhalt im folgenden wiedergegeben wird.

11.3.2. Ausgangspunkt Einwilligungserfordernis

Ausgangspunkt ist dabei die Sondervorschrift des § 21 des Bremischen Datenschutzgesetzes (BrDSG). Spezielle Bestimmungen gibt es u.a. für Schulen (§ 13 SchulDSchG), Krankenhäuser (§ 7 KHDSG) und die Sozialleistungsträger (§ 75 SGB X). Die Erhebung (d.h. z.B. Fragebogenaktion, mündliche Befragung), Auswertung und Übermittlung personenbezogener Daten zu Foschungszwecken ist danach grundsätzlich nur mit Einwilligung der Betroffenen zulässig. Bei Minderjährigen (z.B. Schülern bis zur Sekundarstufe I) sind auch die Erziehungsberechtigten nach ihrer Einwilligung zu fragen.

Eine wirksame Einwilligung setzt voraus, daß die Forscher den bzw. die Betroffenen über Umfang, Art und Zweck der Nutzung seiner/ihrer persönlichen Angaben im Rahmen des Forschungsprojekts aufklären. Die Freiwilligkeit der Teilnahme am Forschungsprojekt muß klar erkennbar und bei der Durchführung auch faktisch gewährleistet sein (z.B. kein "Gruppendruck" zur Beantwortung).

In der Regel ist die Einwilligung schriftlich zu geben, es sei denn, daß ausnahmsweise eine mündliche, telefonische o.ä. Zustimmung ausreichen muß, weil durch die Einhaltung der Schriftform der Forschungszweck - als z.B. bei telefonischen Befragungen die Beantwortungsquote - erheblich beeinträchtigt würde.

Von der Einwilligung der Betroffenen kann im Einzelfall abgesehen werden, wenn wegen fehlender Sensitivität der Daten, wegen deren Offenkundigkeit - z.B. durch anderweitige Publikation o.ä. - oder wegen der Art der Verarbeitung schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Diese Voraussetzungen allerdings sind nur selten erfüllt, der Verzicht auf die Einwilligung ist in der Forschungspraxis daher nur in wenigen Fällen zulässig.

Sollen Daten nicht bei Betroffenen, also unmittelbar bei Einzelpersonen, erhoben, sondern von bremischen Behörden an den/die Forscher übermittelt werden, bedarf es für die Übermittlung ebenfalls grundsätzlich der Einwilligung. Die oben genannten Ausnahmen vom Einwilligungserfordernis gelten entsprechend. Als zusätzliche Ausnahme braucht die Behörde auch dann keine Einwilligung, wenn eine Abwägung ergibt, daß das öffentliche Interesse an der Durchführung des Forschungsvorhabens die Persönlichkeitsrechte der Betroffenen erheblich überwiegt und feststeht, daß der Forschungszweck bei Einholung der Einwilligungen oder bei Anonymisierung der Angaben vor der Übermittlung nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Forscher bzw. Forschungsgruppen haben bei der jeweiligen Behörde einen schriftlichen Antrag mit Erläuterung des Vorhabens und des genauen Informationsbedarfs zu stellen. Hat der Forscher selbst bereits die Einwilligungen eingeholt,sind die Einwilligungserklärungen beizufügen. Soll auf Einwilligungen verzichtet werden, müssen die Gründe für die Ausnahme erläutert werden.

11.3.3. "File-Trennung", Zweckbindung und Datensicherung

Der Forscher hat, sobald der Forschungszweck dies erlaubt, die Hilfs- bzw. Identifikationsmerkmale von den übrigen Daten zu trennen und getrennt zu speichern (Prinzip der File-Trennung). Auswertungen erfolgen nur aus den nicht-personenbezogenen Datenbeständen. Auf die Datei mit den Personalien darf nur im Bedarfsfall und von ausdrücklich dazu ermächtigten Projektmitarbeitern zurückgegriffen werden. Sie muß spätestens dann gelöscht werden, wenn das Forschungsprojekt beendet ist.

Die beim Betroffenen erhobenen oder von bremischen Behörden übermittelten Daten dürfen nur für das jeweilige Forschungsprojekt und im Rahmen der Einwilligung bzw. der Angaben im Antrag ausgewertet werden (Prinzip der Zweckbindung).In diesem Rahmen dürfen sie ggf. - allerdings nur zu Forschungszwecken - auch an andere Forschungsstellen weiterübermittelt werden. Haben Behörden Daten ohne Einwilligung an den Forscher weitergegeben, ist vor einer Weitergabe durch den Forscher die Einwilligung bei den Betroffenen einzuholen.

Konkrete Datensicherungsmaßnahmen (vgl. § 6 BrDSG) müssen sich auf die Gestaltung und den Ablauf des gesamten Projekts beziehen. Sie sind bereits bei der Planung projektspezifisch zu definieren. Maßnahmen sind zu treffen für die Erhebungsphase (z.B. Gewährleistung der Freiwilligkeit, Verhinderung des Einblicks Unbefugter bei Fragebogenaktionen), für die Auswertungsphase (z.B. "File-Trennung", namentliche Festlegung der Zugriffsbefugten, Überprüfung der Ausdrucke auf Reidentifizierbarkeit) und für die Phase nach Abschluß des Projekts (z.B. Vernichtung des Rohmaterials, Löschung von ADV-Datenträgern).

11.3.4. Genehmigungsvorbehalte

Für wissenschaftliche Forschungsvorhaben in Schulen gilt zusätzlich (vgl. § 13 SchulDSG): Sie bedürfen der Genehmigung durch den Senator für Bildung und Wissenschaft. Der Landesbeauftragte für den Datenschutz, der Elternbeirat und der Schülerbeirat sowie bei Einbeziehung mehrerer Schulen die zuständigen Gesamtvertretungen sind vor der Durchführung zu unterrichten. Die Unterrichtung an den Landesbeauftragten muß eine detaillierte Beschreibung des Ablaufs des Projekts und die vorgesehene Datenverarbeitung enthalten (vgl. o. Ziff. 11.2).

Für Erhebungen im Sozialleistungsbereich bedarf es ebenfalls der Genehmigung durch den zuständigen Senator (z.B. Senator für Arbeit und Frauen oder Senator für Gesundheit, Jugend und Soziales). Projekte mit Patientendaten in bremischen Krankenhäusern (außer kirchlichen) sind dem Gesundheitssenator anzuzeigen, der Datenschutzbeauftragte des jeweiligen Krankenhauses ist zu beteiligen.

Bei Zweifeln und Unklarheiten in bezug auf die datenschutzrechtlich korrekte Durchführung von Forschungsvorhaben empfehle ich in jedem Fall eine Rückfrage bei meiner Dienststelle.

11.4. Öffentlicher Aushang von Klausur- und Prüfungsergebnissen

11.4.1. Erster Fall: Hochschule Bremen

11.4.1.1. Mißglückte Verwaltungsvereinfachung

Der AStA eines Fachbereiches der Hochschule Bremen beklagte sich bei mir darüber, daß im Rahmen eines Zulassungsverfahrens zu einem Studienabschnitt getroffene Entscheidungen öffentlich bekannt gegeben worden waren. Auf Listen wären an allgemein zugänglicher Stelle im Fachbereich unter vollständiger Nennung von Namen und Matrikelnummern die Noten und Notendurchschnitte zugelassener und abgelehnter Studierender ausgehängt worden.

Die verantwortliche Fachbereichsleitung der Hochschule bestätigte diese Angaben. Zugleich wies sie darauf hin, daß die Studierenden auf die öffentliche Bekanntmachung der Zulassungsentscheidungen bereits im Veranstaltungsverzeichnis für das Semester aufmerksam gemacht worden wären, so daß sie bereits vor dem Aushang ihrer Daten hiervon Kenntnis erlangen konnten. Außerdem sei aufgrund fehlender personeller Kapazitäten eine Versendung der Zulassungsentscheidungen an die einzelnen Betroffenen auf dem Postwege nicht möglich gewesen.

Das von der Hochschule Bremen durchgeführte Verfahren ist sowohl mit verwaltungswie auch mit datenschutzrechtlichen Bestimmungen nicht zu vereinbaren. Die Entscheidung über die Zulassung einer bzw. eines Studierenden zu einem Studienabschnitt stellt einen Verwaltungsakt im Sinne des Bremischen Verwaltungsverfahrensgesetzes(BremVwVfG) dar, der gem. § 41 Abs.1 BremVwVfG demjenigen Beteiligten bekanntzugeben ist, für den er bestimmt ist oder der von ihm betroffen wird.

Öffentlich hätte die Zulassungsentscheidung gem. § 41 Abs.3 BremVwVfG nur bekannt gegeben werden dürfen, wenn dies durch Rechtsvorschrift ausdrücklich zugelassen gewesen wäre. Eine solche Vorschrift sehe ich nicht. Die Bekanntmachung im Veranstaltungsverzeichnis, daß die Zulassungsentscheidungen oder die Klausurergebnisse am Schwarzen Brett bekannt gemacht werden, reicht in diesem Zusammenhang nicht aus.

Die Übermittlungsbestimmungen des Bremischen Datenschutzgesetzes erlauben den Aushang der Zulassungsentscheidungen in der kritisierten Form ebenfalls nicht. Er wäre nur zulässig gewesen, wenn die Betroffenen hierzu gem. § 3 Abs. 1 BrDSG ihre Einwilligung erteilt hätten. Dies war jedoch nicht der Fall.

11.4.1.2. Datenschutzgerechte Alternativen

Soweit eine direkte Benachrichtigung der Studierenden, z.B. mit einem entsprechenden Anschreiben, nicht möglich war, hätte somit darauf geachtet werden müssen, daß grundsätzlich nur die jeweils Betroffenen, nicht aber alle Personen, denen der kritisierte Aushang zugänglich war, von den Entscheidungen Kenntnis nehmen konnten. Beim Aushang der Entscheidungen hätten deshalb zumindest die Namen der Betroffenen weggelassen werden müssen. Die Matrikelnummer, die dann noch die Identifizierung der einzelnen Studierenden ermöglicht hätte, ist nicht allgemein, sondern in der Regel nur dem Betroffenen selbst, bekannt. Besser noch wäre es gewesen, wenn die Zulassungsentscheidungen nicht ausgehängt, sondern im Sekretariat des Fachbereichs deponiert und dort den jeweiligen Studierenden von einer Verwaltungskraft ausgehändigt worden wären.

Den unzulässigen Aushang der Zulassungsentscheidungen rügte ich gegenüber der Hochschule Bremen. Zugleich forderte ich sie auf, künftig generell in allen Fachbereichen, auch beim Aushang der Ergebnisse von Klausuren, Hausarbeiten etc., entsprechend zu verfahren. Die Hochschule erließ daraufhin eine Dienstanweisung, mit der der von mir vertretenen Auffassung Rechnung getragen wird.

11.4.2. Zweiter Fall: Universität Bremen

Eine vergleichbare Eingabe erhielt ich später von einem Studierenden der Universität Bremen. Dieser beklagte sich darüber, daß in seinem Fachbereich die Ergebnisse von Klausuren mit den Namen und Matrikelnummern der betroffenen Studierenden öffentlich ausgehängt wurden. Die Prüfung des Vorganges ergab, daß auch in diesem Fall die Daten der Betroffenen unzulässigerweise bekannt gegeben worden waren.

Der Rektor der Universität nahm den Fall zum Anlaß, alle Fachbereiche bzw. mit der Durchführung von Prüfungsverfahren befaßten Stellen zu einer datenschutzkonformen Praxis bei der Bekanntgabe von Prüfungsergebnissen anzuhalten. Er forderte dazu auf, künftig bei der Bekanntgabe von Klausur- und vergleichbaren Prüfungsergebnissen durch öffentlichen Aushang auf die Nennung der Namen der Betroffenen zu verzichten.

12. Gesundheit, Jugend und Soziales

12.1. Krankenhäuser

12.1.1. Fall: Patientendaten im Maßregelvollzug

Ein Patient im Maßregelvollzug (d.h. Unterbringung eines schuldunfähigen oder vermindert schuldfähigen strafrechtlich Verurteilten nach § 63 StGB in der forensischen Klinik des Zentralkrankenhauses Bremen-Ost) hatte sich mit einer Reihe von datenschutzrechtlichen Beschwerden an mich gewandt. Bei einer örtlichen Prüfung und in Gesprächen mit den Verantwortlichen im Krankenhaus und beim Senator für Gesundheit, Jugend und Soziales stellte sich heraus, daß einige Beschwerden berechtigt waren. Inzwischen hat die Klinikleitung dem Rechnung getragen.

Künftig sollen vor dem Besuch eines Patienten bei einem auswärtigen Arzt die Sicherheitsaspekte abgeklärt und mit dem Patienten erörtert werden. Wenn möglich, soll vermieden werden, daß ein Pfleger während der ärztlichen Konsultation oder Untersuchung anwesend ist. Ist dies aber aus Sicherheitsgründen nicht zu vermeiden, so soll vorher abgeklärt werden, ob der Patient bereit ist, unter den vorgegebenen Umständen den Termin wahrzunehmen oder ob er lieber auf ihn verzichten möchte. So soll vermieden werden, daß - wie Gegenstand der Beschwerde war - der Patient mit der Gegenwart eines Dritten bei der Konsultation oder Untersuchung konfrontiert wird. Auch er muß - soweit Sicher-

heitserfordernisse dem nicht entgegenstehen - einen Arzt seines Vertrauens unter dem Schutz des gesetzlich sanktionierten Arztgeheimnisses konsultieren können.

Die Klinikleitung hat eine schriftliche Regelung zur Einsicht in Krankenakten durch ihr nichtärztliches Personal getroffen. Zwar setzt die Behandlung in Teamarbeit voraus, daß neben den Ärzten auch die Pfleger umfassend über die Patienten, ihre Störungen und ihre Entwicklungsgeschichte informiert sind. Dennoch aber bedarf es nunmehr des Einverständnisses des Arztes, will ein Pfleger Einsicht in die Akte mit der Krankengeschichte nehmen.

Die neuen Regelungen versuchen, die Persönlichkeitsrechte der Patienten und die ärztliche Schweigepflicht in dem Maße zu wahren, als diese nicht durch die Ziele des Maßregelvollzugs und Sicherheitserfordernisse eingeschränkt werden müssen. Ich habe die Regelungen deshalb als datenschutzgerecht akzeptiert.

12.2. Gesundheit

12.2.1. Zweckbindung der Klientendaten trotz Funktionsvielfalt der Gesundheitsämter

Der Senat hat Ende Februar 1995 den Entwurf für ein Bremisches Gesetz über den öffentlichen Gesundheitsdienst verabschiedet. Der Abschnitt zum Datenschutz im Referentenentwurf ist mit mir abgestimmt worden. Insbesondere stellt er klar, daß die Daten, die die Gesundheitsämter zum Zwecke freiwilliger Beratung erhoben haben, grundsätzlich nicht für Überwachungs- und Zwangsmaßnahmen genutzt werden dürfen. Dies entspricht meiner langjährigen Forderung (vgl. bereits 12. JB Ziff. 2.7.12, zuletzt 16. JB Ziff. 8.5.1).

Allerdings gibt es Situationen, in denen Ausnahmen von diesem Grundsatz unumgänglich sind, etwa in Fällen, in denen andernfalls eine gegenwärtige Gefahr besteht, daß der Kranke Selbstmord begeht oder sich erheblichen gesundheitlichen Schaden zufügt. Dann bedarf es aber für die Nutzung von Daten, die im Rahmen freiwilliger Beratung einem Arzt oder Psychologen z.B. des sozialpsychiatrischen Dienstes eines Gesundheitsamtes anvertraut worden sind, im Rahmen einer Entscheidung über eine Zwangseinweisung einer eindeutigen gesetzlichen Befugnis. Diese sollte möglichst bald durch eine Ergänzung des Bremischen Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankenheiten (PsychKG) vorgenommen werden. Auch die Besuchskommission nach § 34 PsychKG hat in Ziffer 5 ihres letzten Berichts (Drucks. der Bremischen Bürgerschaft (Landtag), 13/1040 vom 17.11.94) Vorschläge zur Novellierung des PsychKG gemacht. Dies verbessert die Chancen für eine datenschutzgerechte Neufassung dieses Gesetzes. Ich hoffe auf Fortschritte in diesem Bereich in der nächsten Wahlperiode.

12.2.2. Anonymität in der Schwangerschaftskonfliktberatung und beim Sozialamt

12.2.2.1. Anerkennungsrichtlinien für Beratungsstellen

Zum 01.01.1995 sind die Richtlinien über die behördliche Anerkennung von Stellen zur Schwangerschaftskonfliktsberatung im Lande Bremen in Kraft getreten. Der Senator für Gesundheit, Jugend und Soziales hat darin meine Vorschläge zur Sicherstellung des Wunsches von Schwangeren auf Wahrung ihrer Anonymität während der Beratung und zur Anonymisierung der einzelfallbezogenen Unterlagen der Beratungsstellen aufgegriffen (vgl. Ziff. 8.5.3 meines 16. Jahresberichts). Den Persönlichkeitsrechten schwangerer Frauen ist dadurch in dem vom Bundesverfassungsgericht in seinem Urteil zum Schwangerschaftsabbruch vom 28.05.1993 vorgegebenen Rahmen soweit wie möglich Rechnung getragen worden.

Die Beratungsstellen haben die ratsuchenden Schwangeren in geeigneter Form darauf aufmerksam zu machen, daß sie sich anonym beraten lassen können. Wenn die Schwangere eine anonyme Beratung gewünscht hat, ist ihr Gelegenheit zu geben, selbst ihren Namen in die über die Beratung auszustellende Bescheinigung für den Arzt einzutragen oder die Bescheinigung durch eine Person ausstellen zu lassen, die am Beratungsgespräch

selbst nicht beteiligt war. Bei der Ausgestaltung des Protokolls, das die Beratungsstelle über die Beratungsgespräche zu erstellen hat, wird jeder Personenbezug ausgeschlossen.

Ich gehe davon aus, daß die Vorgaben des Bundesverfassungsgerichts zur Wahrung der Anonymität der Schwangeren unverändert Eingang finden in die gesetzliche Neuregelung, die derzeit im Deutschen Bundestag vorbereitet wird.

12.2.2.2. Anonymität bei der Antragstellung für Sozialhilfe

Im Lande Bremen wird derzeit Hilfe für die Kosten eines Schwangerschaftsabbruches aus Mitteln der Sozialhilfe geleistet. Ich habe deshalb jüngst die Sozialhilfeträger gefragt,

- welche Vorkehrungen sie getroffen haben, das Sozialgeheimnis schwangerer Hilfesuchender besonders zu schützen,
- ob über die Hilfe für Schwangerschaftsabbrüche in einem gesonderen Verfahren entschieden wird,
- welche Daten in diesem Zusammenhang erhoben, wie sie gespeichert (d. h. zusammen mit dem für andere Hilfearten erhobenen Daten oder getrennt von diesen), an welche Stellen die Daten weitergeben und wann sie gelöscht werden.

Ich habe in diesem Zusammenhang daran erinnert, daß die - letztlich gescheiterten - Beschlüsse des Bundestages und des Bundesrates aus der letzten Legislaturperiode für gesetzliche Regelungen zur Umsetzung des Urteils des Bundesverfassungsgerichts jeweils Regelungen vorsahen, die die Kostenträger, gleich ob dies die Sozialhilfeträger oder die Krankenkassen sein sollten, verpflichten wollten, das Persönlichkeitsrecht der hilfesuchenden Schwangeren besonders zu achten - bzw. die Schwangerschaftsabbrüche betreffenden Daten von anderen Daten zu trennen.

12.3. Jugend und Soziales

12.3.1. Sozialhilfe per Computer - neues Datenschutzkonzept für das PROSOZ-Verfahren

Das mir im November 1994 vorgelegte neue Datenschutzkonzept für das dialogorientierte Sozialhilfeberechnungsverfahren PROSOZ stellt insgesamt eine Anpassung der Konzeption an die Weiterentwicklung des Systems dar. Ich schildere die Funktionsänderungen sowie die vorgesehenen technischen und organisatorischen Maßnahmen im folgenden deshalb so ausführlich, weil sie exemplarisch sind für die Komplexität sowohl moderner Verwaltungsinformationssysteme als auch der ihr adäquaten Beratungstätigkeit des Datenschutzbeauftragten.

12.3.1.1. Erweiterung der Textverarbeitung

Die Erweiterung der einzelnen Sachbearbeiter/-innenarbeitsplätze um eine Textverarbeitungssoftware ist in allen wesentlichen Aspekten im neuen Datenschutzkonzept berücksichtigt worden.

Es ist jedoch nicht gelungen, den bisher festgelegten Datenschutzstandard zu halten. Durch die Möglichkeit der Speicherung von Texten mit personenbezogenen Daten ist eine Öffnung des Systems entstanden. Im Rahmen einer Dienstanweisung sind zwar sowohl das Verzeichnis, in das diese Texte gespeichert werden dürfen, als auch die Dateiendung festgelegt. Es ist jedoch jederzeit möglich, die Texte in anderen Verzeichnissen zu speichern und/oder eine andere Dateiendung zu wählen und sie so der automatischen Löschroutine zu entziehen. Im vorhergehenden Verfahren war dieses technisch nicht möglich.

Die Integration von Textverarbeitungsfunktionen führt zu einer Kontrollücke, die gegenüber der vorher gegebenen technischen Geschlossenheit des Systems nur unzulänglich durch die schwächere Maßnahme der Dienstanweisung kompensiert werden soll. Es ist deshalb zusätzlich notwendig, eine regelmäßige Kontrolle der Festplatten durch den Datenschutzbeauftragten des Senators für Gesundheit, Jugend und Soziales durchzuführen.

Darüberhinaus besteht die Möglichkeit, über die Windows-Oberfläche (unter der die Textverarbeitung läuft) auf PROSOZ zuzugreifen. Damit kann der PROSOZ-Paßwortschutz umgangen werden, sodaß die in § 78a SGB X geforderten technischen Datenschutzmaßnahmen zum Schutz personenbezogener Daten faktisch für das PROSOZ-System aufgehoben sind. Es ist deshalb dringend erforderlich, den Zugang zu den Windows-Funktionen auf gleichem Niveau zu schützen wie den Zugang zum PROSOZ-Verfahren.

12.3.1.2. ADV-Verbindungsstelle

Die ADV-Verbindungsstelle soll in besonderen Fällen nach Veranlassung durch die zuständigen Sachbearbeiter auf einzelne Echtdaten zugreifen können.

In meinem letzten Jahresbericht (vgl. 16.JB, Ziff. 8.7.2) hatte ich gefordert, daß die ADV-Verbindungsstelle im Rahmen von Koordinations- und Weiterentwicklungsaufgaben wie unter Punkt 1.6.2 des alten Datenschutzkonzeptes festgelegt, weiterhin keinen Zugriff auf Echtdaten, sondern nur auf eine Testdatenbank haben darf.

Bei meinem Prüfbesuch im letzten Jahr wurde mir jedoch plausibel gemacht, daß durch eine Erweiterung der Aufgabenstellung der ADV-Verbindungsstelle (Hilfestellung bei technischen Bearbeitungsproblemen in der Fallsachbearbeitung im Einzelfall) der Zugriff auf Echtfälle erforderlich sein kann. Diesem Zugriff habe ich unter der Bedingung zugestimmt, daß neben anderen zusätzlichen technischen und organisatorischen Maßnahmen die uneingeschränkte Zuweisung von Zugriffsrechten fallbearbeitender Sachbearbeiter/-innen für und durch die ADV-Verbindungsstelle verhindert wird. Dieses wurde auch in der Sitzung vom 4.11.94 des Datenschutzausschusses der bremischen Bürgerschaft von einem Vetreter der senatorischen Dienststelle zugesagt. In der neuen Fassung des Datenschutzkonzeptes vom 17.11. 94 sind jedoch noch keine neuen Regelungen enthalten.

Folgende Ergänzungen sind für eine datenschutzgerechte Arbeitsgrundlage der ADV-Verbindungsstelle erforderlich:

- Dem vollen Zugriff der ADV-Verbindungsstelle auf die Falldaten muß eine Freigabe dieser Daten durch die zuständige Sachbearbeitung revisionsfähig vorausgehen.
- Erst dann darf eine Rechteübernahme durch die ADV-Verbindungsstelle erfolgen.
- Der Zwangsausdruck bei Rechteübernahme sollte im Bereich der Fallsachbearbeitung erfolgen.

Die konkrete Umsetzung dieser optimalen Datenschutzbedingungen würde nach Aussage der ID-Bremen einen unverhältnismäßig großen technischen Aufwand erfordern, so daß die Datensicherheit zunächst durch folgendes Verfahren erreicht werden soll:

- Die ADV-Verbindungsstelle darf nur nach telefonischer Anforderung durch die fallbearbeitenden Sachbearbeiter/-innen mithilfe entsprechender Rechteübernahmen Zugriff auf die Falldaten haben.
- Die Speicherfunktion wird gesperrt, sodaß die ADV-Verbindungsstelle keine Veränderungen in den Datensätzen der Falldatenbank vornehmen kann.
- Zusätzlich werden dort alle Echtfallzugriffe in eine Liste eingetragen. Die Liste enthält das Datum, das Organisationskennzeichen, das Aktenzeichen, eine Kurzbeschreibung des Problems und das Datum der Erledigung. Volle Listen werden in Kopie dem ID-Bremen-PROSOZ-Team zugesandt.
- Die Erteilung der Zugriffsberechtigungen an die ADV-Verbindungsstelle werden durch einen automatisch erstellten Beleg dokumentiert. Die Belege werden in einem gesonderten Hefter gesammelt und vier Jahre aufbewahrt.

Da sich dieses Dokumentationsverfahren in den Händen der ADV-Verbindungsstelle selbst befindet, sind die Zugriffe der ADV-Verbindungsstelle dennoch nicht revisionsfähig. Die Speicherung der auf die Mitarbeiter/-innen der ADV-Verbindungsstelle übertragenen Zugriffsrechte in einer gesonderten Datei der ID-Bremen, mit der dieses Problem

gelöst wäre, wird aufgrund des von der ID-Bremen aufgeführten hohen Programmier-und Kostenaufwandes von der senatorischen Dienststelle nicht weiter verfolgt. Da keine Online-Protokollierung stattfindet, wird zur Ausübung meiner Kontrollfunktion die Systemprotokollierung entsprechend den datenschutzrechtlichen Fragestellungen von ID-Bremen aufbereitet und spätestens innerhalb von zwei Tagen zur Verfügung gestellt.

Die im vorangegangen Text beschriebenen Funktionserweiterungen im Rahmen der automatisierten Sozialhilfesachbearbeitung stellen sicherlich eine gewisse Erleichterung für die konkrete Arbeitssituation da, gleichzeitig haben sie zu einem Absinken des Datensicherungsniveaus geführt. Der parallel zur PROSOZ-Systemerweiterung zu betreibende Aufwand zur Erhaltung des ursprünglichen Datenschutzniveaus wird leider eher als unverhältnismäßig eingestuft als der Aufwand für die Systemerweiterung selbst.

Ich werde deshalb in diesem Jahr die Wirksamkeit der als Kompromißlösung zwischen dem Senator für Gesundheit, Jugend und Soziales und mir vereinbarten Datensicherungsmaßnahmen bzw. deren Installation überprüfen.

12.3.2. Datenverarbeitung und Statistik nach dem Betreuungsgesetz

12.3.2.1. Mitteilungen und Statistik der Vormundschaftsgerichte

Am 01.01.1992 ist das Betreuungsgesetz in Kraft getreten. Als Teil seines Bestrebens, die Persönlichkeitsrechte der Betroffenen besser zu achten als die früheren Bestimmungen zur Entmündigung und zur Pflegschaft ist nunmehr im einzelnen geregelt, an welche anderen Stellen unter welchen Voraussetzungen das Vormundschaftsgericht Entscheidungen über die Bestellung eines Betreuers mitteilen muß oder darf (§§ 69a, 69k des Gesetzes über die freiwillige Gerichtsbarkeit). Früher üblichen Praktiken wie etwa regelmäßigen Mitteilungen von Entmündigungen an Kfz-Zulassungsstellen ist damit schon vom Gesetzswortlaut her die rechtliche Grundlage entzogen worden.

Daneben aber werfen das Gesetz, die landesrechtlichen Ausführungsbestimmungen und seine Handhabung in der Praxis eine Reihe datenschutzrechtlicher Probleme auf, zu deren Lösung ich im Benehmen mit den zuständigen Stellen beizutragen versucht habe.

12.3.2.1.1. Datenschutz für Betreute

Zum einen ging es um den vorrangigen Schutz der personenbezogenen Daten Betreuter:

Der Senator für Gesundheit, Jugend und Soziales als überörtliche Betreuungsbehörde entwickelte in Abstimmung mit mir für seine automatisierte Geschäftsstatistik zur Auswertung der Mitteilungen der Vormundschaftsgerichte an die Betreuungsbehörden ein Datenschutzkonzept, wonach zur Vermeidung von Mehrfachzählungen etwa in Folge von Beschlüssen zur Veränderung des Wirkungskreises oder zum Betreuerwechsel lediglich die Aktenzeichen erfaßt werden und dieses Datenfeld noch einmal durch verdeckte Ausgaben zusätzlich gegen unbefugten Zugriff zugesichert ist.

Das Amtsgericht (Vormundschaftsgericht) entwickelte in Abstimmung mit den Betreuungsvereinen und mir ein Verfahren, wonach nicht mehr wie bisher die Vormundschaftsakten den Betreuungsvereinen zwecks Überlegung, ob ein geeigneter ehrenamtlicher Betreuuer genannte werden kann, zur Kenntnis gegeben werden, sondern wonach die Betreuungsvereine ihrerseits dem Gericht potentielle Betreuer mit Art und Umfang der gewünschten Betreuung benennen, das Gericht dann seinerseits einem der Vereine einen nicht personenbezogenen Aktenauszug zuleiten kann, damit dieser einen geeigneten Betreuer vorschlagen kann.

12.3.2.1.2. Datenschutz für Betreuer

Zum anderen aber ging es um den Schutz personenbezogener Daten von Betreuern oder solcher Personen, die hierfür in Frage kommen:

Die überörtliche Betreuungsbehörde stellt aus den ihr zugänglichen Meldungen über die Bestellung von Betreuern den anerkannten Betreuungsvereinen Listen von Anschriften von Betreuern zwecks Bekanntmachung ihrer jeweiligen Einführungs-, Fortbildungs- und

Beratungsangebote zur Verfügung. Da eine Aufgabe der Betreuungsvereine die Fortbildung und Beratung von Betreuern ist (§ 1908 f BGB) und die überörtliche Betreuungsbehörde sie bei der Erfüllung ihrer Aufgaben unterstützen soll (§ 4 Bremisches Ausführungsgesetz zum Betreuungsgesetz), habe ich diese Übermittlungen akzeptiert, aber zugleich darauf gedrungen, daß vor Zusendung der Anschriften die Betreuungsvereine die schriftliche Erklärung abgeben müssen, sie würden die Anschriften nur zu den genannten Zwecken nutzen. Die überörtliche Betreuungsbehörde hat meinen Vorschlag aufgegriffen.

Laut § 6 des Bremischen Ausführungsgesetzes zum Betreuungsgesetz kann die überörtliche Betreuungsbehörde anerkannte Betreuungsvereine nach Maßgabe der Haushaltsmittel und per Richtlinie festgesetzter Voraussetzungen finanziell fördern. Die Betreuungsvereine sollen in diesem Zusammenhang den Nachweis führen, daß sie mindestens über 25 namentlich nachgewiesene Personen "verfügen", die Betreuungen übernommen haben oder doch bereit sind, Betreuungen zu übernehmen. Grundsätzlich habe ich diese Methode der Überprüfung akzeptiert. Es ist inzwischen aber sichergestellt, daß nur die Namen von solchen Personen, die schon Betreuer sind oder doch dem Vormundschaftsgerichts gegenüber benannt worden sind, aber nicht die Namen an Betreuungen lediglich Interessierter der überörtlichen Betreuungsbehörde übermittelt werden. Überdies soll zuvor die Einwilligung der Betroffenen eingeholt werden.

Schließlich hat die überörtliche Betreuungsbehörde meine Forderung aufgegriffen, in ihrer Geschäftsstatistik nur noch anonymisierte Daten zu erfassen. Die Geschäftsstatistik ist von den Dateien, die auch Namen von Betreuern enthalten, separiert worden.

12.3.3. Sozialhilfestatistik- das Sozialamt als Zähler

Das Gesetz zur Umsetzung des förderalen Konsolidierungsprogramms (sog. Solidarpakt, in Kraft getreten am 01.07.93) trifft auch eine umfassende Neuregelung der Bestimmungen über Sozialhilfestatistiken - erklärtermaßen in der Erwartung von Einspareffekten und verbesserten Informationsgrundlagen zur Vermeidung von Mißbrauch. Dem sollen sowohl die Fortentwicklung des Erhebungsverfahrens als auch die Erweiterung der Erhebungsmerkmale dienen.

Eines aber wurde nicht geändert: Nach § 131 BSHG sind nach wie vor nicht die Hilfeempfänger, sondern die Träger der Sozialhilfe zur Auskunft verpflichtet. Diese aber dürfen ihrerseits nur die Daten erheben, die sie für ihre Aufgabenerfüllung, d. h. die Hilfegewährung und ihre Abwicklung benötigen (§ 67 a Abs. 1 SGB X). Die Hilfeempfänger ihrerseits sind lediglich gehalten, die Tatsachen mitzuteilen, die für die Entscheidung über ihren Antrag oder die Weitergewährung der Hilfe erheblich sind (§ 60 Abs. 1 SGB I). Hierzu aber gehören nicht in allen Fällen alle der neuerdings zu den Erhebungsmerkmalen der Sozialhilfestatistik gehörenden Daten. Z.B. ist zwar häufig, aber nicht immer für den Einzelfall erheblich, welchen Schul- oder Berufsausbildungsabschluß ein 15- bis 65jähriger Hilfeempfänger hat, so etwa nicht bei alleinstehenden Müttern von Kleinkindern oder im Falle kurzfristiger Überbrückungdarlehen.

Eine Datenverarbeitung auf Vorrat für künftig vielleicht auftretende Notwendigkeiten aber ist unzulässig. Insoweit sind Hilfeempfänger nicht gehalten, Angaben zu machen, Leistungsträger nicht befugt, Daten zu erheben. Diese Rechtslage hatte der Gesetzgeber des Solidarpakts offenbar nicht bedacht. Nicht nur Datenschutzbeauftragte in Bund und Länder, sondern auch oberste Landesaufsichtsbehörden über Sozialhilfeträger haben inzwischen hierauf hingewiesen.

Dennoch aber haben die statistischen Landesämter bundesweit einen Erhebungsbogen herausgegeben, der die Erhebung auch solcher Merkmale generell vorsieht, die nicht in jedem Einzelfall erheblich sind. Entsprechend wurde - wie mir mitgeteilt wurde - das automatisierte Verfahren zur Sozialhilfezahlung PROSOZ in der Stadtgemeinde Bremen geändert.

Bei einer Besprechung im Juni 1994 im Hause des Senators für Gesundheit, Jugend und Soziales wurde Einigkeit dahingehend erzielt, daß den Sachbearbeitern und Sachbearbeiterinnen ermöglicht werden solle, die Angabe "unbekannt" oder "keine der vorgenannten

sozialen Situationen" einzugeben, falls im Einzelfall eine Datenerhebung unzulässig ist. Inzwischen hat das Ressort mitgeteilt, PROSOZ sei in seiner neuesten Version entsprechend geändert worden. Die Sachbearbeiter/innen seien auch darauf hingewiesen worden, sie könnten bei den Schul- und Berufsausbildungsabschluß "unbekannt" eingeben, wenn eine Eingliederung in das Berufsleben nicht möglich sei.

12.3.4. Fall: Jugendamtsakten auf dem Schuttcontainer

Zuweilen sind es recht rätselhafte Vorfälle, die mich veranlassen, die Einhaltung des Datenschutzes zu überprüfen. So übergab mir ein Lkw-Fahrer drei Akten des ehemaligen Jugendamts Bremen (inzwischen Teil des Amtes für Soziale Dienste), Abteilung Amtsvormundschaft/Amtspflegschaft. Er habe sie, berichtete er glaubhaft, oben auf einem mit Bauschutt gefüllten Container vor einer Baustelle am Flughafen Bremen gefunden.

Da es in den Vortagen geregnet hatte, die Akten aber kaum in Mitleidenschaft gezogen waren, waren sie offensichtlich erst kurz vor dem Fund auf den Schutt gelangt. Die Akten waren in den Jahren 1984/85 abgeschlossen und an das Archiv des Amtes abgegeben worden. Eine spätere Nutzung ist in ihnen nicht vermerkt. Sie enthalten jeweils eine Fülle von Sozialdaten der Klienten und ihrer Familien.

Zu deren Schutz aber sind die Sozialleistungsträger verpflichtet, die erforderlichen technischen und organisatorischen Maßnahmen einschließlich Dienstanweisungen zu treffen. Einschlägige Rechtsgrundlage war bis zum bis 30.06.94 die Vorschrift des § 35 Abs. 1 Satz 2 SGB I, seit der Novellierung des Sozialdatenschutzes gilt § 78 a SGB X. Dadurch soll u.a. auch verhütet werden, daß Sozialdaten in die Hände Unbefugter geraten.

Eine Ortsbegehung sowie Gespräche mit den Mitarbeiter/innen des Amtes, die auf die eine oder andere Weise befugt Zugang zu den Akten hatten, und dem für das zentrale Altarchiv des Amtes Verantwortlichen brachten nicht den geringsten Hinweis für den Weg der Akten auf den Schuttcontainer. Es gab weder einen Hinweis auf befugte Nutzungen nach der Übergabe an das Archiv noch auf eine unbefugte Entwendung der Akten. Das Amt versicherte später gleichfalls, daß seine Bemühungen um eine Aufklärung des Sachverhalts ohne Ergebnis geblieben seien.

Es wurde aber schnell deutlich, daß das Sozialgeheimnis früherer Klienten des Jugendamtes nicht ausreichend geschützt war. So war der Keller des Hauses, in dem das Altarchiv in Räumen untergebracht ist, deren Türen nur mit einfachen Schlössern gesichert sind, frei zugänglich. Dieser Mangel wurde umgehend durch den Einbau von Sicherheitsschlössern und eine sehr restriktive Ausgabe der Schlüssel beseitigt.

Vor allem aber fehlte eine vollständige Suchkartei aller archivierten Altakten, in der Datum, anfordernde Stelle und Begründung der Anforderung sowie die Rückgabe der Akten registriert werden. Dem soll - so wurde mir jüngst versichert - jedenfalls für den Bereich der Amtsvormundschaft/Amtspflegschaft mit der angestrebten Einführung eines ADV-Verfahrens abgeholfen werden. Vorläufig würden für diesen Bereich Vordrucke eingeführt, mit deren Hilfe die Übergabe einer Akte zur Archivierung sowie die Anforderung einer Akte aus dem Archiv durch die Amtsvormundschaft/Amtspflegschaft dokumentiert werden sollten.

12.3.5. Fall: Intime Fragen nach "eheähnlicher Gemeinschaft"

Eine Sozialhilfeempfängerin wandte sich an mich und klagte darüber, daß das Amt für Soziale Dienste Bremen Fragen nach ihrem Privatleben gestellt und von ihrer Antwort die Weitergewährung von Sozialhilfe abhängig gemacht habe. Das Amt wollte von ihr Namen und Anschrift ihres Freundes wissen und wie oft er sich durchschnittlich monatlich in ihrer Wohnung aufhalte.

Diese Datenerhebung war nur zulässig, soweit sie für die Entscheidung über die Hilfegewährung erforderlich war (§ 67 a SGB X). Von Personen, die in einem Haushalt in eheähnlicher Gemeinschaft zusammenleben, vermutet das Bundessozialhilfegesetz (§§ 16,122), daß sie sich gegenseitig entsprechend ihrem Einkommen und Vermögen unterstützen. Steht fest, daß es sich so verhält, können vom Hilfesuchenden Angaben zum

Einkommen und Vermögen seines Partners verlangt werden. Sprechen Indizien für das Vorliegen einer eheähnlichen Wohnungsgemeinschaft, können auch Auskünfte zur Aufklärung des Sachverhalts verlangt werden. Insoweit ist der Hilfesuchende zur Mitwirkung verpflichtet (§ 60 SGB I).

Im vorliegenden Fall allerdings lag nur ein anonymer Hinweis auf einen männlichen Besucher vor. Die Hilfeempfängerin selbst hatte sich bereits dazu geäußert und bestritten, daß sie in einer eheähnlichen Gemeinschaft mit einem Mann zusammenlebe. Deshalb hatte das Amt keine Legitimation, die Hilfeempfängerin weiter auszufragen. Auf meine Intervention hin verzichtete das Amt auf die Beantwortung seiner Fragen.

12.3.6. Schutz des Beratungsgeheimnisses im Amt für Soziale Dienste

12.3.6.1. Neue Dienstanweisungen in Kraft

Im Mai 1994 hat das Amt für Soziale Dienste Dienstanweisungen zum Datenschutz in der Jugendhilfe und zur Hilfeplanung in Kraft gesetzt, die in Abstimmung mit mir entwickelt worden waren (vgl. Ziffer 8.6.3 meines 16. Jahresberichts).

Damit ist nach langjährigen Bemühungen endlich festgelegt worden, daß die Sachgebiete "Wirtschaftliche Jugendhilfe", die im Amt über die Kosten von Jugendhilfemaßnahmen entscheiden, als Entscheidungsgrundlagen nicht mehr die gesamten Fallakten, sondern nur noch die sog. Hilfepläne erhalten, die die Fachkräfte der Sozialdienste in Zusammenarbeit mit den Betroffenen (Jugendliche und Personensorgeberechtigte) erstellt haben. Daneben haben die Sachbearbeiter/innen der Wirtschaftlichen Jugendhilfe noch das Recht, an den in der Geschäftsordnung vorgesehenen Fallkonferenzen teilzunehmen, und erhalten folglich deren Protokolle. Alle übrigen der Vorbereitung des Hilfeplans dienenden Unterlagen verbleiben bei der fallführenden Fachkraft des jeweiligen Sozialdienstes. Zudem wurden, wie von mir empfohlen, zwecks gleichmäßiger Realisierung der Dienstanweisungen für die Hilfepläne und die Protokolle der Fallkonferenzen Vordrucke in Gebrauch gesetzt.

Dienstanweisungen und Vordrucke werden zur Zeit für die Dauer eines Jahres erprobt. Der Datenschutzausschutz der Bremischen Bürgerschaft, der sich mehrfach mit der Angelegenheit befaßt hat, hat mich beauftragt, die Erprobung datenschutzrechtlich zu begleiten und ihm Bericht zu erstatten.

12.3.6.2. Kontroverse um die "Entwicklungsberichte"

Gleichfalls im Mai 1994 aber wurde eine nicht mit mir abgestimmte Dienstanweisung in Kraft gesetzt, die im Falle der Unterbringung eines Jugendlichen in einer Einrichtung neben dem Hilfeplan außerdem den Entwicklungsbericht der Einrichtung als Grundlage für die Verlängerung der Maßnahme bezeichnete. Da dies im Zusammenhang mit der kostenrechtlichen Entscheidung geregelt wurde, rief dies im Amt selbst und bei mir den Eindruck hervor, daß in diesen Fällen entgegen den beiden anderen Dienstanweisungen zusätzlich zu den Hilfeplänen auch die Entwicklungsberichte der Wirtschaftlichen Jugendhilfe zugehen sollen.

Auf meine kritische Nachfrage hin wurde mir versichert, die Amtsleitung habe "deshalb klargestellt, daß sie mehrheitlich die Rechtsauffassung vertritt, daß die Weitergabe der Entwicklungsberichte an die Wirtschaftliche Jugendhilfe so nicht zulässig ist". Sie interpretiere die entsprechende Anweisung so, daß kostenrelevante Daten aus den Entwicklungsberichten in den fortgeschriebenen Hilfeplan einfließen müßten, der dann Grundlage der Entscheidung der Wirtschaftlichen Jugendhilfe sei.

Unklarheiten gab es auch um die Funktion eines Vordrucks der beim Träger der Einrichtung, in der ein Jugendlicher untergebracht ist, Daten abfragt, die für die weitere Fortgeltung der Kostenentscheidung erheblich sind; dazu gehören etwa Fragen nach dem tatsächlichen Aufenthalt des Jugendlichen, nach Anträgen bei anderen Sozialleistungsträgern oder nach Veränderung des Wohnorts der Eltern. Ich habe das Amt darauf hingewiesen, daß es nach § 62 Abs. 2 KJHG die Daten grundsätzlich beim Betroffenen erheben müsse. Die Erhebung beim Träger, also einer dritten Stelle, sei nur zulässig mit Einwilligung des

Betroffenen oder wenn im Einzelfall die Voraussetzungen vorliegen, die das Gesetz für eine Erhebung ohne Mitwirkung des Betroffenen aufgestellt habe.

12.3.6.3. Erstes Prüfergebnis

Schließlich habe ich Ende November 1994 im Amt für Soziale Dienste Ost eine erste Prüfung der bisherigen Handhabung der Dienstanweisungen vorgenommen. Dabei stellte ich fest, daß

- die geprüften Akten der Wirtschaftlichen Jugendhilfe aus der Zeit vor Inkrafttreten der Dienstanweisungen durchweg eine derartige Fülle von Unterlagen mit medizinischen, psychologischen und sozialarbeiterischen Daten der Jugendlichen und ihrer Familien enthalten, daß der Eindruck sich aufdrängt, es handele sich um komplette Parallelakten zu den Unterlagen der Sozialdienste, was schon an sich erhebliche Zweifel an der Erforderlichkeit der Datenverarbeitung erweckt,
- die Anweisung, der Wirtschaftlichen Jugendhilfe lediglich Hilfepläne und Kurzprotokolle der Fallkonferenzen zur Verfügung zu stellen, zu einer wesentlichen datenschutzrechtlichen Verbesserung führen kann,
- dies aber dadurch in Frage gestellt ist, daß auch jetzt noch in einem Teil der Akten der Wirtschaftlichen Jugendhilfe zusätzlich zu den Hilfeplänen eine Fülle weiterer Unterlagen aufgenommen werden, die überhaupt nicht hinein gehören.

Ich habe dies zum Anlaß genommen, auf eine Bereinigung der Akten ab Mai 1994 und darauf zu dringen, daß künftig nur noch die rechtlich zulässigen und durch Dienstanweisung vorgesehenen Unterlagen zu den Akten der Wirtschaftlichen Jugendhilfe genommen werden.

12.3.7. Wirtschaftlichkeits- und Qualitätsprüfung - auch mit Mitarbeiter- und Klientendaten ?

12.3.7.1. Neuregelung der Kontrollen bei Kostenübernahme

Im 16. Jahresbericht hatte ich unter Ziff. 8.7.1 darüber berichtet, daß in zunehmendem Umfang auch für Zwecke der Statistik, Planung und Aufsicht statt aggregierter Zahlen personenbezogene Daten, seien es Arbeitnehmerdaten, seien es Sozialdaten, verarbeitet werden. Diese Entwicklung setzt sich fort.

Zum 01.01.1994 ist mit der Neufassung des § 93 Abs. 2 eine Regelung in das Bundessozialhilfegesetz eingefügt worden, wonach als Voraussetzung für die Kostenübernahme Regelungen mit den Einrichtungen der freien Wohlfahrtspflege zu treffen sind, die den Trägern der Sozialhilfe eine Prüfung der Wirtschaftlichkeit und Qualität von deren Leistungen ermöglichen. Ich sehe insbesondere die Gefahr, daß hierfür auch sensible Daten der Klienten herangezogen werden. Ein Beispiel hierfür stelle ich in diesem Bericht unter Ziff. 13.3 dar.

Auf mein Schreiben, in dem ich den Senator für Gesundheit, Jugend und Soziales und den Magistrat der Stadt Bremerhaven darum bat, bei der Ausgestaltung dieser Regelungen die beruflichen Schweigepflichten der Mitarbeiter/innen von Beratungsstellen und anderen Hilfeprojekten zu beachten und im übrigen den Pesonenbezug erhobener Daten auf das erforderliche Maß zu begrenzen, habe ich bislang schriftliche Antworten nicht erhalten.

Zu der Problemdarstellung in meinem 16. Jahresbericht hat der Senat keine Stellung genommen. Die einzige Reaktion war bisher die Erklärung des Vertreters des Senators für Gesundheit, Jugend und Soziales in der Sitzung des Datenschutzausschusses am 04.11.1994, neben datenschutzrechtlichen Aspekten seien auch die Belange des Kostenträgers zu berücksichtigen. Dem kann nur - genauso allgemein - erwidert werden, daß umgekehrt aber neben den Belangen des Kostenträgers auch die datenschutzrechtlichen Aspekte zu berücksichtigen sind. Gerade um eine rechtlich einwandfreie Abwägung beider Gesichtspunkte ging es mir in meinem Beitrag und in meinem Schreiben an die Träger der Sozialhilfe.

12.3.7.2. Umstellung der Projektförderung in Bremen

Kurz vor Redaktionsschluß dieses Jahresberichts berichtete die Presse davon, daß der Senator für Gesundheit, Jugend und Soziales die Projektförderung von der Subventionierung von Stellen und Sachausgaben auf die Kostenerstattung für fest umrissene Leistungen umstellen. Auch hier muß darauf geachtet werden, daß durch die damit verbundene Erhebung von Daten zur Abrechnung und Kontrolle nicht berufliche Schweigepflichten von Beratern und Sozialarbeitern sowie Persönlichkeitsrechte von Klienten verletzt werden.

Ich werde erneut den Senator für Gesundheit, Jugend und Soziales darauf hinweisen, ihm meine Mitarbeit bei datenschutzgerechten Lösungen anbieten und dem Datenschutzausschuß über den Fortgang der Angelegenheit berichten.

13. Arbeit und Frauen

13.1. Krankenversicherung

13.1.1. Die Krankenversichertenkarte (KVK)

13.1.1.1. Einführung in Bremen

Seit dem 01.10.1994 müssen die gesetzlich Krankenversicherten auch im Lande Bremen beim Arztbesuch nicht mehr den Krankenschein, sondern die Krankenversichertenkarte vorlegen. Kurz nach deren Einführung bot ich in Bremen und Bremerhaven telefonische Sprechstunden an. Das Echo zeigte, daß nicht alle Versicherten den öffentlichen Erklärungen der Krankenkassen Glauben schenken, die Krankenversichertenkarte sei datenschutzrechtlich völlig unbedenklich. So wurde mehrfach gefragt, ob Gesundheitsdaten oder Arztbesuche gespeichert würden bzw. wie ich die künftige Entwicklung der Kartenfunktionen beurteile. Meinen Antworten konnte ich eigene Erkenntnissen zugrunde legen. Durch Gespräche, Prüfungen und Durchsicht zur Verfügung gestellter Unterlagen hatte ich mich zuvor davon überzeugt, daß Kassenärztliche Vereinigung Bremen und AOK Bremen/Bremerhaven das zur Einhaltung der gesetzlichen Vorgaben (vgl. hierzu im einzelnen Ziffer 8.3.1.1 meines 16. Jahresberichts) Gebotene veranlaßt hatten, etwa um den Einsatz von ausschließlich zertifizierter bzw. geprüfter Hard- und Software in den Arztpraxen und die Begrenzung der Speicherkapazität der Krankenversichertenkarten auf die zugelassenen Daten sicherzustellen. Die AOK sagte zudem zu, ihren Versicherten den Einblick in die auf ihrer Karte gespeicherten Daten problemlos zu gewähren.

13.1.1.2. Die Karte als Teil eines Kontrollmechanismus

Dennoch werde ich die Anwendung der Krankenversichertenkarte und ihre Auswirkungen auf die Verarbeitung von Versichertendaten aufmerksam begleiten. Zwar dient die Karte auf den ersten Blick, wie gesetzlich vorgegeben, lediglich der Vereinfachung der Abrechnung zwischen Arzt und Krankenkasse, zumal lediglich Identifikations- und Verwaltungsdaten und keine medizinischen Daten (etwa Arztbesuche, Diagnosen, ärztliche Leistungen, Verschreibungen, Blutdruck o. ä.) gespeichert werden dürfen. Ich hatte aber bereits frühzeitig - zuletzt im 16. Jahresbericht unter Ziffer 8.3.1 - davor gewarnt, daß mit der Einführung der Karte auch darüber hinausgehende Ziele verfolgt bzw. Entwicklungen verbunden seien.

Die Karte dient im Endeffekt auch zur Kontrolle von Ärzten und anderen Erbringern von Gesundheitsleistungen, nicht zuletzt aber auch der Versicherten selbst. Nachdem ich dies in der Landespressekonferenz, deren Gast ich im Juli 1994 war, vorgetragen hatte, löste die Berichterstattung bei den Krankenkassen ein gereiztes Echo aus. Die Senatorinnen für Arbeit und Frauen sowie für Gesundheit, Jugend und Soziales ziehen mich gar einer Falschmeldung, die die Bevölkerung verunsichere und jeder Grundlage entbehre.

Dabei wurde jedoch übersehen, daß die Krankenversichertenkarte nicht isoliert beurteilt werden darf, sondern daß das Gesundheitsreformgesetz von 1989 und das Gesundheitsstrukturgesetz von 1993 sie als einen zentralen Baustein in der zwingend vorgesehenen Automatisierung der Verarbeitung der Versichertendaten zum Zwecke von Abrech-

nung, Risikostrukturausgleich, Auffälligkeits- und Zufälligkeitsprüfungen vorsehen (vgl. hierzu §§ 267, 295 296, 297, 301, 303 SGB V).

Eine technische Voraussetzung hierfür ist es, daß die Ärzte, Krankenhäuser und anderen Leistungserbringer die Identifikations- und Verwaltungsdaten der einzelnen Versicherten von der Karte automatisiert auf ihre maschinenlesbaren Formulare drucken. Damit erhalten auch die Kassen die Versichertendaten EDV-gerecht. Sie werden instandgesetzt, die Daten, unter ihnen eben auch Gesundheitsdaten, anders als bislang zu verknüpfen und auszuwerten. Dazu dient auch, daß Ärzte und Krankenhäuser für die Diagnosen bzw. die Apotheken für die Arzneimittel einheitliche automatisationsgerechte Schlüssel benutzen sollen (ICD-Schlüssel bzw. Pharmazentralnummer).

Zudem ist die Krankenversichertenkarte ausdrücklich als Auslöser für die Automatisation der Datenverarbeitung in den Arztpraxen konzipiert. Dies aber birgt bisher vernachlässigte Datenschutzprobleme (unsichere Datenübermittlung, ungeschützte EDV, Zugriff Dritter auf Patientendaten per Fernwartung usw.) in sich.

13.1.1.3. Datenaustauschvertrag gefährdet Patientengeheimnis

Nun hat der Gesetzgeber des Gesundheitsstrukturgesetzes in das SGB V eine entscheidende Sicherung zum Schutz des Patientengeheimnisses eingezogen, deren einziger erkennbarer Zweck darin besteht, die Krankenversicherungen daran zu hindern, Gesundheitsdaten auf den einzelnen Patienten bezogen auszuwerten. Nach § 295 Abs. 2 SGB V sollen die Kassenärztlichen Vereinigungen den Kassen die Angaben über die Abrechnung ärztlicher Leistungen, darunter auch die Diagnosen, "fallbezogen, aber nicht versichertenbezogen" übermitteln (zur Entstehungsgeschichte vgl. 16. JB, Ziff. 8.3.1.3).

Ein zwischen Kassenärztlicher Bundesvereinigung und den Spitzenverbänden der gesetzlichen Krankenkassen und Ersatzkassen ausgehandelter und für die einzelnen Krankenversicherungen und Kassenärztlichen Vereinigungen verbindlicher Vertrag sieht nunmehr - anders als noch der Entwurf, über den ich in meinem 16. Jahresbericht berichtete - folgende Maßnahmen vor:

- Für einen Übergangszeitraum von einem Jahr sollen die Kassen in allen Fällen zusätzlich zu den automatisiert gespeicherten lediglich fallbezogenen Daten einen Papierausdruck mit den Identifikationsdaten des Versicherten erhalten. Begründung ist, dies sei erforderlich zur Sicherstellung der ordnungsgemäßen Abrechnung in der Übergangsphase bis zum reibungslosen Ablauf der Abrechnung mittels maschinell verwertbaren Datenträgern. Warum dies zusätzlich zum Rückgriff auf Papier als Datenträger auch den Zugriff auf den Versichertenbezug erfordert, bleibt unerfindlich. Inzwischen ist bekannt geworden, daß in einem Bundesland, in dem der Vertrag bereits zeitig praktiziert wurde, die Papierausdrucke über die vorgebrachte Begründung hinaus auch für die versichertenbezogene Überprüfung der Wirtschaftlichkeit ärztlicher Verordnungen genutzt werden.
- Auf Dauer sollen im Einzelfall die Kassenärztlichen Vereinigungen den Kassen auf deren begründetes Verlangen hin die Herstellung des Versichertenbezugs der Abrechnungsdaten ermöglichen, u.a. auch für die sachlich-rechnerische Prüfung in besonderen Einzelfällen und bei Verdacht von Fehlabrechnungen durch Ärzte oder Leistungserschleichung durch Versicherte.

Leider hat der Bundesbeauftragte für den Datenschutz den Vertrag in der abgeschlossenen Fassung im wesentlichen akzeptiert bzw. seine Bedenken gegen ihn zurückgestellt. Hierauf und auf die bundesweite Geltung des Vertrages beriefen sich die Kassenärztlichen Vereinigung Bremen und die Landesverbände der Krankenkassen in ihrer Stellungnahme zu meinem Schreiben, in dem ich kritisiert hatte, daß die genannten Bestimmungen des Vertrages gegen das Gesetz verstießen. Auf meine Fragen danach, nach welchen Verfahren die genannten Einzelfälle ausgewählt und die erhobenen Daten verarbeitet würden, wie die Einhaltung der im Vertrag genannten Zweckbestimmung sichergestellt werde und wann die Identifikationsmerkmale gelöscht werden sollten, habe ich bislang keine inhaltlichen Antworten erhalten.

Auf meinen Hinweis darauf, daß in Kürze ohnehin als Folge der Automatisierung der Datenverarbeitung in der gesetzlichen Krankenversicherung eine Fülle versichertenbezogener Daten in maschinenlesbarer Form zur Verfügung stünden, die es bei entsprechender Ausstattung ermöglichen, nach den unterschiedlichsten Kriterien **versicherten**bezogene Auswertungen vorzunehmen, erhielt ich von der AOK Bremen/Bremerhaven zur Antwort, derartiges prakiziere und plane man nicht. Mir wurde versichert, man habe lediglich Interesse daran, Qualität und Wirtschaftlichkeit der Arbeit der Leistungserbringer, vor allem der Ärzte, zu überprüfen. Welche datenschutzrechtlichen Probleme aber auch in derartigen Prüfungen stecken können, zeigt das AOK-Projekt "TARZAN" (vgl. u. Ziffer 13.1.2.).

13.1.1.4. Auf dem Weg zur Patientenchipkarte

13.1.1.4.1. Die öffentliche Diskussion geht weiter

Die Krankenversichertenkarte ist nicht als simple Magnetstreifenkarte, sondern trotz gesetzlich vorgegebener Begrenzung von Zweckbestimmung und Speicherkapazität als Chipkarte eingeführt worden. Der damit verbundene Einzug der elektronischen Informationstechnik in die Arztpraxen markiert den Beginn eines tiefgehenden Wandels der Verarbeitung medizinischer Daten überhaupt. Zwar dürfen auf der Krankenversichertenkarte nur solche Daten gespeichert werden, die der Identifikation des Versicherten und der Feststellung seines Versicherungsverhältnisses dienen. Der Einsatz der Chipkartentechnik aber macht angesichts ihres technischen Potentials erst Sinn, wenn auf ihr auch Gesundheitsdaten gespeichert werden. Dies zu realisieren ist die erklärte Absicht der Bundesverbände der Krankenkassen, der Kassenärztlichen Bundesvereinigung, von Medizininformatikern und EDV-Industrie.

Die Datenschutzbeauftragten von Bund und Ländern benannten im März 1994 in ihrem Beschluß zu "Chipkarten im Gesundheitheitswesen" (vgl. u. Ziff. 22.1.) zum Schutz der Persönlichkeitsrechte der Patienten eine Reihe von Rahmenbedingungen für den Einsatz von Patientenchipkarten: Schriftliche Einwilligung, Trennung von der Krankenversichertenkarte, Beschränkung der Daten für einzelne Nutzungen je nach Erforderlichkeit, Entscheidungsrecht des Betroffenen über die Speicherung von Daten und den Zugang zu ihnen sowie ihre Änderung und Löschung, schließlich Einsichtsrechte und -möglichkeiten für die Betroffenen. Der Gesetzgeber solle dies durch bereichsspezfische Rechtsgrundlagen sicherstellen.

Währenddessen sind Industrie, Forschung, Kassenärztliche Vereinigung und Krankenkassen intensiv bemüht, die Entwicklung und den Einsatz von Patientenchipkarten voranzutreiben. Veranstaltungen mit wohlklingenden Namen wie Multicard, Smartcard-Forum oder "Forum vertrauenswürdige Informationstechnik für Medizin und Gesundheitsverwaltung" sowie Modellprojekte wie BKK-Gesundheitscard, Vital-Card des AOK-Bundesverbandes, Sanacard der Kassenärztlichen Vereinigung Koblenz und A-Card der Bundesvereinigung Deutscher Apothekerverbände legen hiervon Zeugnis ab.

Den genannten und anderen Veranstaltungen ist gemeinsam, daß nicht mehr das Ob, sondern nurmehr das Wie der Einführung von Patientenchipkarten erörtert wird. Man zerbricht sich die Köpfe über Anwendungsbereiche, Datenumfang, Verschlüsselung, Zugriffsbefugnisse und entwickelt immer konkretere und technisch ausgefeiltere Lösungen hierfür. Dabei werden durchaus auch Datensicherheits- und Datenschutzanforderungen, die ärztliche Schweigepflicht und die Persönlichkeitsrechte der Patienten einbezogen. Hierauf Einfluß zu nehmen, ist sicher eine wichtige Aufgabe von Datenschutzbeauftragten. Darüber hinaus aber ist es zum jetzigen Zeitpunkt vordringlich, die allzuschnell gegebene Antwort auf die Frage nach dem Warum öffentlich zu erörtern, um die Option offen zu halten, nicht alle technischen Möglichkeiten, die die Chipkarten zur Verarbeitung von Gesundheitsdaten bieten, zu nutzen.

13.1.1.4.2. Modellversuche

Die Verlautbarungen seiner Befürworter dagegen zielen eindeutig auf eine möglichst umfassende Realisierung des Projekts Patientenchipkarte hin. Immerhin erklären sie zu-

gleich, die Vorgaben der Datenschutzbeauftragten von Bund und Ländern beachten zu wollen. Anders sieht dies aber schon bei den laufenden bzw. propagierten Modellprojekten aus.

So stellt beispielsweise eine Kasse ihren Mitgliedern Bonuspunkte in Aussicht, wenn sie auf sog. Aktionstagen der Kasse Werte wie Blutzucker, Sauerstoffdynamik, Cholesterol und weitere spezielle medizinische Daten ohne ärztliche Konsultation messen und auf der Patientenchipkarte speichern und aktualisieren lassen (Projekt "BKK-Gesundheits-Card"). Derartige von der Nutzung der Karte abhängigen materiellen Vorteile widersprechen dem Prinzip der Freiwilligkeit. Der Effekt wird noch verstärkt, indem die Kasse die Möglichkeit einer Beitragsrückerstattung in Aussicht stellt.

Der AOK-Bundesverband propagiert sein Projekt "Vital-Card" mit einer noch umfassenderen Zielsetzung, was gespeicherte Daten und Anwendungsfelder angeht. Vor allem aber scheint die Verfügungsgewalt des Patienten über die einzelnen Datenspeicher nur sehr begrenzt und unvollkommen realisiert zu sein.

Bislang sind keine Planungen für einen Einsatz der Patientenchipkarte durch Krankenkassen im Lande Bremen bekannt geworden. Dem stünde derzeit auch die politische Erklärung aus dem Hause des Senators für Arbeit und Frauen, d. h. der Rechtsaufsichtsbehörde über die Krankenkassen im Lande Bremen, in der Sitzung des Datenschutzausschusses der Bremischen Bürgerschaft am 04.11.94 entgegen, daß die Einführung der Chipkarte als Krankenversichertenkarte begrüßt werde, daß jedoch Forderungen nach einer darüber hinausgehenden Anwendung, d.h. als Patientenchipkarte, abgelehnt würden.

13.1.2. Das Projekt TARZAN der AOK

13.1.2.1..Totalerfassung von Rezeptdaten

Die sich zwangsläufig aufdrängende Vorstellung vom mächtigen Dschungelhelden Tarzan hat auf den ersten Blick natürlich nichts mit dem Projekt der AOK Bremen/Bremerhaven zu tun.

Bleibt man jedoch im Bild, so stellt sich schnell die Assoziation einer sich im Daten dschungel der Versicherten von Information zu Information schwingenden Institution ein, die zwar nicht wie Tarzan für die gewünschten Verbindungen zu Lianen greift, sich dafür aber ungleich effektiver geeigneter Datenverarbeitungsprogramme bedient.

TARZAN steht für Transparenzsystem, Arzneimittel und Arzneikosten, Auswertungen und verfolgt als Ziel die versichertenbezogene Anspruchs- und Statusprüfung sowie Arzneimittel- und Arzneikostenauswertungen.

Im Rahmen dieses Projektes hat die AOK Bremen/-Bremerhaven im April 1993 eine Datenverarbeitungsfirma damit beauftragt, Daten von Rezepten für Versicherte der AOK automatisiert versicherten- und verschreibungsbezogen zu erfassen sowie Zuordnungs- und Abrechnungsprüfungen vorzunehmen.

Die Auftragnehmerin erstellt aus den von der AOK angelieferten Rezepten quartalsbezogene Datenträger (Magnetbänder) für die AOK. Neben der Datenerfassung werden Rezepte, denen keine Krankenversichertennummern zugeordnet werden können, sowie Rezepte mit Artikeln ohne zuordnungsfähige Artikelnummer aussortiert und der AOK zur Verfügung gestellt. Darüberhinaus werden Taxprüfungen vorgenommen, d.h. es werden sowohl die Korrektheit der auf den Rezepten angegebenen Medikamentenpreise als auch der Bruttoendbetrag überprüft. Bei nicht korrekter Endsumme werden die entsprechenden Rezeptdaten der AOK in einem gesonderten Bestand zur Verfügung gestellt.

Die manuell erfaßten Daten werden per Datenfernübertragung zur weiteren Verarbeitung in den Großrechner einer Bremerhavener Firma übertragen, deren Rechenzentrum inzwischen von der Auftragnehmerin erworben worden ist. Dort wird eine versichertenbezogene Zuordnung der Rezeptdaten mit Hilfe einer von der AOK zur Verfügung gestellten Korrespondenzdatei vorgenommen. Darüberhinaus wird die Korrektheit der Abrechnung des NARZ (Norddeutsches Apothekerrechenzentrum) überprüft, indem der vom NARZ

zu Abrechnungszwecken auf die einzelnen Rezepte aufgetragene Codierstreifen mit den manuell erfaßten Daten abgeglichen wird.

Die Magnetbänder mit den elektronisch erfaßten Rezepten der einzelnen Versicherten werden nach Abschluß der Bearbeitung der AOK übergeben.

13.1.2.2. Ergebnis der datenschutzrechtlichen Prüfung

Da trotz der datenschutzrechtlich offenen Fragen und damit einer fehlenden endgültigen Bewertung die Totalerfassung der Rezeptdaten fortgesetzt wurde, fand eine Überprüfung im November 1994 statt, in der das im Rahmen des Projektes TARZAN angewandte DV-Verfahren im Haus der AOK anhand der Programmdokumentation dargestellt wurde.

Demnach dient die versichertenbezogene Erfassung der Rezeptdaten drei Zwecken:

- Taxprüfung (apothekenbezogene Prüfung auf rechnerische Richtigkeit sowie Kontrolle der Rechnungslegung durch das Apotheker-Rechenzentrum)
- Anspruchsprüfung (Überprüfung der Mitgliedschaft der Leistungsempfänger/-innen)
- IAI (individuelle Arzneimittelinformation/ statistische Auswertungen für die pharmazeutische Beratungs- und Prüfstelle.

Bei der AOK werden erneut Tax-Prüfungen und die "eigentliche" Anspruchsprüfung (Abgleich der Rezeptdaten mit aktuellem Versichertenbestand) vorgenommen.

Die statistischen Auswertungen für die pharmazeutische Beratungs- und Prüfstelle (IAI) der Krankenkasse bekommen durch die automatisiert vorliegende Datenbasis allerdings eine völlig neue Qualität:

Das **IAI-Verfahren** wurde schon vor der Verfügbarkeit der SDV-Datenbasis durchgeführt, jedoch erfolgte die Auswahl der Ärzte für die Arbeit der Beratungs- und Prüfstelle (PbP) manuell. Die durch die elektronisch verfügbare Datenbasis gegebene Möglichkeit der umfassenden Recherche auf alle Arztnummern ist mit wenigen Änderungen, die im Rechenzentrum der AOK selbst durchgeführt werden können, auch auf Versichertendaten anwendbar. Von seiten der AOK wurde versichert, daß eine automatisierte Recherche nur arztbezogen , nicht versichertenbezogen durchgeführt werde. Mit der Auswahl eines Arztes (dargestellt über die Arztnummer) ist es jedoch ebenfalls möglich, versichertenbezogen die Medikamentation eines Patienten pro Quartal auszuwerten. Auf den mir exemplarisch für eine Arztnummer übergebenen IAI-Ausdrucken sind die Versicherten mit dem ersten Buchstaben des Nachnamens in Kombination mit dem Geburtsdatum, dem Besuchstermin und der Medikamentation genannt. Somit ist ein eindeutiger Versichertenbezug herstellbar.

13.1.2.3. Beanstandung wegen Datenschutzverstoß

Es handelt sich bei dem Projekt TARZAN um eine lückenlose Erhebung von versichertenbezogenen Veschreibungsdaten, für die es keine ausreichende Rechtsgrundlage gibt.

Die Speicherung von Versichertendaten zum Zwecke der Tax- und Anspruchsprüfung ist zwar nach § 284 Abs. 1 Ziffer 1, 8 SGB V dem Grunde nach, aber nicht dem Umfang nach gerechtfertigt. Nach erfolgter Prüfung durch den Auftragnehmer benötigt die AOK den Versichertenbezug nur noch für die Fälle, in denen die Mitgliedschaft eines Versicherten in Frage steht (Anspruchsprüfung). Aber auch insoweit sind die Identifikationsmerkmale nach Abschluß dieser Prüfung zu löschen.

Für die versichertenbezogene Speicherung aller Rezeptdaten zum Zwecke der individuellen Arzneimittelinformation fehlt es an einer Rechtsgrundlage. Nach § 284 Abs. 1 Nr. 9, § 106 Abs. 2 Nr. 2 SGB V ist eine Prüfung der Wirtschaftlichkeit der vertragsärztlichen Versorgung anhand versichertenbezogener Daten nur auf der Grundlage von Stichproben zulässig, die 2% der Ärzte je Quartal umfassen dürfen. Überdies sind die vom Gesetzgeber für das Verfahren vorgesehenen Vereinbarungen der Spitzenverbände noch gar nicht abgeschlossen.

Auch die weiteren von der AOK im nachhinein genannten möglichen künftigen Nutzungszwecke (Forschung, Herstellung "versichertenbezogener Transparenz") rechtfertigen nicht die Speicherung in dem vorgesehenen Umfang bzw. entbehren überhaupt der Rechtsgrundlage.

Ich habe die über das gesetzlich zugelassene Ausmaß hinausgehende Datenverarbeitung versichertenbezogener Rezeptdaten beanstandet und die AOK zugleich aufgefordert, die Daten, deren Speicherung unzulässig ist, zu löschen. Für die Zukunft habe ich die AOK aufgefordert, die unzulässige Speicherung von Daten einzustellen.

13.1.3. Methadon-Substitution — Wegfall der umfassenden Doppelregistrierung

In den letzten Jahrensberichten (zuletzt im 16. JB, Ziff. 8.3.2) berichtete ich über meine langwierigen Bemühungen, die Erhebungen, Speicherung und Nutzung der Daten von Heroin-Abhängigen, die mit Methadon substituiert werden, auf ein datenschutzrechtlich erträgliches Maß einzugrenzen. Die Kassenärztliche Vereinigung Bremen und die AOK Bremen/Bremerhaven beriefen sich demgegenüber auf die bundesweit geltenden für sie verbindlichen sog. NUB-Richtlinien der Kassenärztlichen Bundesvereinigung und der Spitzenverbände der Krankenkassen.

Diese Spitzenorganisationen haben inzwischen die Richtlinien dahingehend geändert, daß die kostentragenden **Krankenkassen** bei den substituierenden Ärzten nurmehr die Daten erheben sollen, die sie benötigen, um die Mitgliedschaft des Substitutionspatienten überprüfen zu können und um zu verhindern, daß einzelne Heroin-Abhängige sich von mehreren Ärzten Methadon verschreiben lassen.

Dagegen erhalten die **Kassenärztlichen Vereinigungen** die Daten, die sie zur Prüfung benötigen, ob - wie vorgeschrieben - Substitution psychologisch und sozialarbeiterisch begleitet wird und ob die einzelnen Ärzte die zugelassene Höchstzahl von Methadon-Patienten einhalten. Hinzu kommen die Angaben, die sie für die für eine Reihe von Fällen vorgesehenen Beratungen in einer Kommission benötigen. Personenbezogene Daten sollen vor deren Verhandlungen anonymisiert werden.

AOK und Kassenärztliche Vereinigung Bremen haben mir daraufhin zugesichert,

- daß die eingehenden Meldungen der Ärzte direkt an die zuständige Sachbearbeiterin bzw. an die Geschäftsstelle der Beratungskommission gehen,
- daß sie die Daten nur für die vorgesehenen Zwecke nutzen,
- daß nach Beendigung der Substitution bzw. nach erfolgter Abrechnungsprüfung die Daten unverzüglich gelöscht werden.

Damit habe ich meine ursprüngliche Rechtsposition (vgl. 15. JB, Ziff. 10.3.1) nicht in vollem Umfang durchsetzen können. Es ist aber schließlich doch erreicht worden, daß an sich selbstverständliche Regeln der Datenverarbeitung - Erforderlichkeit, Zweckbindung, Zugriffsbeschränkungen, Löschungsregelung - auch und gerade in diesem sensiblen Bereich Beachtung finden.

13.2. Bekämpfung illegaler Beschäftigung: Richtlinien für den Informationsaustausch

Am 1o. Januar 1995 ist in Bremen eine Verwaltungsvorschrift zur Bekämpfung illegaler Beschäftigung in Kraft getreten (BremABl. S.1). Der Senator für Arbeit und Frauen hatte mir rechtzeitig den Entwurf zur datenschutzrechtlichen Prüfung vorgelegt.

Ich hatte ihn darauf hingewiesen, daß eine Verwaltungsvorschrift nicht Befugnisse zur Verarbeitung personenbezogener Daten von Arbeitgebern oder Beschäftigten begründen, sondern nur gesetzliche Befugnisse wiedergeben und konkretisieren könne. Diese Befugnisse sind im Laufe der vergangenen Jahre immer weiter ausgebaut worden. Sie sind vor allem im Arbeitsförderungsgesetz, im Arbeitnehmerüberlassungsgesetz, im SGB IV, im Gesetz zur Bekämpfung der Schwarzarbeit und, soweit es um die Vergabe öffentlicher Aufträge geht, im Haushaltsgrundsätzegesetz und der auf dessen Grundlage erlassenen

Vergabeverordnung normiert. Diese Rechtsvorschriften regeln die Datenerhebung, die erlaubten Zwecke der Nutzung und den Datenaustausch der mit der Bekämpfung illegaler Beschäftigung beauftragten Behörden untereinander. Auf Landesebene sind die Gewerbeaufsichtsämter, die Gewerbepolizei und die Ausländerbehörden einbezogen.

Der Senator für Arbeit und Frauen hat auf meine Vorschläge hin seinen Entwurf in einigen Punkten geändert:

- Die Vergabestellen, d. h. die bremischen Behörden, die Bauträge vergeben, sollen von Bewerbern außer einer Erklärung zur Beschäftigung sozialversicherter bzw. ausländischer Arbeitnehmer, von geringfügig Beschäftigten und zum Einsatz von Subunternehmern nur in bestimmten Fällen einen Auszug aus dem Bundeszentralregister (polizeiliches Führungszeugnis), nicht aber mehr - wie ursprünglich vorgesehen - aus dem Gewerbezentralregister vorlegen. Diese Einschränkung trägt dem Umstand Rechnung, daß es zwar gesetzlich vorgesehen ist, ein Führungszeugnis zur Vorlage bei einer anderen Behörde auszustellen (§ 30 Bundeszentralregistergesetz), dies aber nicht für Auskünfte aus dem Gewerbezentralregister gilt (vgl. §§ 150, 150a der Gewerbeordnung).
- Die Vergabestellen sollen der in die Abteilung Arbeitsmarktpolitik des Senators für Arbeit und Frauen angegliederten "Koordinierungsstelle zur Bekämpfung der illegalen Beschäftigung" lediglich anonymisierte Angaben über Feststellungen machen, die auf illegale Beschätigung hindeuten.

Ich hatte auch Gelegenheit, im Einvernehmen mit dem Senator für Arbeit und Frauen dem Gewerbeaufsichtsamt Bremen gegenüber klarzustellen, daß Meldungen über Beschäftigte, die ohne Sozialversicherungsausweis auf einer Baustelle angetroffen werden (Verstoß gegen § 99 Abs. 2 SGB IV), nicht an die genannte Koordinierungsstelle, sondern an die Bundesanstalt für Arbeit zu richten sind. Nach § 107 Abs. 1 Satz 1 SGB IV überprüft diese die Einhaltung der Vorschriften über den Sozialversicherungsausweis, das Gewerbeaufsichtsamt hat sie dabei zu unterstützen und ist zur Übermittlung der hierfür erforderlichen Daten befugt (§ 107 Abs. 1 Sätze 4 und 7 SGB IV).

13.3. Teilnehmerkontrollen bei Zuschüssen aus dem Europäischen Sozialfonds

13.3.1. Gefährdung zugesicherter Vertraulichkeit

Die Koordinierungs- und Beratungsstelle für Frauen "Zurück in den Beruf" im Arbeitsförderungszentrum des Landes Bremen GmbH war von einer nicht-öffentlichen Stelle, die der Bundesminister für Arbeit und Sozialordnung im Auftrag der EG-Kommission zwecks Vorprüfung der ordnungsgemäßen Verwendung eines Zuschusses aus Mitteln des Europäischen Sozialfonds für ein Projekt der Beratung ausländischer Frauen eingeschaltet hatte, aufgefordert worden, Listen mit Namen, Anschriften und Telefonnummern der beratenen Frauen einzureichen - und dies längst nach Abschluß der Beratungsgespräche.

Die Beratungsstelle hatte dies vor allem mit der Begründung abgelehnt, daß sie mit der Preisgabe der Daten das Vertrauen der Frauen in die Vertraulichkeit der Beratung, die ihnen in Unkenntnis der späteren Anforderung zugesichert worden sei, enttäuschen würde. Gerade für ausländische Frauen sei der Entschluß, sich beraten zu lassen, oftmals der erste selbständige Schritt, von dem auch nicht immer die Ehemänner wüßten. Es könne nicht vertretbare Folgen haben, würden diese etwa durch eine Nachprüfung seitens der Vorprüfungsstelle davon in Kenntnis gesetzt. Wären die Frauen - vorausgesetzt das Ansinnen sei damals schon bekannt gewesen - vor Beratung von der Weitergabe ihrer Daten in Kenntnis gesetzt worden, hätte dies von vornherein einen Erfolg des Beratungsprojekts gefährdet.

Ich habe die Beratungsstelle in ihrer Ablehnung bestärkt. Mit einer Übermittlung der Daten der beratenden Frauen verletze sie das Zweckbindungsgebot, ihre Mitarbeiter/innen liefen Gefahr, ihre beruflichen Schweigepflichten zu verletzen. Die Übermittlung sei weder durch eine Einwilligung noch durch eine gesetzliche Befugnis legitimiert. Auch die dem Zuwendungsbescheid des Bundesministeriums beigefügten Förderrichtlinien sähen nicht die Vorlage teilnehmerbezogener Listen vor, sondern lediglich einen Sachbericht,

einen zahlenmäßigen Verwendungsnachweis sowie die Berechtigung der Bewilligungsbehörde bzw. der Vorprüfungsstelle, von Fall zu Fall Bücher, Belege und Geschäftsunterlagen anzufordern oder durch örtliche Erhebungen zu prüfen. Nachdem die Beratungsstelle meine Stellungnahme der Vorprüfungsstelle vorgelegt hatte, verzichtete diese auf die Übermittlung der Listen.

13.3.2. Bundesweite Konsequenzen ?

Der Bundesbeauftragte für den Datenschutz hat die Angelegenheit auf meine Bitte hin dem Bundesministerium für Arbeit und Sozialordnung vorgetragen. Dieses wollte zunächst daran festhalten, daß derartige Namenslisten grundsätzlich zu Prüfzwecken erforderlich seien, und sich nur in ganz bestimmten engbegrenzten Fällen - als Beispiele wurden Suchtmittelabhängigkeit, Vorstrafen, Verschuldung und HIV-Infizierung genannt - mit anonymisierten Teilnehmerlisten begnügen. Nachdem der Bundesbeauftragte für den Datenschutz darauf bestand, daß bei Beratungsprojekten generell anonymisierte Listen, die anhand von Schlüsselnummern für konkrete Prüfzwecke deanonymisiert werden, ausreichen müßten, und auf die besondere Schutzbedürftigkeit beratener ausländischer Frauen hinwies, stellte das Ministerium wenigstens in Aussicht, seine Bedenken bei der Gestaltung zukünftiger Förderverfahren zu berücksichtigen. Das Beispiel zeigt, wie schwer es ist, bürokratischen Instanzen abzuringen, an sich selbstverständliche Zugeständnisse an die Belange des Persönlichkeitsschutzes zu machen.

Ähnliche Probleme ergeben sich bei der Kontrolle von freien Trägern der Wohlfahrtspflege und von Projekten durch den Senator für Gesundheit, Jugend und Soziales (vgl. 16. JB, Ziff. 8.7.1. und Ziff. 12.3.7 in diesem Bericht).

14. Umweltschutz und Stadtentwicklung

14.1. Das Umweltinformationsgesetz - Umsetzung in Bremen

Bereits in meinem 15. Jahresbericht (Ziff. 11.1) hatte ich darauf hingewiesen, daß die Umsetzung der EG-Richtlinie vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt in deutsches Recht nach dem damals vorliegenden Entwurf eines Umweltinformationsgesetzes der Bundesregierung viel zu restriktiv vorgenommen werden sollte. Im übrigen hatte ich angeregt, daß der Senat prüfen solle, welche gesetzlichen Vorschriften im Bereich der Landeskompetenz zu erlassen wären, wie dies in Einzelbereichen, z.B. für die Einsicht in das Wasserbuch nach dem Bremischen Wassergesetz, bereits geschehen ist.

Der Senator für Umweltschutz und Stadtentwicklung hatte mir mitgeteilt, nach dem Inkrafttreten des Umweltinformationsgesetzes des Bundes werde angestrebt, mit anderen Bundesländern eine Handlungsanleitung abzustimmen, um den ohnehin engen Spielraum des neuen Gesetzes hinsichtlich des Informationszugangs voll auszuschöpfen. Dies halte ich für tunlich, weil der vor Inkrafttreten des Gesetzes herausgegebene Erlaß des Senators für Umweltschutz und Stadtentwicklung sich noch unmittelbar auf die EG-Richtlinie bezog und lediglich vergleichsweise allgemeine Hinweise z.B. auf die notwendige Einhaltung der Datenschutzbestimmungen enthielt.

Im Juli 1994 ist das neue Bundesgesetz in Kraft getreten (BGBl. I, S. 1940). Nach Auskunft des Senators für Umweltschutz und Stadtentwicklung sind seitdem mehrere Anfragen eingegangen und positiv beschieden worden. Das öffentliche Interesse an diesem Thema erscheint noch gering. Immerhin fand im Januar 1995 eine öffentliche Veranstaltung der Bremer Umweltberatung statt, in der ein Rechtsanwalt seine praktischen Erfahrungen bei der Anwendung dieses Gesetzes dargelegt hat.

Kernpunkt der Kritik am neuen Bundesgesetz bleiben die zahlreichen Ausnahmeregelungen, mit denen das Akteneinsichtsrecht eingeschränkt oder ausgeschlossen werden kann. Selbst die EU-Kommission hat inzwischen Bedenken, ob das deutsche Gesetz den Anforderungen der Richtlinie entspricht. Bereits Mitte September 1994 wollte die Kommission darüber beraten, ob sie gegen die Bundesrepubkik ein Verfahren wegen Vertragsverletzung einleitet. In einem solchen Verfahren wird geprüft, ob und in welchen Punkten das

deutsche Gesetz gegen die Brüsseler Richtlinie verstößt. Ob und ggf. wann die EU-Kommission den Europäischen Gerichtshof anrufen wird, ist noch offen.

14.2. Datenaustausch im Umweltbereich - Bund/Länder-Vereinbarung

Der Bund und die Länder haben am 24.11.1994 eine Verwaltungsvereinbarung über den Datenaustausch im Umweltbereich abgeschlossen. Die in § 5 enthaltene Datenschutzklausel enthält lediglich die allgemeine Feststellung, daß die Bestimmungen des Datenschutzes von Bund und Ländern und die sonstigen Vorschriften zur Geheimhaltung beachtet werden.

In diesem Zusammenhang habe ich darauf hingewiesen, daß die Übermittlung personenbezogener Umweltdaten nur zulässig ist, soweit dies von einer Rechtsvorschrift, d.h. von den Datenschutzgesetzen des Bundes und der Länder oder speziellen Offenbarungsbestimmungen in Umweltgesetzen oder -verordnungen, erlaubt wird. Die Zulässigkeit der Weitergabe personenbezogener Einzelangaben kann allein auf die Verwaltungsvereinbarung nicht gestützt werden.

Bisher soll lediglich der Datenkatalog von Gewässergütedaten, die ausgetauscht werden sollen, abgestimmt werden. Dieser Katalog enthält noch keine personenbezogenen Daten. Allerdings rechne ich mit der Möglichkeit, daß in Zukunft auch personenbezogene Daten in den Austausch einbezogen werden sollen.

Ich habe daher den Senator für Umweltschutz und Stadtentwicklung gebeten, sicherzustellen, daß ich bei Ergänzung oder Änderung des Datenkatalogs in der Anlage zur Verwaltungsvereinbarung informiert werde. Dieser hält es für die Zukunft zwar für ausgeschlossen, daß personenbezogene Daten verarbeitet werden, und hat im übrigen auf den Informationszugang für die Öffentlichkeit hingewiesen. Gleichwohl hat er mir versichert, er werde mich ggf. beteiligen.

14.3. Altlastenkataster noch immer ohne gesetzliche Grundlage

In den vergangenen Jahren habe ich wiederholt (vgl. 12. JB für 1990 Ziff. 2.8; 13. JB für 1991, Ziff. 2.7) auf das Fehlen datenschutzrechtlicher Regelungen für die Erhebung und Speicherung von Altlastendaten hingewiesen. Außerdem habe ich darauf gedrängt, im Abfallrecht normenklar und abschließend zu regeln, unter welchen Voraussetzungen sowohl öffentliche Stellen als auch Privatpersonen Auskünfte aus dem Altlastenkataster erhalten dürfen. Diese Auskünfte können sensible, insbesondere für den wirtschaftlichen Wert von Grundstücken entscheidende Informationen enthalten. Wichtig ist daher vor allem, wie gesichert die Angaben in dieser Datensammlung sind und wer darauf Zugriff hat.

Das Altlastenkataster ist in den Jahren 1989/90 aufgrund der Erhebungen eines vom Senator für Umweltschutz und Stadtentwicklung beauftragten Ingenieurbüros in der senatorischen Behörde aufgebaut worden und wird durch weitere Erhebungen, Meßergebnisse und ähnliches fortgeschrieben. Aus dem Kataster werden insbesondere Auskünfte im Rahmen von Baugenehmigungsverfahren erteilt. Altlastendaten an Privatpersonen werden nach Angabe der senatorischen Behörde grundsätzlich nicht personenbezogen weitergegeben. Die Weitergabe insbesondere im Baugenehmigungsverfahren beruht derzeit auf keiner Rechtsgrundlage.

Der Senat hat in seiner Stellungnahme zu meinem 13. Jahresbericht (Drs. 12/1281 vom 02.07.1991, S. 11) mitgeteilt, die Behörde beabsichtige, in der 13. Legislaturperiode im Rahmen der Novellierung des Bremischen Ausführungsgesetzes zum Gesetz über die Vermeidung und Entsorgung von Abfällen auch eine landesrechtliche Regelung der Altlastenproblematik zu schaffen. Diese Regelung werde auch die in meinem Jahresbericht genannten Aspekte des Datenschutzes erfassen, insbesondere die Frage der Auskunftserteilung aus einem Altlastenkataster.

Auf erneutes Nachfragen hat die senatorische Behörde im Januar 1994 erklärt, die beabsichtigte Änderung des Landesausführungsgesetzes zum Abfallgesetz sei wegen der in Aussicht stehenden bundesrechtlichen Neuregelung des Abfallgesetzes und des Erlasses

eines Bundesbodenschutzgesetzes bislang zurückgestellt worden, um das Gesetz nicht zweimal in kurzen Abständen ändern zu müssen. Der Entwurf des Bundesbodenschutzgesetzes sehe gerade auch Regelungen über den Umgang mit Altlasten vor.

In der im Dezember 1994 abgelaufenen Wahlperiode des Bundestages ist jedoch das Bodenschutzgesetz des Bundes nicht zustande gekommen. Auch ist das weitere Schicksal dieses Gesetzgebungsvorhabens unklar. Daher sollten die Vorbereitungen für eine landesrechtliche Grundlage für das Altlastenkataster umgehend und nachdrücklich vorangetrieben werden.

14.4. Codierte Mülltonne

14.4.1. Fragen nach der körperlichen Verfassung

Bei der Einführung der codierten Mülltonne in Bremen gab es Proteste von Bürgern, die sich z.B. aufgrund ihres Gesundheitszustands außerstande sahen, die neuen Eimer zu heben bzw. zu transportieren. Die Bremer Entsorgungsbetriebe (BEB) stellen daher auf Antrag einen kostenlosen Bereitstellservice zur Verfügung.

Das Antragsformular enthielt insbesondere den Hinweis, daß für den Fall, daß Betroffene erklärten, aufgrund ihrer körperlichen Verfassung nicht in der Lage zu sein, das Abfallgefäß selbst zur Abholung bereitzustellen, ein geeigneter Nachweis bzw. ein Attest "die Antragsbearbeitung erleichtere".

Aufgrund dieser Formulierung haben sich Bürgerinnen und Bürger an mich gewandt und moniert, daß sie sich dazu gezwungen fühlten, ärztliche Atteste für diesen Zweck vorzulegen. Ich habe daraufhin die BEB gebeten, die Verwendung des Fragebogens sofort einzustellen und diesen datenschutzgerecht umzugestalten.

Die BEB reagierte verständnisvoll und änderte den Vordruck. Nach dem neuen Antrag ist klargestellt, daß der Betroffene keine äztlichen Nachweise einzureichen braucht, sondern lediglich selbst eine kurze Erklärung und Begründung abgibt.

14.4.2. Haushaltsbezug und Fremdabrechnung der Müllgebühren

Im Zusammenhang mit der codierten Mülltonne hat mich der Senator für Umweltschutz und Stadtentwicklung gebeten, zur Vorbereitung einer Mitteilung des Senats zu einer Großen Anfrage der Koalitionsfraktionen zur Abrechnung der Müllgebühren Stellung zu zwei Fragen zu nehmen.

Zum einen ging es um die Frage, welche Gesetze bzw. Verordnungen etc. bei der Umstellung des bisherigen grundstückseigentümerbezogenen Gebühreneinzuges auf einen haushaltsbezogenen Gebühreneinzug geändert werden müßten.

Hierzu habe ich dargelegt, daß dann § 7 des Ortsgesetzes über die Entsorgung von Abfällen in der Stadtgemeinde Bremen dahingehend zu ergänzen bzw. zu ändern ist, daß die Anschlußpflicht unmittelbar den Wohnungsinhabern obliegt. Nur dann besteht für diesen Personenkreis eine eindeutige Rechtsgrundlage für die Verarbeitung ihrer Daten.

Zum anderen ging es um die Frage, ob es datenschutzrechtliche Bedenken bei einer Verarbeitung der Gebührendaten durch Dritte, d.h. außerhalb der BEB, gibt und wie diese ggf. ausgeräumt werden können.

Ich habe auf die Rechtslage hingewiesen, wonach in diesem Fall eine Auftragsdatenverarbeitung nach § 8 Abs. 1 Bremisches Datenschutzgesetz (BrDSG) vorliegt. Datenschutzrechtliche Bedenken bestehen nicht, wenn der Auftragnehmer, der die Gebührenabrechnung vertraglich übernimmt, sorgfältig ausgewählt wird, die erforderlichen technischen und organisatorischen Datensicherungsvorkehrungen getroffenen hat und der Kontrolle des Landesbeauftragten für den Datenschutz unterliegt. Die DV-technische Abwicklung der Gebührenabrechnung ebenso wie die Sicherungsmaßnahmen beim Auftragnehmer wären von den Bremer Entsorgungsbetrieben vertraglich präzise zu regeln.

Die Mitteilung des Senats ist mit der Bürgerschaftsdrucksache 13/681 vom 10. Januar 1995 erfolgt.

15. Bauwesen

15.1. Überprüfung der Einkommensverhältnisse nach dem Wohnungsbauförderungsgesetz

Das am 01.10.1994 in Kraft getretene Wohnungsbauförderungsgesetz (WoBFördG; BGBl I, S. 1184) hat die Regelungen zur Einkommensüberprüfung der Wohnungssuchenden neu gestaltet. Neben einer geringfügigen Anhebung der Einkommensgrenzen wurde u.a. der Begriff des Jahreseinkommens neu definiert.

Zur Umsetzung dieser neuen gesetzlichen Regelungen hat mir das Amt für Wohnung und Städtebauförderung den Entwurf eines Erlasses zur Stellungnahme vorgelegt.

Ich habe zu einer Reihe von Einzelpunkten diese Erlaßentwurfes Stellung genommen. Dabei bestand Anlaß, erneut auf die datenschutzrechtliche Vorgabe (vgl. § 1o Abs. 2 BrDSG) hinzuweisen, daß Daten wie hier die Angaben zum Einkommen grundsätzlich beim Betroffenen mit seiner Kenntnis zu erheben sind und nur unter bestimmten Voraussetzungen eine Datenerhebung bei anderen öffentlichen Stellen, z.B. in Form behördlicher Rückfragen bei Melde- oder Finanzämtern, erfolgen darf.

Das Amt für Wohnung und Städtebauförderung hat mir inzwischen mitgeteilt, daß meine Anregungen im Erlaß und bei der Gestaltung der Vordrucke weitestgehend berücksichtigt werden sollen.

16. Finanzen

16.1. Vorlage des Steuerbescheides statt Nachweis von Einzelangaben

Immer wieder erhalte ich Beschwerden, weil Behörden zur Festsetzung von Beiträgen und Gebühren die Vorlage des kompletten Steuerbescheides verlangen, obwohl sie daraus nur einzelne Angaben wie z.B. die Höhe des Familieneinkommens brauchen. Hinzu kommt, daß diese Ämter zusätzlich auch noch den gesamten Bescheid fotokopieren und diese Kopien zu den Akten nehmen.

Dies widerspricht eklatant dem Grundsatz der Erforderlichkeit, wonach öffentliche Stellen nur die für ihre jeweilige Verwaltungsaufgabe benötigten Angaben vom Bürger erfragen und ihre Akten und Dateien aufnehmen dürfen (vgl. §§ 10 Abs.1,11 BrDSG). Die Finanzbehörden weigern sich jedoch, spezielle Bescheinigungen für z.B. die Berechnung des Kindergartenbeitrages, des Schulgeldes oder des "Bafög" auszustellen. Meine dahingehenden Initiativen bei den Finanzbehörden waren bisher erfolglos; sie verweisen auf den angeblich unverhältnismäßigen Verwaltungsaufwand.

Mein Vorschlag, daß der Antragsteller den Steuerbescheid kopiert und dabei die nicht benötigten Datenfelder abdeckt, hatte wiederum bei den über die Anträge entscheidenden Stellen nur teilweise Erfolg. Immerhin konnte ich in einigen Einzelfällen eine Änderung des Verfahrens, z.B. durch Verringerung der auf den Berechnungsbogen übertragenen Daten, erreichen.

Mir will es noch nicht einleuchten, warum es so schwierig sein soll, mit Hilfe der bestehenden Verfahren der automatisierten Verarbeitung von Steuerdaten Standard-Teilausdrucke etwa über die Höhe des versteuerten Einkommens zu erstellen, wenn man bedenkt, daß diese Angabe Anspruchsvoraussetzung bei zahlreichen Sozialleistungen ist. Ich rechne in diesem Punkt auf die Unterstützung des Datenschutzausschusses.

16.2. Laptops für die Steuerfahndung

Für die im Bereich der Steuerverwaltung geplante Ausstattung der Betriebsprüfer bzw. Steuerfahnder mit Laptops wurde ich an der Ausschreibung beteiligt.

Mit dem in der Ausschreibung formulierten Einsatzkonzept und den dort geforderten Datenschutz- und Datensicherungsmaßnahmen hätte sich ein den grundsätzlich höheren Risiken von tragbaren DV-Geräten entsprechendes hohes Datensicherungsniveau erreichen lassen. Zum Zeitpunkt der Beschaffung war eine diesen Standard bietende Schutzsoftware jedoch nicht verfügbar.

Der Finanzsenator wollte dann, nachdem ein weniger leistungsfähiges Schutzprogramm sich ebenfalls als untauglich erwies, die Laptops lediglich mit einem sog. Bootschutz ausgestattet in Betrieb nehmen. Ich habe mich dagegen ausgesprochen, weil dieser Schutzmechanismus ohne entsprechende Zusatzfunktionen nicht ausreicht.

Die Steuerverwaltung will jetzt doch die Verwendung von Laptops im Bereich der Steuerfahndung und Betriebsprüfung erst nach Installation der entsprechenden Datensicherungssoftware zulassen.

16.3. Finanzamt hilft Handels- und Handwerkskammern

Im letzten Jahr (1994) erhielt ich eine große Anzahl von Anfragen von Gewerbetreibenden nach der Zulässigkeit von Datenübermittlungen der Finanzämter an die Handels- oder Handwerkskammer.

Wie kam es zu dieser Häufung? Erstmals 1994 sind die Kammern durch ein Urteil des Bundesverwaltungsgerichts verpflichtet worden, bei allen Mitgliedern den Kammerbeitrag einzuziehen. In der Vergangenheit ist etwa die Hälfte aller Betroffenen wegen zu geringer Einkünfte nicht herangezogen worden. Manche Gewerbetreibende wußten daher noch nicht einmal von ihrer Kammermitgliedschaft

Seit 1994 versenden die Kammern Beitragsbescheide, bei denen sich die Höhe nach einer Steuermeßzahl (z.B. Umsatz oder Ertrag) richtet. Diese Steuermeßzahl erhalten die Kammern aufgrund der Regelung in § 31 Abs. 1 AO von den zuständigen Finanzbehörden. Diese Datenübermittlungen und die damit verbundene Durchbrechung des Steuergeheimnisses sind mithin explizit zulässig.

Ich habe allerdings diese neue Übermitttlungspraxis zum Anlaß genommen, bei den Kammern "vor Ort" zu überprüfen, ob dort die Datenschutz und Datensicherungsmaßnahmen auch für die von den Finanzämtern zugeleiteten sensible Steuerdaten ausreichen.

Ich konnte feststellen, daß dort nur bestimmte, besonders auf das Steuergeheimnis verpflichtete und mit der Berechnung der Beiträge befaßte Mitarbeiter Zugang zu den Steuermeßzahlen haben. Mitarbeiter mit anderen Aufgaben können ebensowenig zugreifen wie z.B. ehrenamtliche Funktionäre. Bei der Beitragsstelle der Handelskammer Bremen konnte ich mich von der Abschottung dieses Arbeitsbereichs von den anderen Abteilungen überzeugen und insbesondere die Abrufverfahren prüfen. Im anschließenden Beratungsgespräch konnte ich einige Verbesserungsvorschläge, die der Transparenz gegenüber den Mitgliedern förderlich sind, unterbreiten.

17. Datenschutz in der Privatwirtschaft

17.1. Anordnung und Untersagung - die neuen Sanktionsinstrumente der Aufsichtsbehörde nach dem BDSG 1990

17.1.1. Datenschutzkontrolle als Teil staatlicher Wirtschaftsaufsicht

Das novellierte BDSG von 1990 hat der Aufsichtsbehörde für den Datenschutz erstmals Befugnisse eingeräumt, mit deren Hilfe sie bei datenverarbeitenden Stellen in der Privatwirtschaft normgerechten Umgang mit personenbezogenen Angaben gegebenenfalls auch erzwingen kann. Nach dem früheren BDSG konnten die gesetzlichen Anforderungen im nicht-öffentlichen Bereich nicht durch Verwaltungsakt durchgesetzt werden. Mit den Anordnungs- und Untersagungsrechten nach § 38 Abs. 5 BDSG wurde die Stellung der externen Datenschutzkontrolle dem Status anderer Behörden der staatlichen Wirtschaftsaufsicht, etwa im Umweltbereich, angenähert.

In Bremen habe ich von den neuen Sanktionsinstrumenten bisher noch keinen Gebrauch machen müssen. Auch in anderen Bundesländern gibt es noch wenig praktische Erfahrungen. Dies mag nicht zuletzt auch an der Unsicherheit über Anwendungsvoraussetzungen und Verfahren des neuen § 38 Abs. 5 BDSG liegen. Zur Klarstellung auch und gerade gegenüber den bremischen Unternehmen bietet sich dieser Jahresbericht an. In meiner Funktion als Aufsichtsbehörde werde ich die erweiterten Kontrollbefugnisse im Land Bremen nach folgenden Vorgaben und Kriterien handhaben:

17.1.2. Voraussetzungen und Verfahren

17.1.2.1. Dateibezug der Verarbeitung

Für die **Anordnungs- und Untersagungsbefugnisse** des § 38 Abs. 5 gelten die gleichen Bedingungen wie für die Rechte der Aufsichtsbehörde auf Auskunft, Betreten und Einsicht nach § 38 Abs. 3 und 4. Kontrollvoraussetzung bleibt zunächst, daß entweder eine Vorschrift des BDSG oder eine **dateibezogene** Verarbeitung bzw. Nutzung aufgrund einer bereichsspezifischen Norm in Rede steht . Die neuern Befugnisse werden in der Praxis jedenfalls nur dann eingesetzt werden, wenn keine freiwillige Bereitschaft zur Behebung der von der Aufsichtsbehörde gerügten Mängel festzustellen ist.

17.1.2.2. Anordnung

Erster Sanktionsschritt ist die **Anordnung** an die datenverarbeitende Stelle (Satz 1 des § 38 Abs. 5). Sie stellt einen Verwaltungsakt i.S.d. Bremischen Verwaltungsverfahrensgesetzes dar, womit u.a. eine vorherige **Anhörung** notwendig ist. Die Anordnung kann ausschließlich Maßnahmen zur Beseitigung festgestellter **Datensicherungsmängel**, d.h. von Verstößen gegen § 9 BDSG, zum Gegenstand haben. Gefordert werden kann z.B. die Einführung eines Paßwortschutzes oder eines Rückrufverfahren bei Wählleitungen oder die abgeschottete Unterbringung oder Auslagerung von Sicherungsdatenträgern. Die Änderung unrechtmäßiger Formen der Datenverarbeitung, also die Beseitigung von materiellen Rechtsverletzungen, kann die Behörde nicht verlangen; der Bundesrat versuchte noch im Vermittlungsausschuß vergeblich, diese Erweiterung durchzusetzen (vgl. BR-Drucks. 379/90 - Beschluß-Nr. 13).

Allerdings überschneiden sich die materiellrechtlichen und DV- technischen Anforderungen vor allem bei der **Organisationskontrolle** (Nr. 10 der Anlage zu § 9 Satz 1): Rechtswidrige Vorgänge der Datenverwendung können Schlüsse auf eine insgesamt mangelhafte innerbetriebliche Organisation des Datenschutzes zulassen. Die Speicherkontrolle (Nr. 3 der Anl. zu § 9) setzt eine korrekte Erhebung der einzugebenden Daten bzw. wirksame Einwilligungen der Betroffenen voraus. Der **Inhalt** der Anordnung muß sich nicht auf ein von der speichernden Stelle zu erreichendes Sicherungsziel beschränken, bei dem die Art der Realisierung in deren Ermessen steht. Die Aufsichtsbehörde kann im Einzelfall vielmehr auch die **konkrete technische Vorkehrung** vorschreiben, etwa die Einführung einer speziellen Form der Protokollierung von Zugriffen. Allerdings muß die Aufsichtsbehörde in Fällen, in denen ihre Anordnung auch zu einer verstärkten Kontrolle der Arbeitnehmer führen kann (z.B. eine genauere Protokollierung von Zugriffen), darauf achten, nicht in die Mitbestimmungsrechte des Betriebsrats einzugreifen. Anders ausgedrückt: Eine bestimmte technische Realisierung kann nur vorgeschrieben werden, wenn kein Ermessensspielraum besteht.

17.1.2.3. Untersagung

Wird eine Anordnung nach § 38, Abs. 5, Satz 1 nicht befolgt, ermöglicht Satz 2 den weiteren Sanktionsschritt der **Untersagung einzelner Verfahren**, allerdings nur dann, wenn es sich um "**schwerwiegende**" Datensicherungsmängel handelt. Als beispielhafte Kategorie für derartige schwere Defizite nennt Satz 2 Mängel, die mit besonderer Gefährdung des Persönlichkeitsrechts verbunden sind. Maßstab dafür ist zum einen die Sensitivität der betroffenen Daten, wozu § 28 Abs. 2 Nr.1 Satz 2 BDSG einen Hinweis gibt, zum anderen der zu erwartende Schaden, falls sie bekannt oder in sonstiger Weise unzulässig verarbeitet werden. Beispiel für eine derart gravierende Schwachstelle wäre das Patientendatensystem eines Krankenhauses, das ohne wirksamen Zugriffsschutz arbeitet.

§ 38, Abs. 5 verlangt zunächst den Einsatz der Mittel des Verwaltungsvollstreckungsrechts, d.h. die Verhängung eines **Zwangsgeldes** und die Einräumung einer **angemessenen Frist** zur Beseitigung des Mangels. Erst wenn auch diese Instrumente erfolglos bleiben, kann die Aufsichtsbehörde den Einsatz **einzelner Verfahren** untersagen. Nicht möglich ist daher das **sofortige** Verbot eines DV-Verfahrens durch die Behörde, es sei denn, die Unmöglichkeit der Mängelbeseitigung steht von vornherein fest. Die Verfügung der Aufsichtsbehörde kann sowohl ein komplexes Großrechnerverfahren als auch ein einzelnes, vom Anwender selbst programmiertes PC-Verfahren betreffen. Untersagt werden können auch ein spezielles online-Verfahren, die Auftragsdatenverarbeitung bei einem bestimmten unzuverlässigen Vertragspartner oder die Nutzung eines unsicheren Netzes

Eine Untersagungsverfügung nach § 38, Abs. 5, Satz 2 kann und wird für die Aufsichtsbehörde nur das äußerste Mittel sein. Wird sie erfolgreich vor dem Verwaltungsgericht angefochten, drohen Amtshaftungsansprüche des betroffenen Unternehmens bei finanziellen Schäden durch die zeitweilige Stillegung von DV- Verfahren. Unberührt bleibt die Möglichkeit, wegen Zuwiderhandlung gegen eine vollziehbare Anordnung nach Abs. 5 Satz 1 ein **Bußgeldverfahren** einzuleiten (§ 44 Abs. 1 Nr. 7). Die Behörde kann auch den Betroffenen auf den **Rechtsweg** sowie ggf. auf sein **Strafantragrecht** nach § 43 Abs. 4 oder anderen Strafnormen verweisen.

17.1.2.4. Abberufung des betrieblichen Datenschutzbeauftragten

§ 38 Abs. 5 **Satz 3** gibt der Aufsichtsbehörde die Möglichkeit, die Abberufung eines betrieblichen Datenschutzbeauftragten wegen **fehlender Fachkunde und Zuverlässigkeit** zu verlangen. Die Amtl. Begründung des Regierungsentwurfs nennt als maßgebliches Motiv dieser Regelung, daß auf die speichernden Stellen Druck zur Berufung hinreichend qualifizierter Beauftragter ausgeübt werden solle (vgl. BT- Drucks 11/4306, S. 53, zu § 34 Abs. 5)

Bei dem **Abberufungsverlangen** handelt es sich um einen Verwaltungsakt, dem die speichernde Stelle ohne eigenes Entscheidungsermessen nachkommen muß. Unabhängig davon besteht das Risiko eines Bußgeldverfahrens nach § 44 Abs. 1 Nr. 5, da die Benennung eines unqualifizierten Datenschutzbeauftragten der Nichtbestellung gleichzusetzen ist. Bei Defiziten in der Fachkunde aber wird die Aufsichtsbehörde dem Unternehmen immer erst aufgegeben, die Kenntnisse des Beauftragten im Datenschutzrecht durch Nachschulung zu verbessern bzw. verbessern zu lassen, bevor sie die Ablösung verlangt. Anders verhält es sich dann, wenn die Zweifel an der Zuverlässigkeit auf der Inkompatibilität der Funktion des betrieblichen Beauftragten mit anderen Aufgaben beruht, wenn etwa der EDV- Leiter gleichzeitig die interne Kontrollfunktion wahrnehmen soll. Weigert sich das Unternehmen, diesen Zustand abzustellen, ist ein Abberufungsverlangen gerechtfertigt.

17.2. Kreditinformationssysteme und Handelsauskunfteien

17.2.1. Bedeutung für Wirtschaft und Bürger

Kreditinformations-Systeme und Auskunfteien haben im heutigen Wirtschaftsleben große Bedeutung. Der Gesetzgeber des BDSG und die Rechtsprechung haben die Tätigkeit dieser Einrichtungen grundsätzlich akzeptiert, ihre personenbezogene Informationsverarbeitung jedoch bestimmten Regelungen unterworfen. Viele Arbeitnehmer, Handels- und Gewerbetreibende, Freiberufler, Rentner, Sozialleistungsempfänger usw. kommen mit derartigen Einrichtungen in Berührung, oft auch streitig, wie die zahlreichen Eingaben bei mir zeigen.

Für den Normalbürger hat das Kreditinformationssystem der Schufa eine zentrale Bedeutung; für Handel und Gewerbe einschließlich der freien Berufe haben die Handels- und Wirtschaftsauskunfteien, vor allem die Größeren der Branche wie Creditreform, Schimmelpfeng und Bürgel großes Gewicht. Daneben gibt es eine Reihe weiterer spezialisierter Warn- und Infodienste (z.B. die Warndateien der Versicherer), die für die Teilnahme vieler Menschen am Wirtschaftsleben ebenfalls von ausschlaggebender Bedeutung sind. Wegen ihrer z. T. existentiellen Bedeutung für die Teilnahme der Menschen am Wirt-

schaftsleben unserer Gesellschaft kommt der gesetzeskonformen und korrekten Arbeitsweise dieser Einrichtungen eine zentrale Bedeutung zu.

Aus der Bearbeitung von Eingaben ebenso wie aus meiner Prüftätigkeit möchte ich in diesem Bericht einige grundsätzliche Datenschutzfragen dieses Bereichs darstellen.

17.2.2. Nachträgliche Einspeicherung von Negativmerkmalen

Im Berichtsjahr hatte ich mich unter anderem mit dem Problem der nachträglichen Einspeicherung erledigter bzw. nicht-erledigter Negativmerkmale in das Schufa-Informationssystem zu beschäftigen. Negativdaten sind im Sprachgebrauch der Schufa Merkmale über das nicht-vertragsgemäße Verhalten eines privaten Kreditnehmers einschließlich evtl. Merkmale aus den Schuldnerverzeichnissen der Amtsgerichte zu seiner Person. Einzelne dieser Merkmale wie z.B. MB = Mahnbescheid oder KU = Kündigung können dabei durchaus streitig und damit offen sein hinsichtlich ihrer Relevanz für das vertragsmäßige Verhalten eines Kreditnehmers.

In einem Fall wurden Negativdaten zu einer Kreditbeziehung erst ein dreiviertel Jahr nach ihrer Erledigung, in einem anderen Fall sogar erst mehrere Jahre nach ihrer Entstehung in das Informationssystem eingespeichert und weiter genutzt.

Nach dem Schufa-Vertragswerk müssen jedoch Informationen über ein nicht-vertragsgemäßes Verhalten von Kreditkunden von den Kreditinstituten "unverzüglich" der zuständigen Schufa gemeldet werden. Diese Verpflichtung sehe ich als verletzt an, wenn derartige Daten erst so viel später gemeldet und eingespeichert werden. Das schutzwürdige Interesse eines Betroffenen am Ausschluß der Speicherung derartiger Daten ist nach meiner Auffassung in diesen Fällen höher zu bewerten ist als das Speicherungsinteresse der Schufa und ihrer Vertragspartner.Die Schufa muß in diesen Fällen das meldende Kreditinstitut auf die "Verfristung" der Mitteilung hinweisen.

Die Befugnis, das Kreditinformationssystem zu betreiben, ist nach der Rechtsprechung des Bundesgerichtshofs (BGH-Urteil vom 15.12.1983 - III. ZR 207/82) nämlich gekoppelt an die Verpflichtung, nur **richtige** und **aktuelle** Daten zu speichern.

Die Schufa bestreitet meine Rechtsauffassung zur unzulässigen Speicherung nachträglich gemeldeter und eingespeicherter Negativdaten mit dem Argument, daß Verstöße eines Vertragspartners gegen die Verpflichtung zu unverzüglicher Meldung die Zulässigkeit der Verarbeitung dieser Angaben nach § 29 BDSG nicht in Frage stellen können. Ob Betroffene in dieser Sache die Gerichte anrufen, bleibt abzuwarten. Ich werde diese Angelegenheit in den Gremien des Düsseldorfer Kreises weiter verfolgen.

17.2.3. Nachmeldeverfahren

Im Zusammenhang mit der im vorigen Abschnitt geschilderten Fragestellung trat auch das Problem der Übermittlung nachträglich bekanntgewordener Informationen durch die Schufa an ihre jeweiligen Anschlußkunden ohne deren neuerliches Auskunftsersuchen auf (sogenanntes Nachmeldeverfahren).

Vertragspartner der Schufa können Art und Umfang einer Nachmeldung im vorhinein mit der örtlichen Schufa festlegen. Grundlage der Nachmeldungen sind dabei die Mitteilungen anderer Vertragspartner und Informationen aus öffentlichen Verzeichnissen, insbesondere aus den Schuldnerverzeichnissen der Amtsgerichte.

Die Schufa erteilt Nachmeldungen unaufgefordert, das heißt ohne neuerliches Auskunftsersuchen unmittelbar nach Übernahme der Neuinformation in den Datenbestand. Die Zulässigkeit folgert sie aus der bloßen Vermutung, daß das einmal im Zusammenhang mit einem Auskunftsersuchen dargelegte "berechtigte Interesse" des Vertragspartners fortbesteht.

Ich bestreite diese generelle Auffassung zur Auslegung des § 29 Abs. 2 Nr. 1a BDSG schon seit langem. Ich halte allenfalls die Nachmeldung neu bekannt gewordener Negativdaten, die in engem zeitlichen Bezug zu einer neuen Kreditverpflichtung stehen, für ak-

zeptabel, immer vorausgesetzt, daß die Daten unverzüglich - wie es Vertragspflicht ist - an die Schufa übermittelt oder von der Schufa selbst in den Datenbestand eingegeben werden.

Vergleichbare Rechtsprobleme im Hinblick auf das (Fort-)Bestehen des berechtigten Informationsinteresses gibt es auch bei den Wirtschaftsauskunfteien wie z.B. der Creditreform. Auch mein Hamburger Kollege hat sich jüngst kritisch zur Praxis der Nachmeldungen bei einer Handelsauskunftei geäußert (vgl.13. Tätigkeitsbericht des Hamb. DSB für 1994, Ziff. 24.4.). Im Düsseldorfer Kreis, dem Abstimmungsgremium der Obersten Datenschutzaufsichtsbehörden, wird die Angelegenheit weiterverfolgt werden.

17.2.4. Schufa-online-Verfahren

Vertragspartner der Schufa können ihre Auskünfte auf verschiedenen Wegen erhalten, per Brief oder Telefon, per Fax oder Telex/Teletex, per Datenträgeraustausch oder Filetransfer sowie über Terminalkopplung oder Rechner- bzw. Programmkopplung. Die beiden letztgenannten Möglichkeiten, durch Direktanschluß an die zentrale Schufadatenbank selbständig und ohne Mitwirkung der örtlichen Schufageschäftsstellen im Rahmen der eingeräumten Prozeduren Auskünfte erhalten zu können, haben in den letzten Jahren an Bedeutung gewonnen. Auch im Einzugsbereich der Schufa Bremen gibt es inzwischen eine große Zahl von Schufa-Anschlußkunden (überwiegend Banken bzw. Sparkassen), die online, das heißt per Terminal- oder per Rechnerkopplung Anfragen eingeben und Auskünfte erhalten können.

Dieses technische Verfahren bietet beiden Seiten zweifellos Vorteile, beinhaltet jedoch auch datenschutzrechtliche Streitfragen. Sie betreffen zum Beispiel Zeitpunkt und Umfang der Meldepflicht von online-Partnern an die Aufsichtsbehörde gemäß § 32 Abs. 3 Nr. 2 BDSG oder die Reichweite des Auskunftsanspruchs der Betroffenen gemäß § 34 Abs. 1 Nr. 3 BDSG im Hinblick auf die per Direktabruf angeschlossenen Kunden (Kreditinstitute).

Hinzu kommen die Datensicherungsfragen, wie eine unbefugte Nutzung bzw. Abruf-/Zugriffstätigkeit verhindert werden kann und wie die Nutzung des Schufa-Informationssystems zu protokollieren ist. Maßnahmen zur Benutzer- und Zugriffskontrolle müssen sowohl auf seiten der Schufa als auch auf seiten der Anwender (der Schufavertragspartner) vorgesehen werden. Im zentralen DV-System der Schufa läuft nach eigenen Angaben ein Sicherheitssoftwareprodukt mit, das jeden Nutzer nach seiner speziellen Identifikation mit zugehörigem Paßwort oder seiner Netzidentifikation fragt.

Mit dieser Zugriffs- und Benutzerkontrolle kann zwar schufaseitig gewährleistet werden, daß nur solche Benutzer bzw. Vertragspartner Daten abrufen bzw. auf Daten zugreifen können, die im Besitz der o.g. Identifikationskennzeichen sind. Nicht gewährleistet werden kann jedoch, daß bei dem anfragenden Kreditinstitut stets nur die für Abrufe berechtigten Mitarbeiter Zugang zum Datenbestand der Schufa erlangen. Deshalb muß das DV-System der Schufa um Prozeduren zur auch auf einzelne Mitarbeiter bezogenen Berechtigungsprüfung ergänzt werden, wobei diese persönlichen Kennungen zwangsweise vom System abgefordert und geprüft werden müßten. Eine Programmergänzung soll sich nach Aussagen der Schufa derzeit in der Entwicklung befinden.

Auf seiten der Schufa-Vertragspartner, die am online-Verfahren teilnehmen, sind gleichfalls verstärkte Maßnahmen zur Benutzer- und Zugriffskontrolle erforderlich. So ist zum Beispiel darauf zu achten, daß der Kreis der abrufberechtigten Mitarbeiter und ihre Befugnisse exakt definiert sind, daß die Terminal- bzw. Endgerätebenutzung unter Sicherheitsgesichtspunkten technisch und organisatorisch geregelt ist; daß die Paßwortbenutzung einschließlich der Änderungen reglementiert sind, daß die Aufzeichnungspflicht nach § 29 Abs. 2 letzter Satz BDSG sichergestellt ist, daß eine aussagefähige Protokollierung der Zugriffe/Abrufe bzw. der Dateneingaben stattfindet usw. Ich sehe hier eine Gesamtverantwortung der Schufa für ihr DV-System mit der Konsequenz, daß sie die benutzerseitige Gestaltung der Datenzugriffe und Systembenutzungen nicht ihren Vertragspartnern allein überlassen kann.

17.2.5. Versandhäuser als Schufakunden

Versandhäuser gehören ebenfalls zu den Anschlußkunden der Schufa. Sie haben einen sogenannten B-Vertrag, das heißt sie liefern nur Daten über die nicht-vertragsgemäße Abwicklung einer Kreditbeziehung (zum Beispiel eines Versandhauskontos) und können im Gegenzug im Schufasystem gespeicherte Negativdaten übermittelt erhalten. Als Anfragegrund zur Darlegung des berechtigten Interesses wird dabei das Merkmal "VK" gespeichert. Meinungsverschiedenheiten zwischen mir und der Schufa bestehen darüber, inwieweit dieses Merkmal als Auslöser für Datenübermittlungen ohne konkrete Anfrage, also Nachmeldungen (s.o.), verwendet werden darf. Auch dieses Problem werde ich in den zuständigen Gremien des Düsseldorfer Kreises weiterverfolgen.

Ein weiterer Problempunkt ist die Benachrichtigung der Betroffenen über die Tatsache der Speicherung ihrer Daten (vgl. § 33 Abs. 1 Satz 2 BDSG). Bis Ende 1993 hatte die Schufa diese gesetzliche Verpflichtung auf die Versandhäuser verlagert. Dies hat, wie eine Eingabe bei mir zeigte, offensichtlich nicht funktioniert. Seit Anfang 1994 benachrichtigt die Schufa nunmehr selbst in derartigen Fällen.

17.2.6. Stichprobenkontrolle des "berechtigten Interesseses"

Aufkunfteien und ähnliche Datenverarbeiter dürfen nach § 29 Abs. 2 BDSG zulässig gespeicherte Daten nur übermitteln, wenn der Empfänger ein "berechtigtes Interesse" an der Kenntnis dieser Daten glaubhaft dargelegt hat und kein Grund zur Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse am Ausschluß der Übermittlung hat. Die Gründe für das Vorliegen des berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung sind aufzuzeichnen. Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Datenempfänger.

Die Auskunfteien haben also in jedem Einzelfall einer Datenanfrage eine Abwägung der verschiedenen Interessen vorzunehmen; der dargelegte Übermittlungsgrund ist nachprüfbar aufzuzeichnen, von automatisierten Abrufen abgesehen in jedem Fall von der Auskunftei selbst. Die Obersten Datenschutzaufsichtsbehörden haben sich im Hinblick auf die hohe Fallzahl im Anfragegeschäft damit einverstanden erklärt, daß das dargelegte berechtigte Interesse nicht in jedem Einzelfall, sonder nur stichprobenweise von den Auskunfteien überprüft wird.

Die Aufsichtsbehörden haben sich im Falle der Handelsauskunfteien auf ein bis zwei Promille aller Kundenauskünfte pro Auskunftsstelle und Kalenderjahr verständigt, mit einer Mindestquote für kleine Auskunftsstellen. Einbezogen sind dabei auch die sogenannten online-Abrufe, bei denen die zugelassenen Firmen selbständig über entsprechende DV-Technik z.B. Firmendaten aus einem zentralen Datenbestand abrufen können. Auskünfte an Betroffene und Überprüfungen auf Veranlassung der Datenschutzaufsichtsbehörden werden nicht mitgezählt.

Inhaltlich wird bei den Stichprobenkontrollen entweder eine präzise Umschreibung des der Auskunft zugrundeliegenden (belegbaren!) Vorganges oder die Vorlage eines entsprechenden zentralen Dokuments als Nachweis für das Vorhandensein eines berechtigten Interesses verlangt. Ein reines formularmäßiges Ankreuzverfahren ohne Bezug zu einem konkreten Vorgang beziehungsweise Rechtsgeschäft reicht nicht aus.

Über die Höhe der Stichprobe und ihre Bezugsbasis trage ich derzeit eine Meinungsverschiedenheit mit der Auskunftei Creditreform aus. Dabei geht es u.a. darum, daß sich nach meiner Auffassung die Stichprobenkontrollen nicht nur auf Auskünfte über Privatpersonen beziehen dürfen, sondern auch die Firmenauskünfte einschließen müssen. Ich sehe sonst die Gefahr, daß der Kontrollumfang zu stark reduziert wird. Ich werde mit den anderen Aufsichtsbehörden die Handhabung der Stichprobenprüfungen erörtern.

17.2.7. Datenabfrage bei angeblicher Vertragsabsicht

Ein Petent beschwerte sich, daß er telefonisch ziemlich massiv von dem Mitarbeiter einer Auskunftei aufgefordert worden sei, Daten über sich und seine Firma mitzuteilen. Als Begründung sei ihm mitgeteilt worden, daß die Auskunftei selbst um Auskunft gebeten

worden sei und diesem Ersuchen nachkommen wolle. Von wem das Auskunftsbegehren stamme, wurde trotz Nachfrage nicht mitgeteilt.

Meine Überprüfung ergab, daß der Außendienstmitarbeiter einer Lieferantenfirma den Petenten in seiner Firma besucht und Interesse für eine geschäftliche Zusammenarbeit festgestellt hatte. Daraufhin erfolgte eine Kundenstammerfassung bei der Lieferantenfirma und eine Anfrage bei der Auskunftei. Die mit "Geschäftsanbahnung" begründete Anfrage wurde seitens der Auskunftei beantwortet; eine separate Benachrichtung des Betroffenen erfolgte nicht mehr.

Ich habe der Auskunftei gegenüber das dargelegte berechtigte Interesse für die Anfrage nicht akzeptiert mit der Konsequenz, daß die erfolgte Datenübermittlung gemäß § 29 Abs. 2 BDSG nicht zulässig gewesen sei. Als berechtigtes Interesse für eine Datenübermittlung kann nur eine konkrete Vertragsabsicht akzeptiert werden, die durch geeignete Unterlagen zu belegen wäre. Ein einem Außendienstmitarbeiter gegenüber allgemein geäußertes Geschäftsinteresse reicht dafür nicht aus.

Die Auskunftei hat meiner Rechtsauffassung widersprochen. Ich habe dem Petenten zur Wahrnehmung seiner Rechte meine Rechtsauffassung mitgeteilt.

17.3. Schufa-Selbstauskunft von Mietinteressenten

Aus Eingaben erfuhr ich von mehreren Fällen, in denen Vermieter von den Mietinteressenten bzw. Bürgen zur Bonitätsprüfung die Vorlage einer bei der Schufa eingeholten "Selbstauskunft" verlangen. Ich beurteile eine solche Praxis auf der Grundlage des § 28 Abs. 1 BDSG wie folgt:

Zwar kann der Vermieter im Rahmen der Anbahnung eines Mietvertragsverhältnisses durchaus zur Wahrung seiner berechtigten Interessen, insbesondere zur Kalkulierbarkeit von Zahlungsrisiken, dem Mietinteressenten Fragen stellen und Auskünfte verlangen, um feststellen zu können, ob der Bewerber in der Lage ist, die monatlichen Mietzahlungen zu leisten. Insoweit ist der Vermieter berechtigt, z.B. nach Art und Höhe des Einkommens zu fragen.

Eine Schufa-Auskunft ist jedoch hierbei nicht erforderlich, weil der Vermieter dadurch mehr Informationen erhält als er für die Abschätzung seines Risikos benötigt. Hinzu kommt, daß nicht ausgeschlossen werden kann, daß auch Negativdaten zur Person übermittelt werden, die entweder inaktuell geworden sind oder jedenfalls kein unvollständiges Bild über seine wirtschaftliche Situation abgeben (s.o. ausführl. Ziff. 17.2.2). In der kurzen Zeit zwischen Ausschreibung und Vergabe des Mietobjektes wird der Betroffene vielfach keine Möglichkeit mehr haben, unzutreffende Angaben zu seiner Person noch richtigzustellen oder zu vervollständigen.

Im übrigen gehören Wohnungsvermieter mit gutem Grund nicht zum Kreis der zugelassenen Schufa-Vertragspartner, d.h. direkt haben sie keinen Informationszugang. In den Schufa-Richtlinien wird ausdrücklich darauf hingewiesen, daß Anfragen zur Vermietung von Wohn- und Geschäftsräumen unzulässig sind. Durch die Forderung nach der Vorlage einer Selbstauskunft durch den Betroffenen werden diese Regelungen praktisch unterlaufen.

Hinzu kommt ein Mißbrauch des Individualrechts auf Auskunft. Zeitpunkt und Anlaß seiner Geltendmachung sind ausschließlich Sache des Betroffenen. Anders ausgedrückt: Die Nutzung dieses gesetzlichen Schutzrechts auf Veranlassung eines Dritten wie hier zu dem Zweck, die Bonität eines Wohnungsbewerbers zu prüfen, bedeutet eine Verkehrung des gesetzlichen Zwecks dieses Individualanspruchs. Die Freiwilligkeit der Ausübung entfällt erst recht angesichts der allgemeinen Situation der Wohnungsknappheit.

Ich habe den Landesverband Bremischer Haus- und Grundbesitzervereine gebeten, seine Mitglieder in geeigneter Weise auf diese Rechtslage hinzuweisen.

Der Verband hat meiner Auffassung zugestimmt, allerdings betont, aus dem Mitgliederkreis seien ihm bisher keine entsprechenden Fälle bekannt geworden. Inzwischen hat er

das Thema in der Dezember-Ausgabe 1994 seiner Mitgliederzeitung behandelt und dabei auch meine Position dargestellt.

18. Register der nach dem Bundesdatenschutzgesetz meldepflichtigen Stellen

Im Berichtsjahr habe ich erneut eine große Anzahl von Unternehmen, insbesondere Inkassobüros, Kreditschutzorganisationen, Detekteien und Auskunfteien, EDV-Beratungsservice-Firmen, Verlags- und Vertriebsgesellschaften, Organisations- und Beratungsfirmen, Entwicklungsgesellschaften für Kommunikationssysteme, Markt- und Meinungsforschungsinstitute, Entsorgungs- und Umweltdienstleistungsbetriebe, Wirtschafts- und Finanzberatungsfirmen, Mikrofilmservicebetriebe und Adreßhändler angeschrieben und um Prüfung der Meldepflicht nach § 32 BDSG und ggf. Anmeldung ihres Unternehmens gebeten.

Dreiundzwanzig Firmen haben sich daraufhin zu dem bei mir zu Kontrollzwecken geführten Register neu gemeldet. Bei mehreren Unternehmen, die eine Pflicht zur Anmeldung verneint haben, ist aufgrund der zum Teil widersprüchlichen Angaben durch Prüfungen vor Ort zu klären, ob nicht doch die gesetzlichen Voraussetzungen vorliegen.

Insgesamt sind derzeit im Register 100 meldepflichtige Stellen verzeichnet, von denen 83 in Bremen und 17 in Bremerhaven ihren Sitz haben. Weitere Verschiebungen zum alten Berichtsjahr haben sich ergeben, weil einige Firmen gelöscht wurden.

Einzelheiten zeigt die folgende Tabelle:

Art der Tätigkeit	insgesamt	Bremen	Bremerhaven
1. Speicherung personenbezogener Daten zum Zwecke der Übermittlung (insgesamt)	7	4	3
- Auskunfteien	5	4	1
- Detekteien	1		1
- Adreßverlage/Adreßhändler	1		1
2. Speicherung personenbezogener Daten zum Zwecke der anonymisierten Übermittlung (insgesamt)	1		1
-Markt-u. Meinungsforschung	1		1
3. Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (insgesamt)	92	78	14
- Datenerfassung	10	9	1
- Dienstleistung/RZ	74	62	12
- Mikroverfilmer	3	3	
- Mailboxdienste			1
- Entsorgungsbetriebe	4	4	
Gesamt	100	83	17

Stand: 15.01.1995

19. Anlage

Merkblatt zum Datenschutz bei Erhebungen, Untersuchungen und Forschungsvorhaben an öffentlichen Schulen im Lande Bremen

1. Der Umgang mit personenbezogenen Daten von Schülern greift nicht nur in bestehende Elternrechte, sondern auch in das informationelle Selbstbestimmungsrecht der Schüler und ggf. ihrer Erziehungsberechtigten ein. Der bremische Gesetzgeber hat deshalb die Verarbeitung derartiger Daten eingeschränkt und an bestimmte Zwecke gebunden. Die Verarbeitung von Schülerdaten bei Erhebungen, Untersuchungen und wissenschaftlichen Forschungsvorhaben an Schulen ist dabei besonders geregelt worden.

2. Zu beachten sind das Bremische Gesetz zum Datenschutz im Schulwesen (BrSchDSG) sowie das Bremische Datenschutzgesetz (BrDSG). Das BrSchDSG ergänzt die schulrechtlichen Regelungen und gilt vorrangig vor dem BrDSG.

3. Nach § 13 Abs. 1 BrSchDSG können der Senator für Bildung und Wissenschaft sowie der Magistrat Bremerhaven zur Wahrnehmung der ihnen als Schulbehörde obliegenden Aufgaben Erhebungen vornehmen und Untersuchungen durchführen oder sie durch Dritte vornehmen und durchführen lassen. Dabei müssen die Erhebung oder die Untersuchung jeweils in sich abgeschlossen sein. Die Ermächtigung gilt also für den Senator für Bildung und Wissenschaft in Bezug auf innere und äußere Schulangelegenheiten sowie als Anstellungskörperschaft für die Lehrer in Bremen, für den Magistrat Bremerhaven in Bezug auf äußere Schulangelegenheiten, evtl. übertragene innere Schulangelegenheiten sowie als Anstellungskörperschaft für die Lehrer in Bremerhaven.

4. Bei derartigen Erhebungen und Untersuchungen können auch die Schülerdaten, die nach § 2 BrSchDSG zulässigerweise in der Schule gespeichert sind, (z.B. in der Schülerkartei, Schullaufbahnakte) genutzt werden, wenn die Betroffenen hierin eingewilligt haben. Mit Einwilligung der Betroffenen können weitere Daten erhoben, gespeichert und genutzt werden.

   Vom Grundsatz der Einwilligung kann abgewichen werden, wenn das öffentliche Interesse an der Erhebung oder Untersuchung die schutzwürdigen Belange der Betroffenen überwiegt und der Zweck der Erhebung oder Untersuchung nicht auf andere Weise (z.B. durch Verwendung vorhandenen aggregierten statistischen Materials) oder nur mit unverhältnismäßigem Aufwand (z.B. Eltern/Kinder sind ins Ausland verzogen) erreicht werden kann (Abwägung des öffentlichen Interesses mit den schutzwürdigen Belangen der Betroffenen d. h. deren Grundrechtspositionen und Alternativ- bzw. Aufwandsprüfung!). Das Abweichen vom Einwilligungserfordernis muß begründet werden.

   Auch für die Erhebung von personenbezogenen Schülerdaten bei Lehrern gilt der Grundsatz der Einwilligung der Betroffenen.

5. Eine wirksame Einwilligung setzt voraus, daß die Betroffenen über das geplante Vorhaben und über Art, Umfang und Zweck der Nutzung ihrer persönlichen Angaben aufgeklärt werden. Die Teilnahme an dem Vorhaben muß den Betroffenen freigestellt sein.

   Die Einwilligung ist in der Regel schriftlich zu geben. Folge aus § 22 BrSchDSG i.V.m. § 3 BrDSG. Bei minderjährigen Schülern (bis zur Jahrgangsstufe 10) müssen die Erziehungsberechtigten ihre Einwilligung erteilen und vorher aufgeklärt werden. Ab Sek.Stufe II bedarf es auch der Einwilligung der Schüler. Ausnahmsweise kann eine mündliche, telefonische o.ä. Zustimmungserklärung ausreichend sein. Eine pauschale Einwilligungserklärung bei Eintritt eines Schülers in die Schule kann für derartige Datenerhebungen und Untersuchungen nicht gegeben werden, weil die Zwecke im vorhinein nicht beschrieben werden können.

6. Bei der Durchführung eines Vorhabens gemäß § 13 Abs. 1 und 2 BrSchDSG sind die Identifikationsdaten von den Erhebungsdaten getrennt zu halten. Die Merkmale, mit deren Hilfe ein Personenbezug herstellbar ist, sind gesondert zu speichern, d. h. möglichst frühzeitige Anonymisierung der Erhebungs- bzw. Untersuchungsdaten. Auswertungen haben nur aus den nicht-personenbezogenen Datenbeständen zu erfolgen. Auf die abgetrennten personenbezogenen Daten darf nur in begründeten Ausnahmefällen und von ausdrücklich dazu ermächtigten Personen zugegriffen werden. Sie sind zu löschen, sobald der Zweck der Erhebung oder der Untersuchung erreicht ist, spätestens jedoch, wenn das Vorhaben beendet ist. Auswertungen sind so vorzunehmen, daß aus den Ergebnissen (z. B. Ausdrucken, Tabellen) ein Personenbezug nicht zu erkennen ist.

   Für alle Erhebungen und Untersuchungen gilt das Prinzip der strikten Zweckbindung: Die beim Betroffenen oder bei Schulen bzw. Behörden erhobenen Daten dürfen nur für die jeweilige Erhebung bzw. Untersuchung und nur im Rahmen der erteilten Einwilligung ausgewertet werden. Eine Nutzung der Daten zu anderen Zwecken ist unzulässig.

7. § 13 Abs. 6 BrSchDSG schreibt die vorherige Unterrichtung des Landesbeauftragten für den Datenschutz, des Eltern- und des Schülerbeirats und bei Einbeziehung mehrerer Schulen der zuständigen Gesamtvertretungen vor. Die Unterrichtung ersetzt nicht die Einholung der individuellen Einwilligungen. Bei wissenschaftlichen Forschungsvorhaben verlangt § 13 Abs. 7 BrSchDSG zusätzlich die vorherige Genehmigung des Senators für Bildung und Wissenschaft.

8. §§ 18-20 BrSchDSG und § 6 BrDSG schreiben den beteiligten Datenverarbeitern (Schulen, Schulbehörden oder ihren Beauftragten, Schulforschern) vor, angemessene Maßnahmen zur Sicherung der personenbezogenen Daten zu treffen. Derartige Maßnahmen beziehen sich nicht nur auf die Organisation des Vorhabens (z. B. wer? wann? wo?), sondern auch auf seine Durchführung (z. B. Datenerhebung innerhalb oder außerhalb der Klasse? Schulpflichtsituation? Beteiligung der Lehrer?), die Aufbewahrung der Unterlagen und Materialien mit personenbezogenem Inhalt, z. B. wie? wo? wie lange?), die Nutzung der Daten (z. B. Wer hat Zugang zu den Daten? zum System? zweckgebundene Auswertung? Datenweitergabe?) sowie die Datenlöschung (Erhebungsunterlagen? sonstige Datenträger?). Die Sicherungsmaßnahmen müssen schon bei Planung des Vorhabens zusammen mit den Projektverantwortlichen festgelegt werden.

9. Aus dem BrDSG ergeben sich für die Datenverarbeiter dieses Bereichs unter Umständen noch weitere Verpflichtungen (sofern personenbezogene Daten verarbeitet werden und es sich nicht um einen temporären Verarbeitungsvorgang handelt), zum Beispiel

   - Unterrichtung der beteiligten Mitarbeiter über zu beachtende Datenschutzvorschriften und ggf. deren Verpflichtung auf das Datengeheimnis,

   - Erstellung einer Beschreibung der Dateien und eines Geräteverzeichnisses.

20. Beschlüsse der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Jahr 1994

20.1. Chipkarten im Gesundheitswesen

Entschließung vom 09./10. März 1994

Die Datenschutzbeauftragten von Bund und Länder verfolgen die zunehmende Verwendung von Chipkarten im Gesundheits- und Sozialwesen mit kritischer Aufmerksamkeit.

Chipkarte als gesetzliche Krankenversicherungskarte

Die Krankenversicherungskarte, die bis Ende des Jahres in allen Bundesländern eingeführt sein wird, darf nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten. Die Datenschutzbeauftragten überprüfen, ob

- die Krankenkassen nur die gesetzlich zulässigen Daten auf den Chipkarten speichern und
- die Kassenärztlichen Vereinigungen dafür sorgen, daß nur vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte Lesegeräte und vom Bundesverband der Kassenärztlichen Vereinigungen geprüfte Programme eingesetzt werden.

Chipkarte als freiwillige Gesundheitskarte

Sogenannte "Gesundheitskarten", etwa "Service-Karten" von Krankenversicherungen und privaten Anbietern, "Notfall-Karten", "Apo(theken)-Cards" und "Röntgen-Karten" werden neben der Krankenversicherungskarte als freiwillige Patienten-Chipkarte angeboten und empfohlen. Während die Krankenversicherungskarte nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten darf, kann mit diesen "Gesundheitskarten" über viele medizinische und andere persönliche Daten schnell und umfassend verfügt werden.

Gegenüber der konventionellen Ausweiskarte oder einer Karte mit einem Magnetstreifen ist die Chipkarten-Technik ungleich komplexer und vielfältig nutzbar. Damit steigen auch die Mißbrauchsgefahren bei Verlust, Diebstahl oder unbemerktem Ablesen der Daten durch Dritte. Anders als bei Ausweiskarten mit Klartext können Chipkarten nur mit technischen Hilfsmitteln gelesen werden, die der Betroffene in der Regel nicht besitzt. So kann er kaum kontrollieren, sondern muß weitgehend darauf vertrauen, daß der Aussteller der Karte und sein Arzt nur die mit ihm vereinbarten Daten im Chip speichern, das Lesegerät auch wirklich alle gespeicherten Daten anzeigt und der Chip keine oder nur eindeutig vereinbarte Verarbeitungsprogramme enthält.

Die Freiwilligkeit der Entscheidung für oder gegen die Gesundheitskarte mit Chipkarten-Technik ist in der Praxis bisweilen nicht gewährleistet. So wird ein faktischer Zwang auf die Entscheidungsfreiheit des Betroffenen ausgeübt, wenn der Aussteller - etwa ein Krankenversicherungsunternehmen oder eine Krankenkasse - mit der Einführung der Chipkarte das bisherige konventionelle Verfahren erheblich ändert, z.B. den Schriftwechsel erschwert oder den Zugang zu Leistungen Karten-Inhabern vorbehält bzw. erleichert.

So stellt beispielsweise eine Kasse ihren Mitgliedern Bonuspunkte in Aussicht, wenn sie auf sog. Aktionstagen der Kasse Werte wie Blutzucker, Sauerstoffdynamik, Cholesterol sowie weitere spezielle medizinische Daten ohne ärztliche Konsultation messen und auf der Karte speichern und aktualisieren lassen. In Abhängigkeit von der Veränderung dieser Werte wird von der Kasse gegebenenfalls ein Arztbesuch empfohlen. Die Vergabe solcher Bonuspunkte widerspricht dem Prinzip der Freiwilligkeit bei der Erhebung der Daten für die Patienten-Chipkarte. Der Effekt wird noch verstärkt, indem die Kasse die "Möglichkeit einer Beitragsrückerstattung" in Aussicht stellt. Die Datenschutzbeauftragten des Bundes und der Länder sehen in dieser Art der Anwendung der Chipkarten-Technik das Risiko eines Mißbrauchs, solange der Inhalt und die Nutzung der Daten nicht mit den zuständigen Fachleuten - wie den Medizinern - und den Krankenkassen abgestimmt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält für den Einsatz und die Nutzung freiwilliger Patienten-Chipkarten zumindest - vorbehaltlich weiterer Punkte - die Gewährleistung folgender Voraussetzungen für erforderlich:

- Die Zuteilung einer Gesundheitskarte und die damit verbundene Speicherung von Gesundheitsdaten bedarf der schriftlichen Einwilligung des Betroffenen. Er ist vor der Erteilung der Einwilligung umfassend über Zweck, Inhalt und Verwendung der angebotenen Gesundheitskarte zu informieren.
- Die freiwillige Gesundheitskarte darf nicht - etwa durch Integration auf einem Chip - die Krankenversichertenkarte nach dem Sozialgesetzbuch verdrängen oder ersetzen.
- Die Karte ist technisch so zu gestalten, daß für die einzelnen Nutzungsarten nur die jeweils erforderlichen Daten zur Verfügung gestellt werden.
- Der Betroffene muß von Fall zu Fall frei und ohne Benachteiligung - z.B. gegenüber dem Arzt, der Krankenkasse oder der Versicherung - entscheiden können, die Gesundheitskarte zum Lesen der Gesundheitsdaten vorzulegen und ggf. den Zugriff auf bestimmte Daten zu beschränken. Er muß ferner frei entscheiden können, wer welche Daten in seinen Datenbestand übernehmen darf. Der Umfang der Daten, die gelesen oder übernommen werden dürfen, ist außerdem durch die gesetzliche Aufgabenstellung bzw. den Vertragszweck der Nutzer beschränkt.
- Der Kartenaussteller muß sicherstellen, daß der Betroffene jederzeit vom Inhalt der Gesundheitskarte unentgeltlich Kenntnis nehmen kann.
- Der Betroffene muß jederzeit Änderungen und Löschungen der gespeicherten Daten veranlassen können.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dafür aus, daß der Gesetzgeber dies durch bereichsspezifische Rechtsgrundlagen sicherstellt.

20.2. Informationsverarbeitung im Strafverfahren

Entschließung vom 09./10. März 1994

Die Datenschutzbeauftragten des Bundes und der Länder erinnern an ihre Vorschläge zu gesetzlichen Regelungen der Informationsverarbeitung im Strafverfahren, die sie seit 1981 unterbreitet haben.

Während die Befugnisse von Polizei und Staatsanwaltschaft zur Datenerhebung bei Ermittlungen mittlerweile in weitreichender Form gesetzlich abgesichert wurden, fehlen weiterhin Regelungen in der Strafprozeßordnung, wie die erhobenen Daten in Akten und Dateien weiter verarbeitet werden dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder halten die Beachtung folgender Grundsätze für notwendig, die in den Entwürfen des Bundes (Art. 4 §§ 474 ff. StPO des Entwurfs für ein Verbrechensbekämpfungsgesetz - BT-Drucksache 12/6853) und der Länder (Entwurf eines Strafverfahrensänderungsgesetzes 1994 des Strafrechtsausschusses der Justizministerkonferenz) nicht ausreichend berücksichtigt sind:

1. Strafrechtliche Ermittungsakten enthalten eine Vielzahl höchstsensibler Daten insbesondere auch über Opfer von Straftaten und Zeugen, die deshalb eines wirksamen Schutzes bedürfen. Es würde den Besonderheiten der im Strafverfahren - auch mit Zwangsmitteln - erhobenen Daten nicht entsprechen, wenn Strafakten als Informationsquelle für jegliche Zwecke anderer Behörden oder von nicht am Strafverfahren Beteiligten dienten. Die einzelnen Zwecke und die zugriffsberechtigten Stellen sind daher abschließend normenklar festzulegen.

1.1 Ingesamt ist sicherzustellen, daß der in anderen Zweigen der öffentlichen Verwaltung verbindlich geltende Standard des Datenschutzes für Übermittlungen keinesfalls unterschritten wird.

1.2 Soweit ein unabweisbarer Bedarf anderer Stellen an Informationen aus Strafverfahren besteht, ist er in erster Linie durch Erteilung von Auskünften zu befriedigen. Akteneinsichtnahmen oder Aktenübersendungen können erst dann zugelassen werden, wenn eine Auskunftserteilung nicht ausreicht. Nicht erforderliche Aktenteile müssen ausgesondert werden. An Privatpersonen dürfen Informationen aus strafrechtlichen Ermittlungen nur weitergegeben werden, wenn deren rechtliche Interessen davon abhängen.

2. Bei Regelungen zur dateimäßigen Speicherung ist zu unterscheiden zwischen Systemen zur Vorgangsverwaltung (wie z.B. zentrale Namensdateien) und Dateien, die der Unterstützung strafprozessualer Ermittlungen dienen (z.B. Spurendokumentations- und Recherchesysteme).

2.1 Der Datensatz zur Vorgangsverwaltung ist auf die Angaben zu beschränken, die zum Auffinden der Akten und zur Information über den Verfahrensstand erforderlich sind. Daten über Personen, die keine Beschuldigten sind, dürfen nur dann erfaßt werden, wenn dies zur Vorgangsverwaltung zwingend erforderlich ist. In diesen Fällen bedarf es besonderer Zugriffs- und Verwendungsbeschränkungen.

In jedem Fall sind die Daten entsprechend dem Verfahrensstand zu aktualisieren. Vom Gesetzgeber sind konkrete Löschungsfristen vorzusehen. Die Speicherung ist längstens auf den Zeitpunkt zu begrenzen, für den die Akte aufbewahrt wird. Vorgangsverwaltungssysteme können so auch für eine wirksame Kontrolle der Aufbewahrungsfristen genutzt werden.

2.2 Die Staatsanwaltschaft kann sich zur Verwaltung ihres konventionell gespeicherten Datenmaterials grundsätzlich eines behördeninternen, automatisierten Nachweissystems bedienen. Länderübergreifende automatisierte Informationssysteme dürfen in Beachtung des Erforderlichkeitsprinzips demgegenüber allenfalls für solche Vorgänge errichtet werden, bei denen bestimmte Tatsachen die Prognose begründen, daß auf die erfaßten Daten zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben (erneut) zugegriffen werden muß.

Eine solche Prognose wird in der Regel dann nicht gerechtfertigt sein, wenn das zugrundeliegende Verfahren mit einer Einstellung nach § 170 Abs. 2 StPO oder einem rechtskräftigen Freispruch abgeschlossen worden ist, sofern nicht auch nach Abschluß des Verfahrens noch tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte eine strafbare Handlung begangen hat. Eine Bereitstellung von Daten jedenfalls zu Zwecken der Strafverfolgung wird ferner grundsätzlich dann nicht in Betracht kommen, wenn die Ermittlungen konkrete Anhaltspunkte dafür bieten, daß der Beschuldigte nicht erneut strafbare Handlungen begehen wird. Dies kann z.B. bei Fahrlässigkeitstaten der Fall sein. Bei laufenden Verfahren kann die Zulässigkeit der Aufnahme von Daten im Hinblick auf die Möglichkeiten einer Verbindung von Verfahren, die Einstellung nach § 154 StPO oder die Gesamtstrafenbildung gegeben sein.

2.3 Für einen Informationsverbund zwischen verschiedenen speichernden Staatsanwaltschaften mit der Möglichkeit eines Direktzugriffs auf die Daten der jeweils anderen Behörden ergibt sich als Voraussetzung, daß die Weitergabe aller dem Zugriff unterliegenden Daten zumindest bei abstrakter Betrachtung zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben der übermittelnden oder der zugriffsberechtigten Stellen geeignet und angemessen sein muß.

Für den Bereich der Strafverfolgung gilt ein umfassendes Aufklärungsgebot (§§ 152 Abs. 2, 160 StPO). Die Staatsanwaltschaft kann im Rahmen ihrer Ermittlungen grundsätzlich ohne Rücksicht auf das Gewicht des Tatvorwurfs von allen öffentlichen Behörden - also auch von anderen Staatsanwaltschaften - Auskunft verlangen (§ 161 Satz 1 StPO). Diese Auskunftspflicht besteht über das Ermittlungsverfahren hinaus bis zum Abschluß des Strafverfahrens. Daten, die im Falle einer entsprechenden Anfrage zu mit einem Strafverfahren zusammenhängenden Zwecken offenbart werden müßten, können damit - ungeachtet der besonderen Voraussetzungen für die Errichtung eines Direktabrufverfahrens - von jeder Staatsanwaltschaft für andere Staatsanwaltschaften grundsätzlich auch in einem Informationssystem mit Direktab-

rufmöglichkeit bereitgestellt werden, sofern nur bestimmte Tatsachen die Annahme rechtfertigen, daß die Daten in einem Verfahren einer anderen Behörde verwertet werden müssen. Eine solche Annahme wird regelmäßig wiederum in den unter 2.2 dargestellten Fällen nicht zu begründen sein. Eine Bereitstellung von Daten wird darüber hinaus auch dann nicht erfolgen können, wenn diese einem besonderen Amtsgeheimnis unterliegen und deshalb auch auf Anforderung nicht ohne weiteres übermittelt werden dürften. Auf § 78 SGB X ist in diesem Zusammenhang hinzuweisen. Ein Direktabruf durch andere Stellen als Staatsanwaltschaften ist schon nach der Zweckbestimmung des Systems ausgeschlossen.

2.4 In der Praxis dienen derzeit die bestehenden polizeilichen Informationssysteme auch den Zwecken der Strafverfolgung. Eine Abstimmung der polizeilichen und der staatsanwaltschaftlichen Informationssysteme ist geboten. Eine weitere Abstimmung wird im Hinblick auf das Bundeszentralregister zu erfolgen haben, das ebenfalls Daten zu Zwecken der Strafverfolgung, aber auch der Strafvollstreckung speichert.

Die Datenschutzbeauftragten halten daher eine grundlegende Überarbeitung dieser Entwürfe für notwendig und bieten hierfür ihre Unterstützung an (vgl. Beschlüsse der Datenschutzkonferenzen vom 28./29. September 1981 zu "Mindestanforderungen für den Datenschutz bei den Zentralen Namenskarteien der Staatsanwaltschaften", vom 24./25. November 1986 "Überlegungen zu Regelungen der Informationsverarbeitung im Strafverfahren" und vom 05./06. April 1989 zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts vom 03. November 1988).

20.3. Abbau des Sozialdatenschutzes

Entschließung vom 09./10. März 1994

Der Gesetzgeber hat in den vergangenen Monaten die Möglichkeit der Überprüfung von Sozialleistungsempfängern ohne deren vorherige Befragung oder Kenntnis in drastischem Umfang vermehrt. Insbesondere durch das seit dem 1. Juli 1993 geltende Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms ist das Kontrollinstrumentarium von Sozial- und Arbeitsämtern noch einmal erheblich erweitert worden. Ohne Rücksicht auf konkrete Anhaltspunkte für einen unberechtigten Leistungsbezug im Einzelfall sind künftig automatisierte Datenabgleiche zwischen Sozialhilfeträgern sowie zwischen diesen und der Arbeitsverwaltung bzw. der Kranken-, Unfall- und Rentenversicherung gestattet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist sehr besorgt über diese Entwicklung, die zu einem immer dichteren Datenverbundsystem im Sozialleistungsbereich und zu immer nachhaltigeren Eingriffen in das Recht auf informationelle Selbstbestimmung aller Betroffenen, d. h. auch und gerade der großen Mehrheit rechtstreuer Antragsteller und Leistungsbezieher, führt.

Mit Nachdruck wenden sich die Datenschutzbeauftragten gegen Versuche von Sozialverwaltungen, bei der Umsetzung der neuen Kontrollregelungen durch extensive Interpretation über den gesetzlich vorgegebenen Rahmen hinauszugehen. So erlaubt beispielsweise der neugefaßte § 117 Abs. 3 des Bundessozialhilfegesetzes entgegen der Handhabung einzelner Kommunen keinen automatisierten Datenabgleich zwischen Sozialhilfedatei und Kraftfahrzeug-Register, sondern nur den Vergleich von Angaben in Verdachtsfällen.

Die dargestellte Entwicklung macht es erneut notwendig, auf die verfassungsrechtliche Qualität des Grundsatzes der Datenerhebung beim Betroffenen hinzuweisen. An dem Prinzip, daß bei der Überprüfung der Leistungsberechtigung und der Nachweise Auskünfte zunächst beim Antragsteller anzufordern sind und nur aufgrund konkreter Verdachtsmomente Nachfragen bei dritten Stellen oder Datenabgleiche erfolgen dürfen, muß für den Regelfall festgehalten werden, soll der Einzelne mündiger Bürger bleiben und nicht zum bloßen Objekt staatlicher Verhaltenskontrolle werden.

Sorge äußert die Konferenz auch über die hartnäckigen Bestrebungen, Datenbestände der Sozialverwaltung für immer neue Zwecke und Adressaten zu öffnen. Beispiele dafür sind

die im Gesetzgebungsverfahren zum 2. SGB-Änderungsgesetz im letzten Augenblick gescheiterten Anträge, Polizei und Staatsschutz in unvertretbarem Umfang Zugriff auf Daten Arbeitsloser und sonstiger Sozialleistungsempfänger zu geben. Das Sozialgeheimnis muß ein wirksamer Sonderschutz für die besonders sensiblen Daten in der Sozialverwaltung bleiben. Nur dies entspricht der Abhängigkeit des Einzelnen von staatlichen Leistungen und der sich daraus ergebenden speziellen Verletzlichkeit seines Rechts auf informationelle Selbstbestimmung.

20.4. Gesetzentwurf der Bundesregierung zur Neuordnung des Postwesens und der Telekommunikation (Postneuordnungsgesetz - PTNeuOG, BR-Drs. 115/94 = BT-Drs. 12/6718) und zu der dafür erforderlichen Änderung des Grundgesetzes (BR-Drs. 114/94 = BT-Drs. 12/6717)

Entschließung vom 09./10. März 1994

I.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, daß mit der Umwandlung der Deutschen Bundespost POSTDIENST in die Deutsche Post AG und der Deutschen Bundespost TELEKOM in die Deutsche Telekom AG zwei staatliche Einrichtungen aufhören zu existieren, gegenüber denen sich der Bürger bisher unmittelbar auf das Post- und Fernmeldegeheimnis berufen kann. Sie treten deshalb dafür ein, in der Verfassung sicherzustellen, daß jeder, der Post- und Fernmeldedienstleistungen erbringt, das Post- und Fernmeldegeheimnis zu wahren hat.

II.

Im Gesetz zur Neuordnung des Postwesens und der Telekommunikation ist ein den Vorgaben des Bundesverfassungsgerichts in seinem Volkszählungsurteil vom 15. Dezember 1983 und in seinem Fangschaltungsbeschluß vom 25. März 1992 entsprechender Schutz von Individualrechten zu gewährleisten.

Die Datenschutzbeauftragten halten inbesondere folgende Änderungen des Gesetzentwurfs für erforderlich:

a) Der Umfang der zulässigen Verarbeitung personenbezogener Daten im Post- und Telekommunikationswesen ist im Gesetz selbst festzulegen; lediglich deren konkrete Ausgestaltung kann der Regelung durch Rechtsverordnungen überlassen bleiben.

b) Die Gewährleistung des Datenschutzes und des Post- und Fernmeldegeheimnisses muß in den Katalog der Ziele der Regulierung aufgenommen werden.

c) Das Post- und Telekommunikationswesen muß auf Dauer - auch nach dem Wegfall der Monopole - einer effektiven, unabhängigen datenschutzrechtlichen Kontrolle von Amts wegen nach bundesweit einheitlichen Kritierien unterworfen bleiben, auch soweit personenbezogene Daten nicht in Dateien verarbeitet werden.

d) Die Frist für die Speicherung von Verbindungsdaten zur Ermittlung und zum Nachweis der Entgelte ist präzise festzulegen.

e) Die vorgesehene Vorschrift zum Einzelentgeltnachweis schränkt den Kreis der Einrichtungen, die Telefonberatung durchführen und die nicht auf Einzelentgeltnachweisen erscheinen sollen, in unakzeptabler Weise ein. Dem Schutz des informationellen Selbstbestimmungsrechtes und des Fernmeldegeheimnisses der Angerufenen würde es dagegen am ehesten entsprechen, wenn jeder inländische Anschlußinhaber selbst entscheiden kann, ob und gegebenenfalls wie seine Rufnummer auf Einzelentgeltnachweisen erscheinen soll. Damit wäre auch die Anonymität von Anrufen bei Beratungseinrichtungen unbürokratisch sicherzustellen. Ein entsprechendes Verfahren wird in den Niederlanden bereits praktiziert.

f) Es wäre völlig unangemessen, wenn in Zukunft erlaubt würde, daß die Telekommunikationsunternehmen Nachrichteninhalte über die Befugnisse des § 14a Fernmel-

deanlagengesetz hinaus auch für die Unterbindung von Leistungserschleichungen und sonstiger rechtswidriger Inanspruchnahme des Telekommunikationsnetzes und seiner Einrichtungen sowie von Telekommunikations- und Informationsdienstleistungen erheben, verarbeiten und nutzen dürften.

III.

Die Datenschutzbeauftragten betonen, daß angesichts der neuen technischen Möglichkeiten digitaler Kommunikations- und Informationsdienste und der mit ihrer Nutzung zwangsläufig verbundenen Datenverarbeitung eine grundlegende Überarbeitung des § 12 Fernmeldeanlagengesetz, der die Weitergabe vorhandener Telekommunikationsdaten in Strafverfahren erlaubt, überfällig ist. Sie erinnern an die Umsetzung der entsprechenden Entschließung des Bundesrates vom 27. August 1991 (BR-Drs. 416/91).

20.5. Ausländerzentralregistergesetz

Entschließung vom 09./10. März 1994

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

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

Zwar enthält dieser Gesetzentwurf gegenüber früheren Entwürfen eine Reihe datenschutzrechtlicher Verbesserungen, Bedenken bestehen jedoch weiterhin: Die Datenschutzbeauftragten wenden sich insbesondere dagegen, daß das Ausländerzentralregister nicht nur als Informations- und Kommunikationssystem für die mit der Durchführung ausländer- und asylrechtlicher Vorschriften betrauten Behörden dienen, sondern darüber hinaus als Informationsverbund für Aufgaben der Polizei, Strafverfolgungsorgane und Nachrichtendienste zur Verfügung stehen soll. Die Funktionserweiterung wird deutlich durch die Speicherung von Erkenntnissen der Sicherheitsbehörden zu Ausländern in das Register. So soll der INPOL-Fahndungsbestand des BKA, soweit er Ausschreibungen zur Festnahme und zur Aufenthaltsermittlung von Ausländern enthält, in das Ausländerzentralregister übernommen werden. Gleiches gilt für die vorgesehene Speicherung von Angaben zu Personen, bei denen Anhaltspunkte für den Verdacht bestehten, daß sie im einzelnen bezeichnete Straftaten planen, begehen oder begangen haben. Diese Informationen dienen nicht einem Informationsbedarf zur Erfüllung ausländerbehördlicher Aufgaben, sondern - worauf die Entwurfsbegründung hinweist - der Kriminalitätsbekämpfung. Für diese Zwecke stehen den Sicherheitsbehörden aber eigene Informationssysteme zur Verfügung. Nach Auffassung der Datenschutzbeauftragten dürfen deshalb derartige Erkenntnisse nicht in das Register aufgenommen werden.

Die im Entwurf vorgesehenen Voraussetzungen unter denen u.a. für Polizeibehörden, Staatsanwaltschaften und Nachrichtendienste automatisierte Abrufverfahren eingerichtet werden können, stellen keine wirksamen Vorkehrungen für eine Begrenzung der Abrufe dar. Besonders problematisch ist der geplante automatisierte Zugriff durch die Nachrichtendienste auf einen - wenn auch reduzierten - Datensatz. Für die Dienste ist in den jeweiligen bereichsspezifischen Gesetzen der automatisierte Abruf aus anderen Datenbeständen ausgeschlossen. Die Erforderlichkeit derartiger Abrufe ist in keiner Weise belegt.

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

20.6. Vorschlag der Kommission der Europäischen Union für eine Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik - EG-Statistikverordnung - (KOM(94) 78 endg.; Ratsdok. 5615/94 = BR-Drs. 283/94)

Entschließung vom 26./27. September 1994

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, daß die Europäische Union eine allgemeine Regelung für die Gemeinschaftsstatistik trifft, weisen allerdings daraufhin, daß die datenschutzrechtliche Entwicklung bei der Europäischen Union mit dem Aufbau der europäischen Statistik keineswegs Schritt gehalten hat.

Sie stellen mit Besorgnis fest, daß der vorliegende Vorschlag einer EG-Statistikverordnung die nationalen datenschutzrechtlichen Grundsätze und wesentliche Standards des Statistikrechts weitgehend nicht berücksichtigt. Sie fordern daher zur Wahrung des Rechts der Betroffenen auf informationelle Selbstbestimmung mit Nachdruck, daß die Bundesregierung ihre Bedenken gegen diesen Vorschlag geltend macht und diese bei den Beratungen auf europäischer Ebene zum Tragen bringt.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen ausdrücklich den Beschluß des Deutschen Bundesrates vom 8. Juli 1994 (BR-Drs. 283/94 - Beschluß -).

Gegen den vorgelegten Vorschlag einer **Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik** (EG-Statistikverordnung) erheben sie insbesondere die folgenden datenschutzrechtlichen Bedenken:

1. In Art. 1 sollte als die zuständige Gemeinschaftsdienststelle unmißverständlich das Statistische Amt der Europäischen Gemeinschaften (EUROSTAT) bestimmt werden, weil die erforderlichen rechtlichen, administrativen, technischen und organisatorischen Maßnahmen - insbesondere zur Sicherung der Zweckbindung der zu statistischen Zwecken erhobenen Daten sowie zur Wahrung der statistischen Geheimhaltung - bei dieser Stelle bereits aufgrund der EG-Übermittlungsverordnung 1588/90 vom 11. Juni 1990 getroffen werden können. Eine jederzeit revidierbare Organisationsentscheidung der Kommission darüber, welche Dienststelle der Europäischen Union für statistische Aufgaben zuständig ist, birgt dagegen die Gefahr, daß Daten an unterschiedliche Stellen der Kommission zu unterschiedlichen Zwecken übermittelt werden.

   Zugleich sollte EUROSTAT zumindestens einen der Selbständigkeit der Statistischen Ämter in der Bundesrepublik Deutschland vergleichbaren organisationsrechtlichen Status erhalten, der die unter dem Gesichtspunkt der Objektivität und Neutralität gebotenen Eigenständigkeit bei der Aufgabenerfüllung garantiert. Dies könnte anläßlich der für 1996 vorgesehenen Revision des Vertrages über die Europäische Union geschehen.

2. Das mehrjährige statistische Programm sollte nicht wie in Art. 3 vorgesehen von der Kommission beschlossen werden. Die grundlegenden Entscheidungen über die Bürger belastende Datenerhebungen sollten dem Rat mit Zustimmung des Europäischen Parlaments vorbehalten bleiben. Dabei sollte der Planungscharakter des Programms in den Vordergrund gestellt werden.

3. Art. 5 sollte festlegen, daß statistische Einzelmaßnahmen durch einen Rechtsakt gemäß dem Verfahren nach Art. 189 b EG-Vertrag angeordnet werden. Dies gilt auch für die statistische Auswertung von Daten, die bei den administrativen Stellen bereits vorliegen (sog. Sekundärstatistik). Die im Vorschlag vorgesehene generelle Befugnis der Kommission, statistische Einzelmaßnahmen zu regeln, ist viel zu weitgehend.

4. Die in Art. 12 vorgesehene Übertragung der Befugnis zur Organisation der Verbreitung der statistischen Daten auf die Kommission widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag, aus dem folgt, daß grundsätzlich die Mitgliedstaaten nach ihrem nationalen Recht zur Verbreitung der statistischen Daten zuständig sind. Ferner sollte in Art. 12 festgelegt werden, daß an Stellen außerhalb der statistischen Gemeinschaftsdienststelle nur nicht-vertrauliche statistische Daten übermittelt werden dürfen.

5. Der in Art. 13 gegenüber der Definition in der EG-Übermittlungsverordnung 1588/90 neu definierte Begriff "statistische Geheimhaltung" muß präzisiert werden. Dazu gehört insbesondere, daß festgelegt wird, unter welchen Voraussetzungen statistische Daten vertraulich sind und nicht nur als vertraulich gelten. Dies gilt um so mehr, als im Verordnungsvorschlag dieser Begriff nicht nur in Art. 13, sondern auch in Art. 9 Abs. 2 - allerdings mit einem anderen Begriffsinhalt - definiert wird. Der Begriff "statistische Geheimhaltung" sollte an einer Stelle in der Verordnung und so definiert werden, daß er Art. 2 Nr. 1 der EG-Übermittlungsverordnung 1588/90 und damit den derzeit geltenden nationalen Begriffsbestimmungen entspricht. Dies stände auch im Einklang mit dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag.

6. Gemäß dem Grundsatz der Subsidiarität sollte - ebenso wie die Befugnis zur Verbreitung statistischer Ergebnisse (Art. 11 Abs. 1) - auch die Festlegung der Zuständigkeit für die Durchführung der statistischen Einzelmaßnahmen (Art. 7) den Mitgliedstaaten überlassen bleiben.

7. Auch die in Art. 16 vorgesehene generelle Zugangsregelung einzelstaatlicher Stellen und der Gemeinschaftsdienststelle zu Registern der Verwaltung widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag. Dieser gebietet hier, daß - jedenfalls grundsätzlich - die Mitgliedstaaten zu bestimmen haben, in welcher Weise sich die für die Erstellung der Gemeinschaftsstatistiken zuständigen nationalen Stellen Daten beschaffen. Damit ist aber nicht zu vereinbaren, daß auch Stellen der Kommission unmittelbar Zugang zu nationalen Verwaltungsregistern haben sollen.

   Ferner bleibt unklar, ob die nach Art. 16 erhobenen Daten Erhebungs- oder Hilfsmerkmale sein sollen. Im übrigen darf über Art. 16 ein Zugang zu solchen personenbezogenen Daten, die nach nationalem Recht einer besonderen Geheimhaltung, z.B. dem Steuer- oder auch dem Sozialgeheimnis unterliegen, nicht eröffnet werden.

8. Die Regelung des Art. 17 ist mißglückt. Allem Anschein nach soll hier eine weitgehende Ausnahmeregelung von der statistischen Geheimhaltung zugunsten von Forschungsinstituten, einzelner Forscher und von für die Erstellung von Nicht-Gemeinschaftsstatistiken zuständigen Stellen vorgesehen werden, die die Möglichkeit eröffnet, die in diesem Bereich geltenden strengeren nationalen Regelungen zu umgehen. Außerdem würde von der für EUROSTAT geltenden EG-Übermittlungsverordnung 1588/90 abgewichen werden. Art. 17 sollte deshalb so gefaßt werden, daß die nationalen Zugangsregelungen für Einrichtungen mit der Aufgabe der unabhängigen wissenschaftlichen Forschung nicht umgangen werden können.

9. Der Vorschlag der Kommission sieht weder eine alsbaldige Trennung und Aufbewahrung von Erhebungs- und Hilfsmerkmalen noch eine alsbaldige Löschung personenbezogener Hilfsmerkmale vor. In der Bundesrepublik Deutschland dagegen gehören entsprechende Regelungen (vgl. § 12 BStatG) zum Kernbereich des Statistikrechts. Im Volkszählungsurteil hat das Bundesverfassungsgericht ihnen grundrechtssichernde Bedeutung beigemessen.

10. Schließlich fehlt es für die Organe der Europäischen Union noch immer an einer unabhängigen und effektiven Datenschutzkontrollinstanz, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der Europäischen Union in seinen Rechten verletzt zu sein.

20.7. Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen

Entschließung vom 26./27. September 1994

Angesichts der aktuellen Diskussion über die innere Sicherheit weisen die Datenschutzbeauftragten des Bundes und der Länder darauf hin, daß umfangreiche polizeiliche Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten, insbesondere im technischen Bereich, gesetzlich verankert worden sind.

Zum Kreis der Betroffenen zählen dabei nicht nur Personen, gegen die Verdachtsgründe vorliegen, sondern auch nichtverdächtige Kontakt- und Begleitpersonen und Unbeteiligte, deren Schutz nach Auffassung der Datenschutzbeauftragten besonders wichtig ist.

Vor diesem Hintergrund schlagen die Datenschutzbeauftragten vor, den derzeitigen Erkenntnisstand über die Erforderlichkeit polizeilicher Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten sowie ihre Auswirkungen auf die Rechte der Betroffenen durch folgende Maßnahmen zu verbessern:

1. Die Datenschutzbeauftragten teilen die von einigen Innenministern vertretene Auffassung, daß bloße Angaben über Einsatzzahlen der besonderen Befugnisse zur Datenerhebung nur einen begrenzten Aussagewert haben. Aufschluß über die tatsächliche Praxis, ihre Erforderlichkeit und Verhältnismäßigkeit läßt sich nur durch Überprüfung und Auswertung der einzelnen Einsätze gewinnen. Hierzu müssen unter Beteiligung der Datenschutzbeauftragten und der Wissenschaft, insbesondere der Kriminologie und des Polizeirechts, objektive und nachprüfbare Auswertungskriterien entwickelt werden.

   Die Datenschutzbeauftragten begrüßen daher die Initiative für eine sog. Rechtstatsachensammlung, die Erhebungen zu polizeilichen Ermittlungsmethoden und Eingriffsbefugnissen durchführen soll. Sie schlagen vor, in diese Rechtstatsachensammlung insbesondere Angaben über den Anlaß einer Datenerhebung mit besonderen Mitteln, die Örtlichkeit und die Dauer der Maßnahme, den Umfang der überwachten Gespräche, den betroffenen Personenkreis sowie die Anzahl der ermittelten, verurteilten, aber auch der entlasteten Personen einzubeziehen. Derartige Aufstellungen wären nicht nur für elektronische Überwachungsmethoden, sondern auch für Observationen, den Einsatz verdeckter Ermittler und V-Personen sowie für Rasterfahndungen denkbar.

2. Einige Polizeigesetze verpflichten dazu, zu überprüfen, ob es notwendig ist, bestehende Dateien weiterzuführen oder zu ändern. Dabei soll nicht nur darauf eingegangen werden, ob die Anwendungen, d. h. die Dateien, weiterhin erforderlich sind, sondern auch auf ihren Nutzen sowie auf ihre Schwachstellen und Mängel. Ferner sind Vorschläge zu machen, wie festgestellte Defizite beseitigt oder minimiert werden können.

3. Die Datenschutzbeauftragten gehen davon aus, daß sie bei den Überlegungen zur Rechtstatsachensammlung rechtzeitig beteiligt und die jeweiligen Materialien und Zwischenergebnisse mit ihnen erörtert werden.

20.8. Fehlende bereichsspezifische gesetzliche Regelungen bei der Justiz

Entschließung vom 26./27. September 1994

Obwohl seit dem Volkszählungsurteil des Bundesverfassungsgerichts mehr als 10 Jahre vergangen sind, werden im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet. Stattdessen sind in den letzten Jahren in zunehmendem Maße automatisierte Verfahren neu eingesetzt worden. Die Eingriffe in das Recht auf informationelle Selbstbestimmung stützen die Justizverwaltungen auf die Rechtsprechung des Bundesverfassungsgerichts zum sog. Übergangsbonus.

Die Datenschutzbeauftragten des Bundes und der Länder weisen im Hinblick auf die kommende Legislaturperiode den Bundesgesetzgeber erneut darauf hin, daß gesetzliche Regelungen im Bereich der Justiz überfällig sind. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Der zur Zeit dem Bundesrat vorliegende Entwurf eines Strafverfahrensänderungsgesetzes beispielsweise wird datenschutzrechtlichen Anforderungen in keiner Weise gerecht.

Im Bereich der Justiz fehlen ausreichende gesetzliche Regelungen für die

- Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien,
- Datenerhebung, -verarbeitung und -nutzung im Strafvollzug,
- Übermittlung von Daten aus den bei Gerichten geführten Registern (z.B. Grundbuch) und deren Nutzung durch die Empfänger,
- Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen (Justizmitteilungsgesetz)
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien.

Eine Berufung auf den sog. Übergangsbonus auf unbegrenzte Zeit steht nicht in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts. Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe in der neuen Legislaturperiode unverzüglich bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes des Bürgers entgegenwirken.

20.9. Datenschutzrechtliche Anforderungen an ein Übereinkommen der Mitgliedstaaten der Europäischen Union über die Errichtung eines europäischen Polizeiamtes (Europol)

Entschließung vom 26./27. September 1994

Die Datenschutzbeauftragten der Länder gehen gemeinsam mit dem Bundesdatenschutzbeauftragten davon aus, daß bei den Verhandlungen mindestens folgende Punkte berücksichtigt werden:

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

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

20.10. Art. 12 Verbrechensbekämpfungsgesetz zur Trennung von Polizei und Nachrichtendiensten

Entschließung vom 26./27. September 1994

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

- Der BND erhält danach bei der Fernmeldeaufklärung auch Befugnisse, die auf eine gezielte Erhebung von Daten für polizeiliche Zwecke hinauslaufen können. Deshalb ist bei dem Vollzug des Gesetzes darauf zu achten, daß nicht gezielt Informationen gesammelt werden, die vom Auftrag des BND nicht umfaßt werden.
- Zwischen nachrichtendienstlichen Vorfelderkenntnissen und polizeilichen Zwangsmaßnahmen ist ein Filter erforderlich, der vor allem Unbeteiligte vor überzogenen Belastungen schützt.

Die Datenschutzbeauftragten fordern, für die Zusammenarbeit von Nachrichtendiensten und Polizei in der Durchführung und Gesetzgebung das Trennungsgebot strikt zu beachten. Dies gilt auch bei der Fernmeldeaufklärung des BND. Eine wirksame Kontrolle durch den Datenschutzbeauftragten in diesem sensiblen Bereich ist auch nach der Rechtsprechung des Bundesverfassungsgerichts sicherzustellen.

20.11. Geänderter Vorschlag für eine Europäische Richtlinie zum Datenschutz im ISDN und in Mobilfunknetzen vom 13. Juni 1994 (KOM (94) 128 endg. - COD 288)

Entschließung vom 26./27. September 1994

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, daß die Europäische Kommission mit der Vorlage des geänderten Vorschlags für eine Richtlinie zum Datenschutz im ISDN ihre Absicht bekräftigt hat, unionsweit bereichsspezifische Regelungen für den Datenschutz in Telekommunikationsnetzen zu schaffen. Es kann kein Zweifel daran bestehen, daß die digitalen Telekommunikationsnetze in der Europäischen Union zunehmend zur wichtigsten Infrastruktur für die Verarbeitung personenbezogener Daten werden. Der Regelungsdruck wird erhöht durch die Tatsache, daß die Europäische Union die rechtlichen und technischen Voraussetzungen für die Liberalisierung der Telekommunikationsmärkte in weiten Bereichen bereits geschaffen hat und mehrere Mitgliedsstaaten, darunter Deutschland, derzeit ihr nationales Telekommunikationsrecht auf die Vorgaben der EU umstellen.

Aus diesem Grund sollte der geänderte Vorschlag für eine ISDN-Richtlinie so bald wie möglich vom Ministerrat und vom Europäischen Parlament abschließend beraten werden. Die Bundesregierung sollte die deutsche Ratspräsidentschaft dazu nutzen, den geänderten Vorschlag für eine ISDN-Richtlinie im Rat behandeln zu lassen.

Dabei sollte sich die Bundesregierung insbesondere für folgende Verbesserungen des Richtlinienvorschlags aus datenschutzrechtlicher Sicht einsetzen:

1. Für Telekommunikationsorganisationen und Diensteanbieter müssen die gleichen gemeinschaftsrechtlichen Regelungen zum Datenschutz gelten. Die Verarbeitung personenbezogener Daten durch Diensteanbieter darf nicht privilegiert werden.
2. Die Beschränkung der Datenverarbeitung auf Zwecke der Telekommunikation sollte wieder in die Richtlinie aufgenommen werden. Der allgemeine Zweckbindungsgrundsatz der Datenschutzrichtlinie läßt die Zweckentfremdung schon bei "berechtigten Interessen" der Verarbeiter zu. Das ist angesichts zunehmender Di-

versifizierung der Aktivitäten von Netzbetreibern und Diensteanbietern eine zu weitgehende Lockerung der Zweckbindung im Telekommunikationsbereich.

3. Das ursprünglich vorgesehene Verbot, personenbezogene Daten zur Erstellung von elektronischen Profilen der Teilnehmer zu nutzen, sollte wieder in die Richtlinie aufgenommen werden.

4. Die Speicherung von Inhaltsdaten nach Beendigung der Übertragung sollte - wie im ursprünglichen Richtlinienentwurf vorgesehen - untersagt werden.

5. Die Vertraulichkeit der Kommunikationsbeziehungen und -inhalte (Fernmeldegeheimnis) sollte - wie es der ursprüngliche Richtlinienvorschlag ebenfalls vorsah - auf Unionsebene garantiert werden.

6. Um eine Harmonisierung des Gemeinschaftsrechts beim Einzelgebührennachweis zu erreichen, sollten konkrete Vorgaben in die Richtlinie aufgenommen werden, z.B. in dem den angerufenen Teilnehmern die Aufnahme ihrer Rufnummer in Einzelgebührennachweise freigestellt wird.

7. Im Fall der Anrufweiterschaltung sollte die automatische Information des anrufenden Teilnehmers darüber, daß sein Anruf (z.B. bei einem Arzt) an einen Dritten weitergeschaltet wird, gewährleistet sein.

Die Konferenz begrüßt die im geänderten Vorschlag vorgesehene Kostenfreiheit für die verschiedenen Optionen der Anzeige der Rufnummer des Anrufers und für die Nichtaufnahme von Daten in das Teilnehmerverzeichnis (Telefonbuch).

Diese Vorschläge berücksichtigen das Subsidiaritätsprinzip und beschränken sich auf Änderungen, die zur Gewährleistung der Vertraulichkeit der Kommunikation in der Europäischen Union realisiert werden müssen. Zudem wird die Europäische Union insoweit im Rahmen ihrer ausschließlichen Zuständigkeit tätig. Die Konferenz bittet auch die Entscheidungsträger auf Unionsebene sowie die Datenschutzbehörden der anderen Mitgliedsstaaten, diese Anregungen zu unterstützen.