216 Seiten

Deutscher Bundestag
12. Wahlperiode

Drucksache 12/4805

27. 04. 93

Sachgebiet 204

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz

14. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 26 Abs. 1 des Bundesdatenschutzgesetzes — Berichtszeitraum Anfang 1991 bis Anfang 1993 —

Gliederung

		Seite
1	**Schutz und Risiken für Persönlichkeitsrecht und Privatsphäre**	10
1.1	Ausweitung des rechtlichen und tatsächlichen Instrumentariums zur Kontrolle und Überwachung	10
1.2	Zunehmende Erhebung, Verarbeitung und Nutzung personenbezogener Daten aufgrund von Entscheidungen der EG	12
1.3	Verschärfung der öffentlichen Diskussion über den Datenschutz insgesamt	13
1.4	Einführung des Datenschutzes als Schutz des Persönlichkeitsrechts und der Privatsphäre in den neuen Ländern	13
1.5	Eingaben von Bürgern	14
1.6	Besondere Erfolge und erfreuliche Feststellungen	14
1.7	Beratungen und Kontrollen, insbesondere Beanstandungen	15
1.8	Zusammenarbeit mit den Landesbeauftragten für den Datenschutz und anderen Stellen	16
1.9	APC-Programm zur automatisierten Registermeldung	17
2	**Datenschutz im Beitrittsgebiet**	18
2.1	Einigungsvertrag	18
2.2	Abwicklung des Zentralen Einwohnerregisters (ZER)	20
2.2.1	Die Personenkennzahl	20
2.3	Datenspeicher „Gesellschaftliches Arbeitsvermögen der DDR" jetzt im Bundesarchiv	21
2.4	Die Gesundheitsunterlagen aus der Urangewinnung SDAG Wismut — ein komplexes Datenschutzproblem —	21
2.5	Kaderakten der Nomenklatura nicht auffindbar — Personaldatenrechtliche Probleme aufgrund der Vereinigung —	23
2.6	Schutz von Sozialdaten — Probleme beim Umgang mit ihnen —	25
2.6.1	Übernommene Akten nicht ordnungsgemäß gesichert	25
2.6.2	Bundesanstalt für Arbeitsmedizin hat arbeitsmedizinische Daten übernommen	25
2.6.3	Wismut-Gesundheitsdaten für nachgehende Untersuchungen erfaßt	26
2.6.4	Datenübermittlung für Rentenüberleitung korrekt	26

Zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz — I — 111/16 — vom 27. April 1993 gemäß § 26 Abs. 1 des Bundesdatenschutzgesetzes.

		Seite
2.7	Statistisches Material der ehemaligen DDR auf Statistisches Bundesamt und Landesämter für Statistik aufgeteilt	27
2.8	Soldaten und Wehrpflichtige der ehemaligen NVA	27
2.8.1	Unzulässige Daten auf den Wehrstammkarten der ehemaligen NVA werden nun doch gelöscht	27
2.8.2	Unzulässige Daten auf Wehrstammkarten der ehemaligen NVA werden auch beim Bundesamt für den Zivildienst gelöscht	28
2.8.3	Unterlagen über ehemalige Bausoldaten noch nicht vollständig an das Bundesamt für den Zivildienst abgegeben	28
2.9	Das Sicherungsgesetz für das Nationale Krebsregister der ehemaligen DDR	29
2.10	Besondere Gefahren für das Fernmeldegeheimnis im Telefonnetz der neuen Bundesländer	29
2.11	Wohin mit Datenbeständen der ehemaligen DDR? — Bundesarchiv Potsdam —	30
2.12	Treuhandanstalt	31
3	**Deutscher Bundestag**	32
3.1	Welches Datenschutzrecht soll für den Deutschen Bundestag gelten?	32
3.2	Steht der Datenschutz dem Fragerecht von Abgeordneten entgegen?	33
4	**Innere Verwaltung und Auswärtiger Dienst**	33
4.1	Ausländerzentralregister weiter ohne ausreichende Rechtsgrundlage	33
4.2	Asylverfahren	35
4.3	Notwendige Verwaltungsvorschriften zum Ausländergesetz fehlen	36
4.4	Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR	36
4.4.1	Stasi-Unterlagen-Gesetz	36
4.4.2	Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR widmet Datenschutz große Aufmerksamkeit	38
4.5	Umgang mit brisanten Daten aus dem Geschäftsbereich des früheren Bundesministers für innerdeutsche Beziehungen und des ehemaligen Ministeriums des Innern der DDR	40
4.5.1	Unterlagen über Familienzusammenführung bleiben erhalten	40
4.5.2	Unterlagen in Häftlingsangelegenheiten	40
4.5.3	Sicherung der Daten von Strafgefangenen der ehemaligen DDR unbefriedigend	40
4.6	Nicht mehr benötigte Daten aus der Aufnahme von Übersiedlern vernichtet — Heimatortskartei Gießen —	41
4.7	54-seitiger Fragebogen wird mindestens halbiert — Aussiedleraufnahmeverfahren —	41
4.8	Suchdienst des Deutschen Roten Kreuzes	42
4.9	Darf ein Bundesministerium eine Eingabe stets an eine andere — zuständige — Behörde abgeben?	43
4.10	Auslandsvertretungen	44
4.10.1	Diskretionszonen eingerichtet	44
4.10.2	Unverschlüsselte Übermittlungen empfindlicher Informationen an und von Auslandsvertretungen sind riskant	44
5	**Rechtswesen**	45
5.1	Änderungen des Strafverfahrensrechts	45
5.1.1	Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG)	45
5.1.2	Gewinnaufspürungsgesetz	46
5.1.3	Lauschangriff	47
5.1.4	Strafverfahrensänderungsgesetz	48
5.1.5	Genomanalyse im Strafverfahren	49
5.1.6	Weitere Empfehlungen für den Persönlichkeitsschutz im Strafverfahren	50
5.2	Persönlichkeitsschutz im Rehabilitierungsverfahren — Erstes SED-Unrechtsbereinigungsgesetz —	50
5.3	Auch Funktionsträger der früheren DDR müssen amtlich bekanntgewordene Privatgeheimnisse wahren	51
5.4	Das jugendgerichtliche Verfahren ist datenschutzrechtlich besonders sensibel	51
5.5	Schutz des Persönlichkeitsrechts auch bei Strafgefangenen — Zum Strafvollzugsgesetz —	52
5.6	Mitteilungen aus gerichtlichen und staatsanwaltschaftlichen Verfahren an andere Stellen — Justizmitteilungsgesetz —	53
5.7	Auch im Konkursverfahren geht es nicht ohne Datenschutz	54

		Seite
6	**Finanzwesen**	54
6.1	Die Abgabenordnung braucht Datenschutzregelungen	54
6.1.1	Wann und in welchem Umfang dürfen Steuerdaten offenbart werden?	54
6.1.2	Einheitliches Datenschutzrecht im Steuerverfahren	54
6.2	Datenschutz im Zinsabschlaggesetz	55
6.3	Antragsteller nach Vermögensgesetz kann Offenbarung seiner Daten widersprechen	55
6.4	Zollverwaltungsgesetz datenschutzrechtlich noch mangelhaft — Zum Zollrechtsänderungsgesetz —	55
6.5	EG-weite Kontrolle über Warenlieferungen und -bewegungen	56
6.6	Erweiterte Amtshilfe unter den EG-Staaten im Bereich der Verbrauchsteuern	56
6.7	Europäische Zollunterstützungsabkommen	57
6.7.1	EG-Zollinformationssystem muß Datenschutz berücksichtigen	57
6.7.2	Kooperationsabkommen der EG mit Drittländern	57
6.7.3	Bilaterale Verträge mit datenschutzrechtlichen Mängeln	57
6.8	EG-Kommission erhält automatisiert Daten über EG-Agrarausgaben	57
6.9	Abschriften von Urkunden an Finanzbehörden	58
6.10	Kontrollmitteilungen an Finanzbehörden müssen neu geregelt werden	58
6.11	Keine Pflicht zu Meldungen für die Betriebskartei der Hauptzollämter	58
7	**Wirtschaft**	58
7.1	Bundesausfuhramt und Änderung des Außenwirtschaftsgesetzes	58
7.2	Personenbezogene Daten eines Wirtschaftsprüfers trotz Widerspruchs veröffentlicht	59
7.3	Datenschutzgerechte Änderung gewerberechtlicher Vorschriften vorgesehen	59
7.4	Umgang mit personenbezogenen Daten von Handwerkern — Zur Handwerksordnung —	59
7.5	Unzulässige Datenspeicherung beim Bundesaufsichtsamt für das Versicherungswesen geändert	60
8	**Landwirtschaft**	60
8.1	Kommt der gläserne Landwirt? — Die neue Struktur der Agrarförderung —	60
8.2	Prüfungsteilnehmer muß Betriebsdaten seines Ausbilders nicht offenbaren	61
9	**Personaldaten**	61
9.1	Schutz von Arbeitnehmerdaten endlich gesetzlich regeln	61
9.2	Verbesserung des Personalaktenrechts der Beamten, Soldaten und Zivildienstleistenden	62
9.3	Beihilfedaten sind besonders sensibel	62
9.3.1	Abschottung der Beihilfestelle — immer wieder problematisch	62
9.3.2	Trennung von Beihilfestellen und Personalverwaltung trotz Einwilligung des Bediensteten erforderlich	63
9.3.3	Beihilfeverfahren im Widerspruchsfall jetzt datenschutzgerecht geregelt	63
9.3.4	Hochsensible Diagnosedaten dürfen nicht in den normalen Geschäftsgang	64
9.4	Zugriff der Personalvertretung auf Teile der Personaldatei der Dienststelle	64
9.5	Telefondatenverarbeitung	64
9.5.1	Dienstanschlußvorschriften endlich erlassen	64
9.5.2	Physikalisch-Technische Bundesanstalt beseitigte Mängel	66
9.6	Der künftige Dienstherr/Arbeitgeber darf nicht alles und jedes fragen	66
9.7	Angefochtene Beurteilungen dürfen in Personalakten nur mit Vorbehalt gespeichert werden	68
9.8	Personalnebenakten viel zu umfangreich	69
9.9	Anonyme Hinweise an den Dienstherrn	69
9.10	Vorsicht bei der Durchführung von Verfahren zur Personalauswahl und Personalförderung, besonders wenn Privatfirmen mitwirken	69
9.11	Was darf dem Konkurrenten um eine Stelle im öffentlichen Dienst im gerichtlichen Verfahren über andere Bedienstete mitgeteilt werden?	70
9.12	Disziplinarunterlagen Unbefugten zugänglich gemacht	71
9.13	Defizite beim Sozialdienst einer obersten Bundesbehörde	72
9.14	Umgang mit ärztlichen Unterlagen	73

		Seite
9.14.1	Im wesentlichen korrekte Handhabung bei der Physikalisch-Technischen Bundesanstalt	73
9.14.2	Ärztliche Begutachtung ohne Wissen des Bediensteten	73
9.14.3	Anforderung ärztlicher Unterlagen über einen Beamten nur mit dessen Kenntnis	74
9.14.4	Deutsche Bundesbank zur besseren Wahrung des Patientengeheimnisses veranlaßt	74
10	**Sozialwesen — Allgemeines**	75
10.1	Der Datenschutz im Sozialgesetzbuch wird neu geregelt	75
10.2	Grundsatz der Ersterhebung beim Betroffenen verletzt	77
10.3	Rechte Betroffener auf Einsicht in ärztliche Unterlagen durchgesetzt	78
10.3.1	Bundesversicherungsanstalt für Angestellte (BfA) wollte nur über Hausarzt Einsicht gewähren	78
10.3.2	Ersatzkasse gewährt nach Diskussion Akteneinsicht	78
10.4	Datenoffenbarung im Sozialgerichtsverfahren	78
10.4.1	Unaufgeforderte Weitergabe eines Bescheides einer Landesversicherungsanstalt	78
10.4.2	Darf stets die gesamte Versicherungsakte dem Sozialgericht zugeleitet werden?	79
10.4.3	Dürfen Gesundheitsdaten im Sozialgerichtsverfahren in öffentlicher Sitzung bekanntgegeben werden?	79
10.5	Datenoffenbarung nach § 69 SGB X	80
10.5.1	Weitergabe von Sozialdaten an die Staatsanwaltschaft	80
10.5.2	Weitergabe von Sozialdaten an Versicherte	80
10.6	Muß ein Leistungsträger den Informanten über einen angeblichen Leistungsmißbrauch benennen?	81
10.7	Zweckbindung übermittelter Sozialdaten nicht beachtet	81
10.8	Erfüllt der Sozialversicherungsausweis seinen Zweck?	82
10.9	Drei Sozialversicherungsträger wollen eine gemeinsame Datei — Zum Agrarsozialreformgesetz 1994 —	82
11	**Arbeitsverwaltung**	83
11.1	Schärfere Kontrolle von Leistungsbeziehern der Bundesanstalt für Arbeit	83
11.2	Computerviren in automatisierten Dateien der Arbeitsverwaltung im Beitrittsgebiet	84
11.3	Verdeckte Kennzeichnung als Alkoholiker beseitigt — Computerunterstützte Arbeitsvermittlung („coArb") —	85
11.4	Pflicht zur Offenbarung von Einkommensdaten Unterhaltsverpflichteter deutlich eingeschränkt	86
11.5	Ärztlicher Dienst der Bundesanstalt für Arbeit	86
11.5.1	Ärztliche Untersuchung und Begutachtung gegen den Willen eines Arbeitssuchenden	86
11.5.2	Besserer Umgang mit ärztlichen Gutachten	87
11.6	Maßnahmeträger diskriminiert Arbeitslose im Zusammenhang mit deren Umschulung und Fortbildung	88
11.7	Bewerberdaten können ins Ausland gehen — SEDOC-Verfahren der Bundesanstalt für Arbeit —	88
12	**Krankenversicherung**	89
12.1	Der gläserne Patient kommt nicht — Gesundheitsstrukturgesetz —	89
12.2	Dürfen Krankenkassen der Bundesanstalt für Arbeit und der Zollverwaltung Mitgliederbestandslisten überlassen?	91
12.3	Krankenkasse beschaffte sich bei Betriebsprüfung Arbeitnehmerdaten für Werbezwecke	91
12.4	Krankenversichertenkarte als Chipkarte	92
12.5	Patientendaten auf Müllkippe — Kontrolle eines Knappschaftskrankenhauses —	93
12.6	Ein Spitzenverband der Krankenkassen beanstandet	94
13	**Rentenversicherung**	94
13.1	Die Dateien der Datenstelle des Verbandes Deutscher Rentenversicherungsträger (VDR) sind kein zentrales Auskunftsregister	94
13.2	Datenabgleich zur Aufdeckung unberechtigter Versorgungsbezüge	95
13.3	Kontrolle bei der Bundesversicherungsanstalt für Angestellte (BfA)	96

		Seite
13.3.1	Ärztliche Unterlagen trotz Widerspruchs des Versicherten weitergegeben	97
13.3.2	Abtretungsgläubigern darf keine Kenntnis von nachrangigen Gläubigern eines Rentenempfängers gegeben werden	97
13.3.3	Nach der „letzten Regel" wird nicht mehr gefragt	97
14	**Unfallversicherung**	97
14.1	Voraussetzungen für eine wirksame Einwilligung von Versicherten der gesetzlichen Unfallversicherung bei Erhebung, Verarbeitung und Nutzung ihrer Daten	97
14.2	Teilweise Verbesserung des Datenschutzes bei der Berufsgenossenschaft der chemischen Industrie	98
14.3	Ansprechpartner für Datenschutz in räumlich getrennten Organisationseinheiten von Berufsgenossenschaften	99
14.4	Kein Einsichtsrecht des Arbeitgebers in die Unfallakte seines Arbeitnehmers bei der Berufsgenossenschaft	100
15	**Verteidigung**	100
15.1	Besserer Schutz für Personalakten der Soldaten	100
15.2	Besserer Schutz, aber auch Probleme beim Umgang mit Personalakten von Wehrpflichtigen und Zivildienstpflichtigen	101
16	**Zivildienst**	101
16.1	Regelungen über Umgang mit Personalakten der Zivildienstpflichtigen und Zivildienstleistenden verbessert	101
16.2	Akten von Kriegsdienstverweigerern	102
16.2.1	Bundesamt für den Zivildienst zeigt erfreuliche Praxis bei Vernichtung von Akten aus laufenden Verfahren	102
16.2.2	Bundesamt für den Zivildienst konnte Frist für Vernichtung von Unterlagen aus Verfahren vor 1989 nicht einhalten	102
17	**Gesundheitswesen**	103
17.1	Bundeskrebsregistergesetz	103
17.2	Genomanalyse	104
18	**Verkehrswesen**	105
18.1	Offenbarung von Verfahrensbeteiligten im Gesetzgebungsverfahren abgestellt (Stendal-Umfahrung)	105
18.2	Nur wenige Probleme mit dem Konzept von ZEVIS — Der ZEVIS-Bericht der Bundesregierung —	106
18.3	Fragen aus der ZEVIS-Praxis	106
18.3.1	Zentrale Fragen des ZEVIS-Betriebes	106
18.3.2	Die Nutzung von Funkterminals	107
18.3.3	ZEVIS-Nutzung durch das Bundeskriminalamt	107
18.3.4	ZEVIS-Nutzung durch den Bundesgrenzschutz	107
18.4	Kraftfahrt-Bundesamt	107
18.4.1	Dieselbe Fahrzeug-Identifizierungsnummer bei mehreren Kraftfahrzeugen	107
18.4.2	Übermittlung von Halterdaten an die Automobilindustrie für umweltfördernde Maßnahmen	108
18.5	Muß der Geburtstag im Fahrzeugschein stehen? — Eintragungen in Fahrzeugpapieren —	108
18.6	Rechtsgrundlage für Datei über Ordnungswidrigkeiten im Güterkraftverkehr	108
18.7	Verkehrszentralregister	109
18.7.1	Erteilung von Auskünften bei Zweifeln an der Personenidentität	109
18.7.2	Gebührenfreiheit für Auskünfte nach dem Bundesdatenschutzgesetz wird mißachtet	109
18.8	Brauchen wir eine zentrale Führerscheindatei?	109
18.9	Datenübermittlung durch Luftfahrt-Bundesamt führte zu Verlust einer ausländischen Fluglizenz	110
18.10	Defizite im Luftverkehrsrecht	110
18.10.1	Luftverkehrsgesetz — Überprüfung des Luftfahrtpersonals —	111
18.10.2	Gesetzliche Regelung der Datenerfassung über Luftfahrer fehlt weiter	111
18.10.3	Veröffentlichung von Daten aus der Luftfahrzeugrolle	111
18.10.4	Hauptflugbuch	111
18.10.5	Flugunfalluntersuchung	111
18.11	Schiffahrt	112

		Seite
18.11.1	Lange Speicherung über Ordnungswidrigkeitsverfahren — Kontrolle der Wasser- und Schiffahrtsdirektion Südwest —	112
18.11.2	Meldesystem Gefahrguttransporte	112
19	**Umweltschutz**	113
19.1	Umweltinformationssysteme	113
19.2	Umweltinformationsgesetz	113
20	**Deutsche Bundespost — Gute Entwicklung des Datenschutzes bei Postdienst und Postbank —**	114
20.1	Postdienst	114
20.1.1	Nachsendungsanträge garantieren nicht die Geheimhaltung der neuen Anschrift	114
20.1.2	Fehlerhafte Postzustellungen	115
20.1.3	Auskunft über die Anschrift des Postfachinhabers	115
20.2	Postbank	116
20.2.1	Die Zusammenarbeit mit der Schufa	116
20.2.2	Bankeinzugsverfahren	116
20.2.3	Die Kontonummer muß nicht in der Anschrift auf dem Kontoauszugsbrief stehen	117
21	**Telekommunikation**	117
21.1	Regelung über Fangschaltung und Einsatz von Zählvergleichseinrichtungen in TDSV verfassungswidrig	117
21.2	Telekom konnte Datenschutzverordnung nur teilweise in die Praxis umsetzen	118
21.2.1	Wahlrecht der Telekom-Kunden für die Verbindungsdatenspeicherung nicht realisiert	118
21.2.2	Probleme beim Einzelverbindungsnachweis und bei Anrufen z. B. bei der Telefonseelsorge	118
21.3	Nicht nur die Telekom gibt Telefonbücher heraus	119
21.4	Kundendaten der Telekom können zu Werbezwecken verwendet werden	120
21.5	Unzutreffende Information der Telekom-Kunden abgestellt	120
21.6	Wer sich über die Telefonrechnung beschwerte, wurde heimlich mit einer Zählvergleichseinrichtung kontrolliert	120
21.7	Risiko zu langer Überwachung des Fernmeldeverkehrs nach der Strafprozeßordnung	121
21.8	Auch bei Textverarbeitung auf Personalcomputern muß Datenschutz gewährleistet sein	122
21.9	Bekanntgabe von Telefonschulden an den Ehemann und die Großmutter der Schuldner	122
21.10	Abhören von Funksendungen durch Unbefugte erleichtert	123
21.11	Auch große behördeninterne Kommunikationsanlagen erzeugen datenschutzrechtliche Risiken	123
21.12	Telefonate wurden auf Antrag des Nachbarn registriert	125
22	**Wissenschaft und Forschung — Forschungsvorhaben „Anonymisierung" —**	125
23	**Statistik**	126
23.1	Europäische Gemeinschaft aktiviert ihre Statistik	126
23.1.1	Statistikgeheimnis durch Entwurf einer EG-Unternehmensregisterverordnung gefährdet	126
23.2	Rechtslücke geschlossen — Schutz von Statistikdaten auch bei EG —	127
23.3	Zwangsweise Erhebung von Geburtsgewicht und Körperlänge der Neugeborenen — Zum Bevölkerungsstatistikgesetz —	127
23.4	Haushaltsmitglieder müssen monatliches Nettoeinkommen angeben — Zum Wohnungsstatistikgesetz —	128
23.5	Umweltstatistik wird geregelt	128
23.6	Strafverfolgungsstatistik noch immer ohne Rechtsgrundlage	129
23.7	Einsatz von Laptops und fernmündliche Datenerhebung bei der Durchführung von Statistiken	129
24	**Bundeskriminalamt**	129
24.1	Gesetzgebungsstand	129
24.1.1	Neues BKA-Gesetz fehlt immer noch	129
24.1.2	Das Schengener Durchführungsübereinkommen bedarf der Ergänzung durch nationale Regelungen	130
24.2	Polizeiliche Datenverarbeitung in Europa	130
24.2.1	Europäisches Informationssystem — EIS —	130
24.2.2	Polizeiliche Datenspeicherung europaweit — EUROPOL, das Zentrale Europäische Kriminalpolizeiamt, kommt —	130

		Seite
24.2.3	Polizeiliche Zusammenarbeit mit Staaten in Osteuropa	131
24.3	Viel leistungsfähigeres Fingerabdruckidentifizierungssystem AFIS eingerichtet	132
24.4	INPOL Sachfahndung — Übermittlung von Kfz-Sachfahndungsdaten an den HUK-Verband und an Kfz-Hersteller grundsätzlich zulässig —	132
24.5	Neue Dateien — Geplante Datei „Gewalttäter Sport" (Hooligandatei) —	133
24.6	Der Umgang mit Daten aus der Überwachung des Fernmeldeverkehrs muß präziser geregelt werden	133
24.7	Aussonderungsprüffristen und Löschung gespeicherter Daten	133
24.8	Zur Speicherungspraxis des Bundeskriminalamtes	134
24.8.1	Das Bundeskriminalamt prüft die Löschungsmöglichkeit von Datenspeicherungen zu spät — Kontrolle beim Referat TB 22 des Bundeskriminalamtes —	134
24.8.2	Speicherungen in APIS besser — aber noch nicht problemlos	135
24.8.3	Speicherung von „Palästinenser-Daten" in APIS	137
24.9	Unschuldiger aufgrund fehlerhafter Datenspeicherung des BKA bei der Grenzkontrolle „auseinandergenommen"	137
25	**Bundesgrenzschutz**	137
25.1	Dienstanweisung Amtshilfe/Grenze	137
25.2	Arbeitnehmer verliert Arbeitsplatz durch zweifelhafte Sicherheitsüberprüfung	138
25.3	Kommen automatisierte Personenkontrollen an den Grenzen?	138
26	**Zoll- und Außenwirtschaftskontrolle**	139
26.1	Telefonüberwachung bei Außenwirtschaftskontrolle eingeführt	139
26.2	Zollkriminalamt als Bundesoberbehörde geschaffen — aber ohne bereichsspezifischen Datenschutz	140
26.3	Gemeinsames Zollinformationssystem der EG-Mitgliedstaaten — CIS (Customs Information System) — kommt	140
26.4	Übermittlungsersuchen von Nachrichtendiensten an das Zollkriminalamt nicht präzise genug	141
27	**Verfassungsschutz**	141
27.1	Die Sicherheitsüberprüfung ist gesetzlich zu regeln	141
27.2	Das Bundesamt für Verfassungsschutz offenbarte Privatpersonen Erkenntnisse über Dritte	143
27.3	Auskünfte an den Betroffenen zu restriktiv	144
27.4	Das Bundesamt für die Anerkennung ausländischer Flüchtlinge darf nicht alle Daten aus Asylverfahren an Nachrichtendienste übermitteln	145
27.5	Bundesamt für Verfassungsschutz behindert datenschutzrechtliche Kontrolle	145
27.6	Gesperrte NADIS-PZD-Daten dürfen nicht rechtswidrig genutzt werden	146
28	**Bundesnachrichtendienst**	146
28.1	Bundesnachrichtendienst überprüft Altdatenbestände	146
28.2	Schwierigkeiten bei datenschutzrechtlicher Kontrolle	147
29	**Militärischer Abschirmdienst — Altdatenbereinigung braucht sehr viel Zeit —**	147
30	**Datensicherung**	147
30.1	Der Sachverstand von Fachleuten wird genutzt — Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik —	147
30.2	Gestaltung und Verwendung von Paßwörtern will gelernt sein	148
30.3	Kryptographische Verschlüsselung vielfach dringend zu empfehlen	149
30.4	Vorsicht bei Protokolldateien	149
30.5	Datennetze können außer Kontrolle geraten — Sicherheit von Datennetzen —	150
30.6	Beauftragter für die Sicherheit in der Informationstechnik (IT-Sicherheitsbeauftragter) mit nur schwer zu vereinbarenden Funktionen	151
30.7	Private Arbeitsplatzcomputer entfernt — APC-Einsatz bei der Deutschen Bundesbahn —	151
30.8	Automatisierte Abrufverfahren bedürfen besonderer Sicherheitsvorkehrungen	152

		Seite
30.9	Zugangssicherung sollte nach Wartungsarbeiten überprüft werden	152
31	**Entwicklung des allgemeinen Datenschutzrechts**	152
31.1	Erste Erfahrungen mit dem neuen BDSG	152
31.2	Datenschutz im Grundgesetz	154
31.3	Neues BDSG und Kirchen	155
32	**Nicht-öffentlicher Bereich**	155
32.1	Neues Bundesdatenschutzgesetz	155
32.2	Weitergabe von Patientendaten an Verrechnungsstellen nur mit Einwilligung	156
32.3	Fortschritte bei den Schweigepflichtentbindungsklauseln, aber immer noch Unbehagen	156
32.4	Datenschutz ist auch bei electronic-cash erforderlich	157
32.5	Datenübermittlung im Rahmen von Allfinanzkonzepten nur mit Einwilligung	157
33	**Ausland und Internationales**	157
33.1	Entwicklung des Datenschutzes im Ausland	158
33.2	Internationale Zusammenarbeit der Datenschutzkontrollinstanzen	158
33.3	Europarat	158
33.4	Europäische Informationssysteme	159
33.5	EG-Datenschutzrichtlinie	159
33.6	Informationstätigkeit	160
34	**Aus zurückliegenden Tätigkeitsberichten — Bilanz —**	160

Anlage 1 (zu 4.1 u. a.)

Beschlußempfehlung und Bericht des Innenausschusses des Deutschen Bundestages zum 10. bis 13. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz ... 163

Anlage 2 (zu 1.8, 5.1.1)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. Juni 1991 — gegen die Stimme Bayerns — zum Bundesratsentwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität ... 179

Anlage 3 (zu 1.8, 9.2)

Entschließung der 42. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1991 zum Datenschutz im Recht des öffentlichen Dienstes ... 180

Anlage 4 (zu 1.8, 9.1)

Entschließung der 43. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. März 1992 zum Arbeitnehmerdatenschutz ... 182

Anlage 5 (zu 1.8, 4.2)

Entschließung der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. April 1992 — gegen die Stimme Bayerns in Abwesenheit Sachsens — zur Neuregelung des Asylverfahrens (BT-Drucksache 12/2062) ... 184

Anlage 6 (zu 1.8, 31.2)

Entschließung der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. April 1992 — gegen die Stimme Bayerns — zum Grundrecht auf Datenschutz ... 185

Anlage 7 (zu 1.8, 21.11)

Entschließung der 44. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Datenschutz bei internen Telekommunikationsanlagen ... 186

Anlage 8 (zu 1.8, 12.1)

Entschließung der 44. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Entwurf eines Gesetzes zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung — Gesundheits-Strukturgesetz 1993 (BR-Drucksache 560/92) ... 187

Anlage 9 (zu 1.8, 12.4)

Entschließung der 44. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zur Krankenversichertenkarte als Chipkarte ... 188

Anlage 10 (zu 1.8, 5.1.3)

Entschließung der 44. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 — gegen die Stimme Bayerns — zum „Lauschangriff" ... 189

Seite

Anlage 11 (zu 1.8, 19.2)
Entschließung der 45. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. Februar 1993 zur Richtlinie des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt (30/313/EWG) 190

Anlage 12 (zu 21.5)
Merkblatt der DBP Telekom:
Hinweise zum Datenschutz für unsere Telefonkunden 191

Anlage 13 (zu 30.2)
Empfehlungen zur Paßwortgestaltung und zum Sicherheitsmanagement 193

Anlage 14 (zu 30.4)
Hinweise zu Protokolldateien 194

Anlage 15 (zu 30.8)
Hinweise zu automatisierten Abrufverfahren i.S. § 10 BDSG 195

Anlage 16 (zu 32.3)
Schweigepflicht-Entbindungsklauseln in Versicherungsverträgen 197

Seite

Anlage 17 (zu 33.2)
Probleme des Fernmeldegeheimnisses und der Satellitenkommunikation
Bericht der Arbeitsgruppe Telekommunikation und Medien der Internationalen Datenschutzkonferenz
und
Gemeinsame Erklärung der 14. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 29. Oktober 1992 198

Anlage 18 (zu 1.7)
Übersicht über durchgeführte Kontrollen, Beratungen und Informationsbesuche 203

Anlage 19 (zu 1.7)
Wichtige Themen und die Art ihrer Bearbeitung 205

Anlage 20
Organigramm der Dienststelle 210

Sachregister 211

Abkürzungsverzeichnis 213

1 Schutz und Risiken für Persönlichkeitsrecht und Privatsphäre

Der Berichtszeitraum wurde von vier grundsätzlichen Entwicklungen geprägt:

— eine nachdenklich stimmende Ausweitung des rechtlichen und tatsächlichen Instrumentariums zur Kontrolle und Überwachung der Bürger in der Bundesrepublik Deutschland durch vermehrte Erhebung, Speicherung, Verknüpfung und Auswertung ihrer Daten (s. u. 1.1)

— zunehmende Erhebung, Verarbeitung und Nutzung personenbezogener Daten aufgrund von Entscheidungen der EG (s. u. 1.2)

— eine deutliche Verschärfung der öffentlichen Diskussion über „den Datenschutz" insgesamt (s. u. 1.3)

— die erfreulich verlaufene Einführung des Datenschutzes als Schutz des Persönlichkeitsrechts und der Privatsphäre in den neuen Ländern (s. u. 1.4)

1.1 Ausweitung des rechtlichen und tatsächlichen Instrumentariums zur Kontrolle und Überwachung

In manchen öffentlichen und veröffentlichten Meinungen scheint die Ansicht weit verbreitet, der demokratische Rechtsstaat Bundesrepublik Deutschland sei eine Art „Nachtwächterstaat", in dem Straftäter und Betrüger ziemlich ungestört ihr Unwesen treiben könnten. Straftäter hätten nur geringes Risiko, entdeckt zu werden. Betrüger könnten sich Sozialleistungen und Subventionen erschleichen, ohne daß die verantwortlichen Stellen etwas dagegen unternähmen. Und als Grund dafür wird häufig — zu Unrecht — der Datenschutz genannt. Die rechtliche und tatsächliche Entwicklung im Berichtszeitraum macht deutlich, daß dieses Vorurteil falsch ist. Die rechtlichen und tatsächlichen Möglichkeiten zur Kontrolle und Überwachung des Verhaltens der Bürger sind in den letzten Jahren nämlich kräftig ausgebaut und perfektioniert worden. Einige Beispiele mögen das verdeutlichen:

— Mit dem *Gesetz zur Neuregelung des Asylverfahrens* vom 26. Juni 1992 (BGBl. I S. 1126) wurde bestimmt, daß künftig erkennungsdienstliche Maßnahmen bei nahezu allen Asylbewerbern durchzuführen und die so gewonnenen Unterlagen beim Bundeskriminalamt aufzubewahren sind sowie unter bestimmten Voraussetzungen auch zur Strafverfolgung genutzt werden dürfen (s. u. 4.2).

— Das *Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität* vom 15. Juli 1992 (BGBl. I S. 1302) hat zum Zweck der Strafverfolgung Rechtsgrundlagen für die Rasterfahndung, den Einsatz verdeckter Ermittler, die Anwendung technischer Observationsmittel und die polizeiliche Beobachtung geschaffen (s. u. 5.1).

— Mit dem *Gesetz über die Errichtung eines* Bundesausfuhramtes vom 28. Februar 1992 (BGBl. I S. 376) wurde die Rechtsgrundlage für die Einrichtung des Bundesausfuhramtes geschaffen. Das Gesetz verfolgt das Ziel, die Kontrolle des Außenwirtschaftsverkehrs zu intensivieren (s. u. 7.1).

— Das *Gesetz zur Änderung des Außenwirtschaftsgesetzes, des Strafgesetzbuches und anderer Gesetze* vom 28. Februar 1992 (BGBl. I S. 372) hat erstmals die Überwachung des Brief-, Post- und Fernmeldeverkehrs zur Kontrolle des Außenwirtschaftverkehrs eingeführt und die Befugnis dazu dem Zollkriminalamt übertragen (s. u. 26.1).

— Das sogenannte *Zinsabschlaggesetz* vom 9. November 1992 (BGBl. I S. 1853) hat bestimmt, daß die zum Abzug von Steuern auf Zinseinkünfte Verpflichteten (z. B. Kreditinstitute) dem Bundesamt für Finanzen auf Anforderung die Daten aus allen Freistellungsanträgen ihrer Kunden mitzuteilen haben (s. u. 6.2).

— Mit dem *Gesundheitsstrukturgesetz* vom 21. Dezember 1992 (BGBl. I S. 2226) wurden neue Datenübermittlungen zugelassen und bestehende ausgeweitet. Damit wurden auch die Möglichkeiten für Kontrollen von Leistungsempfängern und von abrechnenden Ärzten/Zahnärzten verstärkt (s. u. 12.1).

— Durch Gesetz vom 18. Dezember 1992 (BGBl. I S. 2044) wurde in *§ 132a des Arbeitsförderungsgesetzes* festgelegt, daß und unter welchen Voraussetzungen die Bundesanstalt für Arbeit bei Betriebsprüfungen Daten für einen automatisierten Datenabgleich mit ihrer Leistungsdatei erheben darf (s. u. 11.1).

— Mit dem gleichen Gesetz wurde die Bundesanstalt für Arbeit ermächtigt, einmalig bei ihr vorhandene Leistungsdaten mit Daten bei Trägern früherer *Sonderversorgungssysteme der ehemaligen DDR* und der Bundesversicherungsanstalt für Angestellte abzugleichen (s. u. 11.1 letzter Absatz).

Viele Anzeichen sprechen dafür, daß die Tendenz zur stärkeren Kontrolle und Überwachung der Bürger sich aus den unterschiedlichsten Gründen fortsetzen und noch verstärken wird. Auch dafür einige Beispiele:

— Im Deutschen Bundestag wird zur Zeit der *Entwurf eines Gewinnaufspürungsgesetzes* — Drucksache 12/2704 — beraten, das die Verwertung der Gewinne aus Straftaten erschweren und damit den Anreiz zu Straftaten, die auf Gewinn zielen, nehmen soll. Meine Bemühungen richteten sich darauf, die darin vorgesehen nachhaltigen Eingriffe in die Rechte Nichtverdächtiger auf das unbedingt erforderliche Maß zu begrenzen (s. u. 5.1.2).

— Kurz vor Redaktionsschluß erfuhr ich, daß dem Deutschen Bundestag zur Zeit der *Entwurf eines Gesetzes zur Umsetzung des Föderalen Konsolidierungsprogramms* — Drucksache 12/4401 — vorliegt. Dieser soll — ohne nähere Begründung — den erst zum 1. Januar 1993 in Kraft getretenen § 132a AFG (s. o.) aufheben und durch einen § 150a AFG ersetzen. Der Gesetzentwurf be-

schränkt die in den Datenabgleich einzubeziehenden Daten nicht mehr auf einen bestimmten Datenkatalog und schreibt auch die Zweckbindung der so gewonnenen Daten nicht fest. Zudem sollen Arbeitgeber, Arbeitnehmer und alle auf dem Betriebsgrundstück angetroffenen Personen verpflichtet werden, unter anderem Auskünfte über Tatsachen zu erteilen, die darüber Aufschluß geben, ob Leistungen der Bundesanstalt für Arbeit zu Unrecht bezogen werden oder wurden.

— Mit dem gleichen Gesetzentwurf soll durch *Änderung des Sozialhilfegesetzes* auch ein regelmäßiger Datenabgleich zwischen den Trägern der Sozialhilfe einerseits sowie der Bundesanstalt für Arbeit und den Rentenversicherungsträgern andererseits eingeführt werden. Darüber hinaus sollen weitreichende Verfahren zur Übermittlung erforderlicher Informationen an die Träger der Sozialhilfe eingeführt werden.

— Der Bundesrechnungshof fordert einen *Abgleich der Datenbestände über Versorgungs- und Rentenleistungen*. Falls dessen dringende Notwendigkeit im überwiegenden Interesse der Allgemeinheit wirklich dargelegt werden kann, wäre für die Zulässigkeit des Abgleichs eine gesetzliche Regelung erforderlich (s. u. 13.2).

— die Europäische Gemeinschaft veranlaßt zunehmend die Erhebung und Verarbeitung personenbezogener Daten sowie deren Nutzung für Kontrollzwecke (s. u. 1.2).

Die tatsächliche Bedeutung dieser Entwicklung kann man nur ermessen, wenn man sich vor Augen führt, daß gleichzeitig neue oder weit leistungsfähigere Verfahren zur automatisierten Datenverarbeitung, insbesondere zu sogenannten Datenabgleichen, geschaffen worden sind oder — wo sie bereits vorhanden waren — weit intensiver genutzt werden. Beispiele dafür sind:

— Am 3. Dezember 1992 hat das Bundeskriminalamt die erste Ausbaustufe des neuen *Automatisierten Fingerabdruck-Identifizierungssystems AFIS* in Betrieb genommen. Es ermöglicht die automatisierte Verformelung aller Fingerabdrücke eines Datensatzes in ca. 2 bis 3 Minuten und ist damit etwa *30mal* schneller als das bisherige halbautomatische Verfahren. Schon jetzt können mit dem neuen Verfahren jährlich etwa 550 000 Datensätze verformelt werden. Nach Presseberichten ist — je nach Entwicklung der Asylbewerberzahlen — ein Ausbau um weitere 200 000 Datensätze pro Jahr möglich (s. u. 24.3).

— Das Zollkriminalamt hat im Berichtszeitraum das zur Überwachung des Außenwirtschaftsverkehrs im Jahr 1991 eingerichtete Datenverarbeitungssystem *KOBRA* (s. 13. TB S. 71f.) weiter ausgebaut.

— Mit dem Verfahren *DALEB* der Bundesanstalt für Arbeit wird die Datei der Versicherten (sie umfaßt etwa 40 Millionen Personen) mit der etwa 10,5 Millionen Personen speichernden Leistungsbezieherdatei laufend abgeglichen. Nach Mitteilung der Bundesanstalt für Arbeit konnten im Jahr 1992 damit mehr als 300 000 Fälle ermittelt werden, in denen der Verdacht bestand, daß Leistungsbezieher versicherungspflichtig beschäftigt waren.

— Im Rahmen der auf § 132a AFG gestützten *Betriebsprüfungen* wurden nach Mitteilung der Bundesanstalt für Arbeit im Jahr 1992 940 000 Lohnkonten überprüft (s. u. 11.1).

— Die *Stammsatzdatei des Verbandes Deutscher Rentenversicherungsträger*, in der etwa 84 Millionen Datensätze mit personenbezogenen Daten gespeichert sind, wird anscheinend zunehmend als eine Art zentrales Melde- und Auskunftsregister genutzt, was der Gesetzgeber nicht gewollt hat (s. u. 13.1).

— Demnächst wird auf dem Flughafen Frankfurt ein Versuch beginnen, in dem ein Verfahren zur *automatisierten Personenkontrolle* mit Hilfe von biometrischen Daten getestet werden soll (s. u. 25.3).

— In dem immer weiter ausgebauten ISDN-Telefonnetz werden — für eine bestimmte Zeit — die Verbindungsdaten der Telefongespräche gespeichert. Das gibt der nach § 12 des Fernmeldeanlagengesetzes bestehenden Pflicht zur Auskunftserteilung in Strafverfahren eine völlig neue Dimension.

— Die technische Ausgestaltung der sich immer mehr ausweitenden *Funktelefonnetze* gestattet es dem Netzbetreiber, sobald der Kunde seine Berechtigungskarte in das Gerät eingeführt und sich „eingebucht" hat, jederzeit den Standort des Telefons — und damit des Kunden — festzustellen.

Diese Liste ließe sich leicht verlängern.

Ich erwähne dies alles nicht, um den Gesetzgeber und die für die Einrichtung von Datenverarbeitungssystemen Verantwortlichen zu kritisieren, sondern mit dem Ziel einer objektiven Darstellung der für Persönlichkeitsrecht und Privatsphäre bedeutsamen Entwicklung im Berichtszeitraum. Für fast alle aufgeführten Rechtssetzungsakte und Maßnahmen gibt es gute Gründe. An der Vorbereitung der meisten Maßnahmen war ich beteiligt. Dabei habe ich die Vorhaben kritisch auf ihre Notwendigkeit hinterfragt. Soweit diese plausibel dargelegt wurde, habe ich einer Rechtssetzung oder Maßnahme nicht widersprochen, sondern begleitende Schutzvorkehrungen gefordert, um zu gewährleisten, daß das Recht auf informationelle Selbstbestimmung — entsprechend der Rechtsprechung des Bundesverfassungsgerichts — nur im überwiegenden Allgemeininteresse und nur in dem dafür erforderlichen Umfang eingeschränkt wird. Diese von mir geforderten Schutzvorschriften sollen den unverdächtigen Bürger vor nicht gerechtfertigten Eingriffen in sein Persönlichkeitsrecht und seine Privatsphäre bewahren — nicht den Täter.

Ich habe Sorge, daß der beschrittene Weg zu intensiverer Kontrolle und Überwachung, insbesondere zum Abgleich der verschiedensten Datenbestände, auch unter dem Gesichtspunkt der Gleichbehandlung zu immer neuen Forderungen nach solchen oder wenigstens vergleichbaren Maßnahmen führt, die dann z. B.

jede Ausgabe einer öffentlichen Körperschaft erfassen. Und mit einer gewissen Logik liegt bereits die Forderung auf dem Tisch, derartige Kontrollen auch auf die öffentlichen Einnahmen zu erstrecken. Wird dieser Weg ungebremst fortgesetzt, könnte sich aus einer Unsumme von automatisierten Dateien und aus einem Netz von Datenabgleichen, das schließlich alle Bürger und fast alle ihre Lebensbereiche erfaßt, der — jedenfalls wirtschaftlich und finanziell — „gläserne Bürger" ergeben. Deshalb muß bei jeder Forderung nach neuen Datenabgleichen — so plausibel sie für sich allein erscheint — eine Gesamtbetrachtung der Möglichkeiten zu Eingriffen in Persönlichkeitsrecht und Privatsphäre unserer Bürger erfolgen, und es muß geprüft werden, ob nicht ein Verzicht auf eine solche Maßnahme die im Interesse des Gemeinwohls insgesamt bessere Lösung wäre.

Oft gibt es für die Lösung einer Sachfrage oder eines Problems mehrere Möglichkeiten. Sie sind im sachlichen Ergebnis oft fast gleichwertig, unter Aspekten des Schutzes der Persönlichkeit und der Privatsphäre aber nicht selten sehr unterschiedlich zu bewerten. Ich empfehle in solchen Fällen dringend, schon früh auch die datenschutzrechtlichen Folgen in den Entscheidungsprozeß einzubeziehen. Was damit gemeint ist, zeigt deutlich die Diskussion um die Autobahngebühr: Ob eine solche eingeführt werden soll, ist eine verkehrs- und finanzpolitische Frage, zu der ich mich nicht äußere. Von erheblicher Bedeutung für Persönlichkeitsrecht und Privatsphäre ist aber, wie eine solche Gebühr erhoben werden soll. Wird sie — wie in der Schweiz — mit einer für einen bestimmten Zeitraum geltenden Vignette oder mit Hilfe einer Karte, deren Wert „abgefahren" wird, erhoben, entstehen kaum Risiken für das Persönlichkeitsrecht. Soll dagegen mit Hilfe eines in jedes Kraftfahrzeug einzubauenden kleinen Senders jedes Auffahren und Verlassen einer Autobahn zentral registriert werden, so entstehen Bewegungsbilder für das betreffende Kraftfahrzeug und seinen Fahrer, die einen erheblichen und für den verfolgten Zweck absolut unnötigen Eingriff in das Persönlichkeitsrecht darstellen.

1.2 Zunehmende Erhebung, Verarbeitung und Nutzung personenbezogener Daten aufgrund von Entscheidungen der EG

Die Europäische Gemeinschaft fordert von ihren Mitgliedstaaten in zunehmendem Umfang, personenbezogene Daten für Gemeinschaftszwecke zu erheben, zu verarbeiten und zu nutzen. Zentrale automatisierte Datenverarbeitungssysteme werden geschaffen, um einen gleichmäßigen gemeinschaftsweiten Informationsstand zu sichern oder der Kommission die Ausübung von Kontroll- und Überwachungsaufgaben zu ermöglichen oder zu erleichtern. Die Mitgliedstaaten müssen dafür die — oft auch personenbezogenen — Daten an Gemeinschaftseinrichtungen übermitteln. Im einzelnen ist zur Skizzierung dieser Entwicklung auf folgendes hinzuweisen:

— Die Einrichtung des *Schengener Informationssystems SIS* (vgl. 12. TB S. 95 f) ist bereits weit gediehen. Infolge des Beitritts von Spanien, Portugal, Italien und Griechenland wird es sich auf alle kontinentalen EG-Mitglieder — außer Dänemark — erstrecken (s. u. 24.1.2).

— In Ergänzung des Schengener Informationssystems soll ein *Europäisches Informationssystem EIS* errichtet werden, dem auch Dänemark, Irland und das Vereinigte Königreich angehören sollen (s. u. 24.2.1).

— Im Dezember 1991 hat der Europäische Rat in Maastricht die Schaffung eines *Europäischen Kriminalpolizeiamtes EUROPOL* beschlossen. Im Endausbau soll dieses Amt ein gemeinschaftsweites Informationssystem zur Bekämpfung des Terrorismus, des illegalen Drogenhandels und anderer schwerwiegender Formen der Kriminalität betreiben (s. u. 24.2.2).

— Die EG-Mitgliedstaaten beabsichtigen die Einrichtung eines gemeinsamen automatisierten *Zollinformationssystems CIS* (Customs Information System), das die Zollverwaltungen bei der Verhinderung, Ermittlung und Verfolgung schwerwiegender Zuwiderhandlungen gegen nationale Zollbestimmungen unterstützen soll, die dem Schutz der öffentlichen Sicherheit oder der Bekämpfung der Geldwäsche dienen (s. u. 26.3).

— Über die Einführung eines europaweiten *Systems zur Erfassung der Fingerabdrücke von Asylbewerbern — EURODAC —* wird diskutiert (s. u. 33.4).

— Die von der EG beschlossene neue Struktur der *Agrarförderung* macht es notwendig, daß über jeden landwirtschaftlichen Betrieb detaillierte Angaben erhoben und verarbeitet werden. In den Agrarverwaltungen der Länder werden daher umfangreiche und tiefgegliederte Datensammlungen entstehen. Diese Sammlungen sollen nach einer einschlägigen EG-Regelung auch zur Kontrolle der landwirtschaftlichen Betriebe, u. a. mit Hilfe von Luftbildern und Satellitenaufnahmen, genutzt werden (s. u. 8.1).

— Die Zahlungsvorgänge aus dem *Europäischen Ausrichtungs- und Garantiefonds für die Landwirtschaft* müssen der EG-Kommission zur Prüfung des Rechnungsabschlusses mitgeteilt werden, im Falle von Stichproben auch in personenbezogener Form (s. u. 6.8).

— Die EG-Kommission beabsichtigt, in Form einer zentralen Datenbank ein *EG-Zollinformationssystem* einzurichten, um die ordnungsgemäße Anwendung der von der EG erlassenen Zoll- und Agrarregelungen zu gewährleisten (s. u. 6.7.1).

— Die EG aktiviert ihre *Statistik* und strebt dabei Regelungen an, die das Statistikgeheimnis verletzen würden (s. u. 23.1 und 23.1.1).

Es ist unübersehbar, daß die Europäische Gemeinschaft auch zur Informations- und Datengemeinschaft wird. Es muß also beachtet werden, daß das dabei entstehende System von Kontrollen und Überwachungen zu den nationalen Kontrollmechanismen hinzutritt, so daß sich die Einschränkungen des Persönlichkeitsrechts und der Privatsphäre der Bürger vervielfachen.

1.3 Verschärfung der öffentlichen Diskussion über den Datenschutz insgesamt

Im Berichtszeitraum bin ich wegen der in Ausübung meines Amtes vertretenen Position aus dem politischen Raum auch persönlich angegriffen worden. Mir wurde vorgeworfen, die Privatsphäre des Verbrechers a priori vor dem Staat schützen zu wollen. Dies wurde als skandalös bezeichnet. Was war der Hintergrund?

Im Zusammenhang mit der Erörterung des großen Lauschangriffs (s. u. 5.1.3), hatte ich in einer Diskussionsrunde auf die Rechtsprechung des Bundesverfassungsgerichts hingewiesen, wonach dem Einzelnen ein „Innenraum" verbleiben muß, in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und sein Recht auf Einsamkeit genießt (BVerfGE 27/1/6). Ich hatte u. a. ergänzend betont, daß die Frage der Wanze und der Videokamera im engsten Wohnungsbereich die Menschenwürde berührt. Und ich habe daraus die Konsequenz gezogen, daß das vom Bundesverfassungsgericht aus der Menschenwürde abgeleitete Recht auf diesen „Innenraum" auch dem zusteht, der einer Straftat verdächtigt wird. Es mag sein, daß mein von einer Tageszeitung veröffentlichter Beitrag aus einer Diskussionsrunde sehr knapp und vielleicht auch nicht ganz glücklich formuliert war. Aus dem Zusammenhang ergab sich aber klar, was gemeint war, und ich habe dies unter 5.1.3 noch einmal zusammenfassend dargestellt. Daraus ergibt sich, daß meine Position der Polizei den Lauschangriff auch auf Wohnungen zur Abwehr und einer Gefahr für die Existenz und Menschenwürde anderer zugesteht und auch für Strafverfolgungszwecke lediglich den Bereich der echten Privatwohnung von Lauschangriffen frei halten will. Ich habe auch vorgeschlagen, zur Versachlichung der Diskussion vor einer Änderung des Grundgesetzes erst einmal die Entscheidung des Bundesverfassungsgerichts über zwei Verfassungsbeschwerden gegen die Regelung des Lauschangriffs im Polizeigesetz Baden-Württemberg und im hamburgischen Gesetz über die Datenverarbeitung der Polizei abzuwaren. Ich wiederhole diesen Vorschlag.

Eine andere Attacke ist grundsätzlicher und zielt auf den Datenschutz, ja auf die grundrechtlich geschützten Freiheitsrechte insgesamt. Aus der Leitung des Bundeskriminalamtes wird in Pressegesprächen und Vorträgen immer wieder erklärt, in der Bundesrepublik Deutschland seien die individuellen Freiheitsrechte „außerordentlich stark ausgebildet und entwickelt", „mitunter sogar verabsolutiert". Eine „Überlast zugunsten der Freiheitsrechte" wird beklagt. Dabei wird auch der Datenschutz ausdrücklich genannt und als „Überrecht", das „die Arbeit der Polizei erheblich erschwert", diffamiert. Die Behauptungen gipfeln dann darin, daß personeller Aufwand zugunsten des Schutzes von Persönlichkeitsrecht und Privatsphäre mit der Begründung abgelehnt wird, die dafür eingesetzten Beamten fehlten bei den kriminalpolizeilichen Ermittlungen. Solche Erklärungen überraschen besonders deshalb, weil meine Zusammenarbeit mit dem Bundeskriminalamt in der Sache außerordentlich gut ist. Es hat noch kein praktisches Problem gegeben, bei dem nach Diskussion nicht ein Ergebnis erzielt werden konnte, mit dem beide Seiten leben konnten. Ich verweise für den Berichtszeitraum insbesondere auf die Beiträge zu AFIS (24.3) sowie zur Übermittlung von Kfz-Sachfahndungsdaten an den HUK-Verband und an Kraftfahrzeughersteller (24.4).

In der Einleitung zu meinem 13. Tätigkeitsbericht habe ich erklärt, daß ich jederzeit zu Gesprächen und auch zu Mitverantwortung bereit bin, wenn es darum gehen sollte, echte und vermeintliche datenschutzrechtliche Schranken für ein Tätigwerden der Strafverfolgungsorgane bei der Terrorismusbekämpfung zu erörtern und — wenn möglich — zu beheben. Entsprechend dieser Position habe ich die Leitung des BKA mehrfach gebeten, mich doch zu unterrichten, wenn irgend eine konkrete Regelung datenschutzrechtlicher Art sich auf Grund der gewonnenen Erfahrungen als echtes Hindernis für eine wirksame Strafverfolgung erwiesen habe. Nichts dergleichen habe ich im Berichtszeitraum gehört.

Die oben erwähnten Angriffe sind stets sehr allgemein gehalten. Konkretes und Nachprüfbares findet sich nicht. Vor kurzem wurde in einer Wochenzeitung als Meinung aus der Leitung des BKA wiedergegeben, die für das BKA geltenden Löschungsregelungen verhinderten die Ermittlung von Straftätern. Da man verschiedentlich diese Fristen übersehen habe, hätten dann mit Hilfe der noch vorhandenen Daten Straftäter identifiziert werden können. Ich habe das BKA sofort aufgefordert, mir die entsprechenden Fälle zu nennen. Trotz mehrfacher Fristsetzung ist mir bis Redaktionsschluß eine Antwort auf meine Fragen nicht zugegangen. Ich erwarte auch keine überzeugende Antwort, denn die geltenden Regelungen sehen ja keinen Löschungsautomatismus vor, wie ich unter 24.7 näher darlege.

Es kann sein, daß eine Regelung, die in bester Absicht getroffen wurde, in der Praxis Probleme aufwirft. Wenn das der Fall sein sollte, muß nüchtern geprüft werden, ob sie auf Grund von Erfahrungen zu ändern ist. Dazu ist aber notwendig, daß man die hinderlichen Regelungen benennt und die dagegen sprechenden Erfahrungen offen darlegt. Dies muß ein Prozeß sein, zu dem beide Seiten bereit sind. Vor der Erzeugung einer allgemeinen Stimmung gegen die Freiheitsrechte einschließlich des Datenschutzes kann ich nur nachdrücklich warnen.

1.4 Einführung des Datenschutzes als Schutz des Persönlichkeitsrechts und der Privatsphäre in den neuen Ländern

Nach dem Einigungsvertrag trat das damals geltende Bundesdatenschutzgesetz am 3. Oktober 1990 mit einigen Maßgaben (s. u. 2.1) im Beitrittsgebiet in Kraft. Es wurde am 1. Juni 1991 durch das neue Bundesdatenschutzgesetz abgelöst, das zunächst auch für die öffentlichen Stellen der Länder — und zwar ohne Befristung — galt. Der Bundesbeauftragte für den Datenschutz durfte die ihm durch den Einigungsvertrag übertragene Datenschutzkontrolle im öffentlichen Bereich der Länder und Gemeinden längstens bis zum 31. Dezember 1991 ausüben. Daraus

ergab sich für die neuen Länder der Zwang, sehr schnell eigene Landesdatenschutzgesetze mit Regelungen für die Bestellung eines Landesbeauftragten für den Datenschutz zu verabschieden, wenn sie eine datenschutzkontrollfreie Zeit vermeiden wollten.

Den Ländern Thüringen und Sachsen ist es gelungen, ihre Datenschutzgesetze noch vor dem 1. Januar 1992 zu verabschieden, die anderen neuen Länder folgten, zuletzt Mecklenburg-Vorpommern mit dem Landesdatenschutzgesetz vom 24. Juli 1992. Das Land Thüringen, bei dem zuerst die gesetzlichen Voraussetzungen für die Bestellung eines Datenschutzbeauftragten vorhanden waren, hatte bei Redaktionsschluß, also etwa 17 Monate nach Inkrafttreten des Gesetzes, leider immer noch keinen Datenschutzbeauftragten. Die übrigen neuen Länder haben sehr schnell nach Verabschiedung ihrer Landesdatenschutzgesetze eigene Landesdatenschutzbeauftragte bestellt; diese wirken bereits in der Konferenz der Datenschutzbeauftragten von Bund und Ländern tatkräftig mit (s. u. 1.8).

In den Jahren 1991 und 1992 habe ich mich im Beitrittsgebiet bei vielen Stellen informiert und insbesondere öffentliche Stellen des Bundes kontrolliert; über die dabei getroffenen wesentlichen Feststellungen berichte ich nachfolgend, vor allem im Teil 2. Zu Informations- und Kontrollbesuchen bei öffentlichen Stellen der Länder und Gemeinden im Jahre 1991 habe ich Berichte gefertigt, die ich den betroffenen Stellen und ihren vorgesetzten Behörden zugeleitet habe. Nachdem Landesbeauftragte für den Datenschutz bestellt worden waren, habe ich die Vorgänge, die sich auf Informations- und Kontrollbesuche bei öffentlichen Stellen der Länder und Gemeinden bezogen haben, an den jeweils zuständigen Landesdatenschutzbeauftragten abgegeben.

1.5 Eingaben von Bürgern

Auch im Berichtszeitraum haben wieder zahlreiche Bürger von ihrem Recht Gebrauch gemacht, sich mit Eingaben an mich zu wenden. Die Eingaben betreffen ein breites Spektrum des Lebens. Einige besonders bemerkenswerte möchte ich schon an dieser Stelle erwähnen:

— In mehreren Fällen beschwerten sich Bürger darüber, daß bei ihnen zugegangenen Briefsendungen in Kuverts mit Sichtfenstern sie betreffende teilweise empfindliche personenbezogene Daten wahrgenommen werden konnten. Die Daten reichten von der Nummer des Postscheckkontos über einen Betreff: „Kriegsdienstverweigerung; hier: Rücknahme Ihres Antrages" bis zur sichtbaren Angabe „Verletzung Ihrer Dienstpflichten". Die Eingaben zeigen, daß bei der Verwendung von Kuverts mit Sichtfenstern darauf geachtet werden muß, daß nicht — in der Regel ungewollt — belastende personenbezogene Informationen über einen Bürger offenbart werden.

— In einem anderen Fall wandte sich ein Zollbeamter dagegen, daß er auf einem ihm zur Benutzung übersandten Überweisungsformular als Verwendungszweck ausdrücklich „Geldbuße im Disziplinarverfahren" angeben sollte. Die Forderung entsprach den noch geltenden Richtlinien, wurde aber kurzfristig geändert, als ich mich eingeschaltet hatte.

— Ein ehemaliger Angestellter der Bundesanstalt für Arbeit wandte sich dagegen, daß ohne sein Wissen ärztliche Gutachten nach Aktenlage über ihn eingeholt und ohne sein Wissen zu seinen Personalakten genommen worden waren. Die Bundesanstalt für Arbeit hat ihr Verfahren so umgestellt, daß sich ein ähnlicher Vorgang nach menschlichem Ermessen nicht mehr wiederholen kann.

— Ein Arbeitsloser beschwerte sich mit Recht darüber, daß er ohne sein Wissen von einem Nervenarzt im Rahmen eines Gesprächs „untersucht" und daß über diese Untersuchung ein mehrseitiges Gutachten erstellt worden war, das ihm zunächst vorenthalten wurde.

— In zwei Fällen beklagten Petenten, daß Bedienstete des Bundesamtes für Verfassungsschutz Informationen über sie in ihr privates Umfeld (Arbeitgeber und Mitbewohner) gegeben hatten. Erst nach Einschaltung des Innenausschusses des Deutschen Bundestages hat das Bundesministerium des Innern eingeräumt, daß diese Verfahren unzulässig waren.

— Ein Arbeitnehmer beschwerte sich darüber, daß er nach einer „Sicherheitsüberprüfung" durch den Bundesgrenzschutz seinen Arbeitsplatz verloren hatte. Die Hintergründe des Falles konnten leider nicht völlig geklärt werden.

— Ein Petent führte Klage darüber, daß die Deutsche Bundespost — TELEKOM — auf Antrag eines Nachbarn eine Fangschaltung auf seinen Telefonapparat geschaltet und ihn nach deren Ende trotz eines entsprechenden Antrags darüber nicht unterrichtet hatte. Die Nachprüfung des Falles ergab deutliche Mängel im Verfahren über die Einrichtung von Fangschaltungen.

— Ein Gewerbetreibender teilte mit, die Deutsche Bundespost Telekom habe seine Telefonnummer unverzüglich nach seinem Auszug aus den bisherigen Geschäftsräumen dem nachfolgenden Pächter dieser Räume zugeteilt. Dies führe dazu, daß für ihn bestimmte Telefax-Mitteilungen von Geschäftspartnern, darunter auch von ausländischen Banken, bei denen die Fax-Nummer gespeichert sei, dort eingingen und damit Unbefugten zugeleitet würden.

1.6 Besondere Erfolge und erfreuliche Feststellungen

Wie im 13. Tätigkeitsbericht möchte ich nicht nur kritisieren, sondern auch auf einige besonders erfreuliche Feststellungen hinweisen:

Wie unter 1.1 dargelegt, war die Gesetzgebung mehr durch Ausweitung und Perfektionierung staatlicher Kontrolle und Überwachung als durch Ausbau des Schutzes von Persönlichkeitsrecht und Privatsphäre gekennzeichnet. Soweit meine Beteiligung rechtzeitig erfolgte — was erfreulich oft geschah —, konnte

häufig sichergestellt werden, daß nicht mehr als unbedingt erforderlich in Persönlichkeitsrecht und Privatsphäre der Bürger eingegriffen wurde. Ich denke hier z. B. an die sehr erfreuliche Zusammenarbeit mit dem Bundesgesundheitsministerium beim Sicherungsgesetz für das Nationale Krebsregister (s. u. 2.9) sowie bei der Vorbereitung des Bundeskrebsregistergesetzes (s. u. 17.1). Sehr intensiv und erfreulich war die Diskussion mit der Bundesregierung auch bei der Vorbereitung der Regelung in § 29 d des Luftverkehrsgesetzes für die Sicherheitsüberprüfung des Personals auf Flughäfen (s. u. 18.10.1), beim Gesundheitsstrukturgesetz (s. u. 12.1), bei der Vorbereitung der Neuregelungen des Datenschutzes im Sozialbereich (s. u. 10.1) und der Sicherheitsüberprüfung (s. u. 27.1). Dabei konnten fachliche und datenschutzrechtliche Forderungen mit gegenseitigem Verständnis fast immer auf einen gemeinsamen Nenner gebracht werden.

Bei der Anwendung datenschutzrechtlicher Vorschriften zeigten öffentliche Stellen des Bundes in einer ganzen Reihe von Fällen das Bestreben, sich beim Schutz des Persönlichkeitsrechts und der Privatsphäre nicht mit dem gesetzlich gebotenen Minimum zu begnügen, sondern die möglichst beste Lösung anzustreben.

— Auf Weisung des damaligen Bundesministers für Jugend, Familie, Frauen und Gesundheit vernichtet das Bundesamt für den Zivildienst seit dem 1. Februar 1990 die Anerkennungsunterlagen anerkannter Kriegsdienstverweigerer bereits unmittelbar nach Bestandskraft des Anerkennungsbescheides, also deutlich früher als das Gesetz es vorschreibt (s. u. 16.2.1). Damit wird zuverlässig gewährleistet, daß diese sensiblen Unterlagen nicht Personen zur Kenntnis gelangen, die sie für die Erfüllung ihrer Aufgaben nicht benötigen.

— Die Kaufmännische Krankenkasse Hannover hat auf Grund meiner Empfehlungen die Bearbeitung von Beihilfevorgängen in vorbildlicher Weise vollständig von der Personalverwaltung getrennt (vgl. 9.3.1).

— Die Berufsgenossenschaft für Fahrzeughaltungen hat die Anregung in meinem 13. Tätigkeitsbericht, in den Bezirksverwaltungen Ansprechpartner für den Datenschutz zu bestellen, umgesetzt, obwohl das Gesetz eine solche Maßnahme nicht ausdrücklich vorschreibt.

1.7 Beratungen und Kontrollen, insbesondere Beanstandungen

Im Berichtszeitraum haben der Deutsche Bundestag, die Bundesministerien und zahlreiche andere öffentliche Stellen des Bundes wieder meine Beratung gewünscht. Dem bin ich gern gefolgt. Ich habe aus eigener Initiative, auf Grund von Eingaben oder nach Berichten in den Medien zahlreiche Informations- und Kontrollbesuche bei Dienststellen durchgeführt. Darüber unterrichten die Anlagen 18 und 19.

Auch im Berichtszeitraum mußte ich wieder eine Reihe von Verstößen gegen datenschutzrechtliche Vorschriften und Mängel beim Datenschutz förmlich beanstanden. Entsprechend der bisherigen Praxis mache ich von diesem Recht nur bei erheblichen Verstößen und Mängeln oder dann Gebrauch, wenn eine öffentliche Stelle nicht bereit ist, Verstöße und Mängel von geringerer Bedeutung abzustellen.

Die Zahl der Beanstandungen liegt im Jahresschnitt wieder etwa auf der Höhe der Vorjahre. Zahlenmäßige Schwerpunkte zeigen sich in den Geschäftsbereichen des Bundesministeriums des Innern, der Bundesanstalt für Arbeit und der Deutschen Bundespost Telekom. Ich gehe davon aus, daß die notwendigen Beanstandungen im Bereich des Bundesamtes für Verfassungsschutz wenigstens teilweise auf Anfangsschwierigkeiten bei der Auslegung des neuen Verfassungsschutzgesetzes zurückzuführen sind. Ich vertraue auch darauf, daß das Bundesministerium des Innern und das Bundesamt für Verfassungsschutz den Beschluß des Deutschen Bundestages vom 5. Februar 1993 beachten (s. Anlage 1). In den Beanstandungen im Bereich der Bundesanstalt für Arbeit sind zwei — für sich gesehen schwerwiegende — Verstöße in Einzelfällen enthalten. Aus ihnen kann nicht auf generell unzureichenden Datenschutz bei der Bundesanstalt für Arbeit geschlossen werden. Zahlenmäßig an der Spitze der Beanstandungen liegt — leider — wieder der Bereich der Deutschen Bundespost Telekom. Die Beanstandungen im einzelnen:

Auswärtiges Amt

Verstoß gegen §§ 9 und 18 BDSG bei der Verarbeitung personenbezogener Daten auf Arbeitsplatzcomputern in Auslandsvertretungen (s. u. 4.10.2 am Ende)

Bundesministerium des Innern

— Drei Verstöße des Bundesamtes für Verfassungsschutz gegen § 19 Abs. 4 Bundesverfassungsschutzgesetz durch unzulässige Weitergabe personenbezogener Daten an nicht-öffentliche Stellen (s. u. 27.2)

— Mangelhafte Unterstützung des BfV bei der Erfüllung meiner Aufgaben; Verstoß gegen § 22 Abs. 4 BDSG (s. u. 27.5)

— Verstöße des BKA gegen § 2 Abs. 1 Nr. 1 BKA-Gesetz i.V.m. § 14 BDSG wegen unzulässiger Speicherung „anderer Personen" in der Datei APIS sowie gegen die Errichtungsanordnung zu APIS wegen unterlassener Prüfung der weiteren Erforderlichkeit der Speicherung „anderer Personen" (s. u. 24.8.2)

— Unzulässige Übermittlung von Hinweisen auf vorhandene „Sicherungsvorgänge" des ehemaligen Staatssicherheitsdienstes durch den Sonderbeauftragten der Bundesregierung für die personenbezogenen Unterlagen des ehemaligen Staatssicherheitsdienstes an öffentliche Stellen im Zusammenhang mit Überprüfungsanträgen; Verstoß gegen §§ 2 und 5 der Anlage I, Kapitel II Sachgebiet B Abschnitt II Nr. 2b zum Einigungsvertrag i.V.m. § 15 Abs. 1 Nr. 1 BDSG (s. u. 4.4.2).

Bundesministerium der Finanzen

Verstoß gegen § 9 BDSG (alt) durch unzulässige Speicherung von Personalien freier Mitarbeiter von Versicherungsgesellschaften im Bundesaufsichtsamt für das Versicherungswesen (s. u. 7.5)

Bundesministerium der Verteidigung

Verstoß gegen das Löschungsgebot des § 12 Abs. 4 in Verbindung mit § 35 Abs. 2 Satz 2 Nr. 1 und 3 BDSG bei bestimmten Daten auf Wehrstammkarten der ehemaligen NVA (s. u.2.8.1)

Wirtschaftsprüferkammer

Mißachtung des Widerspruchs eines Betroffenen gegen die Veröffentlichung seiner Daten im Wirtschaftsprüferverzeichnis (s. u. 7.2)

Bundesanstalt für Arbeit

— 3 Verstöße durch ein Arbeitsamt in einem Einzelfall gegen

  a) Artikel 6 der Datenschutzkonvention des Europarates, § 14 Abs. 2 und § 27 Abs. 2 AFG und § 1 a der Berufsordnung für die deutschen Ärzte

  b) § 35 SGB I i. V. m. §§ 67, 69, 76 SGB X

  c) ärztliches Standesrecht und § 25 Abs. 1, 2 SGB X (s. u. 11.5.1)

— Unzulässige Datenspeicherung durch ein Arbeitsamt; Verstoß gegen § 14 Abs. 1 BDSG (s. u. 11.6).

— 3 Verstöße durch ein Arbeitsamt in einem Einzelfall gegen

  a) Recht auf informationelle Selbstbestimmung

  b) § 35 Abs. 1 SGB I i.V.m. §§ 67, 69 Abs. 1 SGB X

  c) § 13 Abs. 2 des Manteltarifvertrages für die Angestellten der Bundesanstalt für Arbeit (s. u. 9.14.2).

Vorstand der Deutschen Bundespost Postdienst

Zweimalige Verletzung des Personalaktengeheimnisses in einem Einzelfall (s. u. 9.12).

Vorstand der Deutschen Bundespost Telekom

Risikoträchtige Systemgestaltung und mangelhafte Zugriffssicherung eines Rechnernetzes zur Administration von Telefonanschlüssen (OMDS); Verstoß gegen § 9 Satz 1, § 18 Abs. 2 Satz 3 BDSG (s. u. 21.6)

Rechtswidrige Registrierung von Telefonverbindungsdaten („Verkehrssondermessungen") durch ZVE-Schaltungen; Verstoß gegen § 4 Abs. 1 BDSG, § 3 Abs. 1 TDSV (s. u. 21.6)

Verfahrensmängel bei einer ZVE-Schaltung auf den Telefonanschluß eines angeblichen Belästigers; Verstoß gegen § 18 BDSG. Unterlassene Unterrichtung des Betroffenen; Verstoß gegen § 8 Abs. 2 Satz 2 TDSV (s. u. 21.12)

Unzulässige Weitergabe von Informationen über Schulden eines Telekomkunden durch ein Fernmeldeamt; Verstoß gegen § 454 Abs. 2 TKO(s. u. 21.9)

Bundesversicherungsanstalt für Angestellte

Verstoß gegen das Sozialgeheimnis nach § 35 Abs. 1 SGB I i.V.m. § 76 Abs. 2 Nr. 1 SGB X (s. u. 13.3.1)

Eine Berufsgenossenschaft

Verstoß gegen das Sozialgeheimnis nach § 35 SGB I i.V.m. § 79 SGB X und § 9 BDSG (s. u. 2.6.1)

Eine Berufsgenossenschaft

Verstoß gegen das Sozialgeheimnis nach § 35 SGB I i.V.m. § 69 Abs. 1 Nr. 1 2. Alternative SGB X in einem Einzelfall (s. u. 10.4.1)

Eine Berufsgenossenschaft

Verstoß gegen das Sozialgeheimnis nach § 35 SGB I und § 79 SGB X i.V.m. § 9 BDSG (s. u. 14.2)

Eine Berufsgenossenschaft

Verstoß gegen den Ersterhebungsgrundsatz nach § 13 Abs. 2 Satz 1 BDSG (s. u. 10.2)

Ein Spitzenverband der gesetzlichen Krankenkassen

Mangelnde Unterstützung des BfD; Verstoß gegen § 24 Abs. 4 BDSG (s. u. 12.6)

1.8 Zusammenarbeit mit den Landesbeauftragten für den Datenschutz und anderen Stellen

Auch im Berichtszeitraum hat die gemeinsame Konferenz der Datenschutzbeauftragten von Bund und Ländern wichtige Themen des Datenschutzes erörtert. 1991 hatte ich turnusgemäß den Vorsitz, 1992 die Landesbeauftragte für den Datenschutz Baden-Württemberg, 1993 der Berliner Datenschutzbeauftragte. Auf fünf Konferenzen in Weimar, Stuttgart und Berlin

wurden Entschließungen zu folgenden Themen gefaßt:

— Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität — OrgKG (Entschließung vom 25. Juni 1991, Anlage 2)

— Datenschutz im Recht des öffentlichen Dienstes (Entschließung vom 26./27. September 1991, Anlage 3).

— Arbeitnehmerdatenschutz (Entschließung vom 23./24. März 1992, Anlage 4).

— Neuregelung des Asylverfahrens (Entschließung vom 28. April 1992, Anlage 5).

— Grundrecht auf Datenschutz (Entschließung vom 28. April 1992, Anlage 6).

— Datenschutz bei internen Telekommunikationsanlagen (Entschließung vom 1./2. Oktober 1992, Anlage 7).

— Entwurf eines Gesetzes zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung — Gesundheitsstruktur-Gesetz 1993 — (Entschließung vom 1./2. Oktober 1992, Anlage 8)

— Krankenversichertenkarte als Chipkarte (Entschließung vom 1./2. Oktober 1992, Anlage 9)

— „Lauschangriff" (Entschließung vom 1./2. Oktober 1992, Anlage 10)

— Richtlinie des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt — 30/313/EWG (Entschließung vom 16./17. Februar 1993, Anlage 11)

Im Berichtszeitraum konnte die Konferenz vier Kollegen aus den neuen Ländern begrüßen: Die Landesdatenschutzbeauftragten von Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und Sachsen. Die Zusammenarbeit mit den neuen Konferenzteilnehmern ist außerordentlich gut, die Konferenz hat durch diese Neuzugänge eine Bereicherung erfahren. Leider hat das Land Thüringen immer noch keinen Landesdatenschutzbeauftragten bestellt.

Auf meine Anregung hat sich im Frühjahr 1991 eine Arbeitsgruppe „Neue Länder" konstituiert. Zur ersten Sitzung hatte ich im Rahmen meiner Kontrollzuständigkeit für den öffentlichen Bereich im Beitrittsgebiet die damaligen Ansprechpartner für den Datenschutz aus den Innenministerien der neuen Länder eingeladen. Diese Arbeitsgruppe befaßt sich mit den zahlreichen Sonderproblemen datenschutzrechtlicher Art im Beitrittsgebiet. Sie setzt sich jetzt zusammen aus den Landesbeauftragten für den Datenschutz der neuen Länder sowie Berlins, dem Ansprechpartner in Thüringen und dem Bundesbeauftragten für den Datenschutz; der Datenschutzbeauftragte der Treuhandanstalt wird bei Bedarf beteiligt.

Wie auch in den Vorjahren habe ich im Berichtszeitraum an den Beratungen der Obersten Aufsichtsbehörden der Länder im sogenannten „Düsseldorfer Kreis" und seiner Arbeitsgruppen teilgenommen, um mich über die wichtigsten Entwicklungen des Datenschutzes im nichtöffentlichen Bereich zu informieren (s. u. 32).

Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) hat seine Kapazitäten zur Beratung weiter auf- und ausgebaut. Ich konnte daher auch seine — mir gesetzlich zustehende — Unterstützung bereits in Anspruch nehmen, z. B. bei der Erarbeitung einer Konzeption der Krankenversichertenkarte (s. u. 12.4 und 30.1).

Von Bedeutung für meine Arbeit ist auch der Informationsaustausch mit Obersten Bundesbehörden im Interministeriellen Koordinierungsausschuß für den Einsatz der automatisierten Datenverarbeitung (IMKA) und im Interministeriellen Arbeitskreis für die Sicherheit in der Informationstechnik (ISIT).

Die Kooperation mit den europäischen Institutionen des Datenschutzes ist in den Jahren 1991 und 1992 noch intensiver geworden, vor allem aufgrund der gemeinsamen Arbeit an dem Vorschlag der EG-Kommission für eine Datenschutzrichtlinie. An der 13. und an der 14. Internationalen Datenschutzkonferenz, die im Oktober 1991 in Straßburg und im November 1992 in Sydney, Australien, stattfanden, habe ich mich beteiligt. (Näheres zum internationalen Datenschutz s. u. 33)

1.9 APC-Programm zur automatisierten Registermeldung

Voraussetzung für einen wirksamen Datenschutz in einer öffentlichen Stelle ist, daß diese vollständige und aktuelle Kenntnis darüber hat, welche Dateien personenbezogener Daten bei ihr wie und für welchen Zweck betrieben werden sowie welche Daten diese enthalten. Das BDSG alter Fassung forderte deshalb, eine „Übersicht" über diese Dateien zu führen, das neue BDSG konkretisiert und ergänzt in § 18 Abs. 2 diese Forderung.

Öffentliche Stellen haben für die bei ihnen geführten Dateien schriftlich festzulegen:

1. Bezeichnung und Art der Dateien,
2. deren Zweckbestimmung,
3. die Art der gespeicherten Daten,
4. den betroffenen Personenkreis,
5. die Art der regelmäßig zu übermittelnden Daten und deren Empfänger,
6. die Regelfristen für die Löschung der Daten,
7. die zugriffsberechtigten Personengruppen oder die Personen, die allein zugriffsberechtigt sind.

Soweit es sich um automatisiert geführte Dateien handelt, meldet die speichernde Stelle den Inhalt dieses Dateiverzeichnisses — mit Ausnahme der Zugriffsberechtigten — zu dem von mir geführten „Register der automatisiert geführten Dateien" (§ 26 Abs. 5 Satz 1 BDSG). Dieses Register ist öffentlich, es kann von jedermann eingesehen werden. Um den Verwaltungsaufwand — sowohl bei den speichernden Stellen als auch in meiner Dienststelle — gering zu

halten, aber auch um den Nutzungswert von Dateiverzeichnis und Datenschutzregister zu erhöhen, habe ich ein APC-Programm entwickeln lassen, das auf allen IBM-kompatiblen Rechnern unter dem Betriebssystem MS-DOS, PC-DOS und DR-DOS ablauffähig ist. Es wird von meiner Dienststelle auf Anforderung kostenlos an Bundesbehörden abgegeben.

Das Programm unterstützt die speichernde Stelle — und zwar die dateiführende Stelle (Fachreferate) und den Datenschutzbeauftragten — sowohl beim Führen des Dateiverzeichnisses als auch bei der Meldung zum Register. Es umfaßt u. a. folgende Funktionen:

— Manuelle Eingabe und Bearbeitung der für die genannten Zwecke zu erfassenden Dateien von den dateiführenden Stellen des Hauses (Fachreferate usw.),

— „Einspielen" eines Datenbestandes von Diskette („Import"),

— Ausgabe des Datenbestandes auf Diskette zur Datensicherung und zur Weitermeldung von der dateiführenden Stelle an den Datenschutzbeauftragten sowie von diesem an den Bundesbeauftragten („Export"),

— Erstellen von Listenauswertungen (z. B. Liste der Dateien nach § 18 Abs. 2, Liste der gemäß § 26 Abs. 5 zum Register gemeldeten Dateien).

Das Programm enthält außerdem eine Hilfsfunktion, mit der eine Ausfüllanleitung für die Meldung zum Register aufgerufen werden kann.

Bei Bedarf kann das Programm auch bei den Untergliederungen einer Behörde (z. B. Abteilungen) eingesetzt werden. Die dort geführten Dateiverzeichnisse können auf Diskette an eine zentrale Stelle weitergegeben werden. Von dieser werden sie mit der Importfunktion gesammelt, zusammengefaßt und ergeben so das Gesamtdateiverzeichnis der öffentlichen Stelle. Aus diesem heraus kann dann auf Diskette die Meldung zu dem von mir geführten Register erstellt werden.

In meiner Dienststelle wird das mit Hilfe des APC-Programms geführte Register für die Erteilung von Auskünften an Interessierte darüber, bei welchen Stellen für welche Aufgaben welche Daten gespeichert werden, für die Durchführung von Beratungen und bei der Vorbereitung von Kontrollen genutzt. Wünsche nach Einsicht in das Register sind äußerst selten.

2 Datenschutz im Beitrittsgebiet

2.1 Einigungsvertrag

Mit dem Wirksamwerden des Beitritts, also am 3. Oktober 1990, trat in den neuen Bundesländern das Bundesdatenschutzgesetz vom 27. Januar 1977 mit drei Maßgaben in Kraft (Einigungsvertrag, Anlage I Kapitel II Sachgebiet C Abschnitt III Ziff. 3).

Das neue Bundesdatenschutzgesetz, das erst am 20. Dezember 1990 verkündet wurde, konnte im Einigungsvertrag noch keine Berücksichtigung finden.

Die drei Maßgaben besagten folgendes:

1. Datenschutzkontrolle auch im Bereich der Länder und Gemeinden durch den Bundesbeauftragten für den Datenschutz bis zur Schaffung einer eigenen Datenschutzkontrolle, längstens bis 31. Dezember 1991.

2. Veröffentlichung über die bei Inkrafttreten des Vertrages gespeicherten Daten nach § 12 BDSG (alt) innerhalb eines Jahres.

3. Unverzügliche Löschung aller nicht mehr benötigten oder nach Bundesrecht unzulässig gespeicherten personenbezogenen Daten, wenn schutzwürdige Belange Betroffener nicht entgegenstehen.

Nach Inkrafttreten des neuen Bundesdatenschutzgesetzes, das das Bundesdatenschutzgesetz von 1977 ablöste, stellte sich die Frage, ob die Maßgaben des Einigungsvertrages noch fortgelten.

Zum Teil wurde die Auffassung vertreten (so etwa vom BMI), die Maßgaben des Einigungsvertrages seien durch die Neufassung des BDSG außer Kraft gesetzt worden. Ich habe diese Ansicht für zu weitgehend gehalten.

Ohne Zweifel ist die zweite Maßgabe, die eine nach dem neuen BDSG nicht mehr erforderliche Veröffentlichungspflicht vorsah, mit Inkrafttreten der neuen Vorschriften gegenstandslos geworden.

Die erste Maßgabe (Kontrollbefugnis des Bundesbeauftragten für den Datenschutz bei öffentlichen Stellen der Länder und Gemeinden) galt auch nach Inkrafttreten des neuen BDSG als speziellere Vorschrift fort. Ich habe meine sich daraus ergebende Zuständigkeit als Kontrollorgan im öffentlichen Bereich in den neuen Ländern auch nach Inkrafttreten des neuen BDSG bis zum 31. Dezember wahrgenommen.

Aus verschiedenen konkreten Anlässen war vor allem die dritte Maßgabe, die Löschungsanordnung, Gegenstand kontroverser Diskussionen.

Die Vorschrift, an deren Fassung ich mitgewirkt hatte, ging vom Regelfall der Löschung, d. h. vom Unkenntlichmachen (§ 3 Abs. 5 Nr. 5 BDSG) der nicht mehr gebrauchten oder rechtswidrigen Daten in Dateien aus, sofern nicht ausnahmsweise schutzwürdige Interessen Betroffener am Erhalt der Daten bestehen. Das Konzept ging dahin, daß in den angesprochenen Fällen Löschung die Regel, eine Aufrechterhaltung der Datenspeicherung eher die Ausnahme sei. Tatsächlich ist die Löschung im Sinne dieser Maßgabe des Einigungsvertrages in der Praxis nur selten zum Zuge gekommen.

Dies hatte mehrere Gründe:

— Es stellte sich heraus, daß in einer großen Zahl von Fällen durchaus beachtliche schutzwürdige Belange der Betroffenen der Löschung entgegenstehen, oder wenigstens entgegenstehen können, etwa das Bedürfnis rentenrechtliche Nachweise

oder Zeugnisse über erlittenes Unrecht zu erhalten.

— Die Landesdatenschutzgesetze der neuen Länder haben für Daten, die ihrer Zuständigkeit unterfallen, durchgehend nicht eine Löschung, sondern nur eine Sperrung bis zum Inkrafttreten der neuen Landesarchivgesetze vorgesehen.

— Auch im Bundesbereich wurde aus Gründen der historischen Aufarbeitung der DDR-Vergangenheit die Erhaltung und Archivierung bestimmter Datenbestände gefordert.

— Die Erhaltung mancher Datensammlungen wurde im Interesse wissenschaftlicher Forschung als unabdingbar angesehen.

— Schließlich wurde — vor allem bei manuellen Dateien, deren Inhalt nur zum Teil rechtswidrig ist, zum anderen Teil aber noch benötigt wird — geltend gemacht, der Aufwand für eine partielle Löschung sei zu hoch.

Die aus diesen Gründen praktizierte Umkehr des Regel-Ausnahmeverhältnisses liegt — wie ich mich in jedem Einzelfall überzeugen konnte — sehr häufig im Interesse der betroffenen Bürger, das auch dann zu beachten ist, wenn es sich nur um ein mutmaßliches Interesse handelt. Angesichts der großen zentralen Datenbestände der früheren DDR war es in der Praxis äußerst schwierig, den Betroffenen vor einer Löschung individuell Gelegenheit zu geben, ihre schutzwürdigen Interessen geltend zu machen. Die Behörden der neuen Länder wie auch Bundesbehörden im Beitrittsgebiet haben sich deshalb zu Recht gescheut, durch Löschung von Datenbeständen „vollendete Tatsachen" zu Lasten der Bürger zu schaffen.

Im Bereich der öffentlichen Verwaltung der Länder verdrängten die speziellen Datenschutzvorschriften der neuen Länder für Altdatenbestände, die nur vorläufige Regelung des Einigungsvertrages und damit auch die genannte Maßgabe des Einigungsvertrages zum BDSG (§ 1 Abs. 1 Nr. 2 BDSG).

Im Bundesbereich bleibt die dritte Maßgabe des Einigungsvertrages, die grundsätzliche Löschungsanordnung, gültig. Sie geht als lex specialis der Löschungsregelung des § 20 des neuen BDSG vor. Die Voraussetzungen für eine obligatorische Löschung sind in § 20 Abs. 2 BDSG zwar die gleichen wie im Einigungsvertrag. Das BDSG enthält aber eine Reihe von Gründen, bei deren Vorliegen an die Stelle der Löschung eine Sperrung tritt, die der Einigungsvertrag nicht kennt. Dieser läßt nur die schutzwürdigen Belange der Betroffenen als Grund für ein Absehen von der Löschung gelten. Nach § 20 Abs. 3 BDSG tritt an die Stelle einer Löschung eine Sperrung auch dann, wenn einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen oder wenn eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Dieser erweiterte Katalog für Sperrungsmöglichkeiten gilt im Falle der Altdaten der ehemaligen DDR nicht.

Problematisch war auch die Frage, ob rechtswidrig zustande gekommene Datenbestände archiviert werden können. Dabei bin ich zu folgender Auffassung gelangt: Die Frage, *ob und wann* Daten aus der ehemaligen DDR zu löschen sind, beantwortet der Einigungsvertrag. Das Verfahren jedoch, *wie* gelöscht wird, richtet sich nach dem geltenden BDSG. Das bedeutet: Gemäß § 20 Abs. 8 BDSG i. V. m. § 2 Abs. 1 des Bundesarchivgesetzes sind zu löschende Daten zunächst dem Bundesarchiv anzubieten. Wenn dieses entscheidet, daß es sich um Unterlagen von bleibendem Wert handelt, sind die Bestände zu übergeben. Damit kommt es zwar nicht zu dem vom Wortlaut des Einigungsvertrags verlangten Unkenntlichmachen der Daten. Die Betroffenen, meist Bürger der neuen Bundesländer, können aber sicher sein, daß mit ihren Daten kein Mißbrauch getrieben wird. Archivgut des Bundes, das sich auf natürliche Personen bezieht, unterliegt strengen datenschutzrechtlichen Regelungen; es darf z. B. mit nur wenigen, sehr eng begrenzten Ausnahmen erst dreißig Jahre nach dem Tode der Betroffenen durch Dritte genutzt werden (§ 5 Abs. 2 BArchG).

Eine Archivierung von Datenbeständen, die personenbezogene Daten der in der dritten Maßgabe des Einigungsvertrages angesprochenen Art enthalten, ist also nach Maßgabe des Bundesarchivgesetzes zulässig.

Kontrovers diskutiert wurde die Frage, ob der Datenbestand des Nationalen Krebsregisters (s. u. 2.9) gelöscht werden müsse. Ich habe der vorläufigen Aufbewahrung unter strengen datenschutzrechtlichen Sicherheitsvorkehrungen unter dem Vorbehalt zugestimmt, daß Verarbeitung und Nutzung der in diesem Register enthaltenen empfindlichen Daten durch Gesetz geregelt wird, was inzwischen geschehen ist.

Die Regelung des Einigungsvertrages über die Altdaten der ehemaligen DDR bezieht sich im übrigen nur auf Daten in Dateien, ganz im Sinne des BDSG 1977. Im Berichtszeitraum fragten mehrere Bürger aus der ehemaligen DDR bei mir an, ob vorhandene Akten bei Kommunen, Bezirksbehörden, Volkspolizei oder anderen Institutionen, die auch außerhalb des Stasi-Bereiches belastende Angaben enthalten konnten, an sie herausgegeben oder vernichtet werden können. Leider mußte ich unter Hinweis auf die Rechtslage die Betroffenen enttäuschen, obwohl ich dies in einigen Einzelfällen unbefriedigend fand. Weder die Maßgabe des Einigungsvertrages, der sich eben nur auf Dateien bezieht, noch das neue BDSG geben einen Anspruch auf Herausgabe oder Vernichtung von Akten. Denn § 20 Abs. 5 BDSG schreibt für personenbezogene Daten in Akten allenfalls eine Sperrung vor, und dies auch nur für den Fall, daß ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind. Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur in dem geringen in § 20 Abs. 6 BDSG beschriebenen Umfang übermittelt oder genutzt werden.

Ob ein Folgenbeseitigungsanspruch in besonderen Härtefällen Aussicht auf Erfolg gehabt hätte, ist fraglich. Mir ist kein Fall bekannt geworden, in dem

versucht wurde, ein Vernichtungsverlangen gerichtlich durchzusetzen.

Die Beiträge, die sich schwerpunktmäßig mit dem Datenschutz im Beitrittsgebiet oder mit datenschutzrechtlichen Folgen der deutschen Einheit befassen, sind im Abschnitt 2 dieses Berichtes zusammengefaßt. Einzelne Aspekte des Datenschutzes im Beitrittsgebiet finden sich aber, wegen des Zusammenhangs auch in anderen Teilen (s. u. z. B. 4.5.3 und 11.2).

2.2 Abwicklung des Zentralen Einwohnerregisters (ZER)

Über das Zentrale Einwohnerregister (ZER), insbesondere seine Entwicklung und Rolle in der ehemaligen DDR, habe ich in meinem 13. Tätigkeitsbericht (S. 26ff.) bereits ausführlich berichtet. Nach dem Einigungsvertrag war ich bis zum 31. Dezember 1991 für die datenschutzrechtliche Kontrolle des ZER zuständig. Danach ging diese Verantwortung auf die Datenschutzbeauftragten der neuen Bundesländer und Berlins über.

Die fachliche Verantwortung für das ZER lag seit der Vereinigung bei den Innenministerien der neuen Bundesländer und dem Innensenator von Berlin. Bei der Abwicklung des ZER zum 31. Dezember 1992 ergaben sich einige organisatorische und technische Probleme. Eine Ursache ergab sich daraus, daß das Rechenzentrum, in dem das ZER seine Daten verarbeiten ließ, zu DDR-Zeiten eine eigene gleichwertige Dienststelle des Ministeriums des Innern war, also kein Teil des früheren Büros für Personendaten, aus dem sich das ZER entwickelt hat. Dieses Rechenzentrum hat das Ministerium des Innern der ehemaligen DDR auch noch bei vielen anderen Aufgaben unterstützt. Diese anderen Aufgaben, die sog. Projekte, wurden nach meiner Kenntnis zum Teil noch bis Ende 1990 fortgeführt und die damit zusammenhängenden Daten und Programme im Rechenzentrum archiviert. Das Rechenzentrum war einige Zeit als eigene organisatorische Einheit im Organigramm der Außenstelle des BMI ausgewiesen. Da es aus der Sicht des Bundes jedoch notwendiger Teil für die Aufgabenerfüllung des ZER war, wurde es schließlich dem ZER zugeschlagen und kam somit auch unter die Verantwortung der Innenministerien der neuen Länder und des Senators für Inneres von Berlin.

Während meiner Zuständigkeit für das ZER wurde ein Teil meiner Empfehlungen umgesetzt, einige Empfehlungen blieben aufgrund der Personalsituation im ZER ohne Folge (s. auch 13. TB S. 27). Die Löschung von Daten im ZER habe ich nicht in allen Fällen forciert, da ich nicht abschließend beurteilen konnte, ob diese Daten wirklich nicht für andere Fachbereichsverwaltungen von Bedeutung sind (z. B. erteilte Erlaubnisse über Waffen, Gift oder Sprengstoff). Auch zeichnete sich bald ab, daß die Probleme der Rehabilitation von ehemaligen DDR-Bürgern oder die der Strafverfolgung vielschichtiger waren, als bei Abschluß des Einigungsvertrages angenommen. So bin ich aus heutiger Sicht froh, daß die Personenkennzahlen aus dem Meldedatenbestand des ZER nicht gelöscht und durch ein anderes Ordnungsmerkmal ersetzt wurden.

Die eigentliche Abwicklung des ZER wurde 1992 von den Innenministerien der neuen Länder durchgeführt, wobei sie von den Landesbeauftragten für den Datenschutz unterstützt wurden. Die faktische Federführung lag beim Innenministerium Brandenburg und die für den Datenschutz beim Landesbeauftragten für den Datenschutz von Brandenburg. In einer Entschließung der Landesbeauftragten für den Datenschutz von Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen und Sachsen-Anhalt sowie des Innenministeriums Thüringen vom 25. September 1992, an der ich beteiligt war, wurde den für das ZER verantwortlichen Bundesländern empfohlen, eine Abwicklungsstelle einzurichten, die für eine sichere Auflösung des ZER und des Rechenzentrums sorgen sollte. Dies ist leider wohl deshalb nicht geschehen, weil der Betrieb des ZER bereits am 15. Oktober 1992 eingestellt wurde.

Die Innenministerien haben sich vor allem für eine schnelle Überleitung der Meldedaten in örtliche Melderegister eingesetzt. Diese Überführung war im Oktober 1992 abgeschlossen; die Frist des Einigungsvertrages — 31. Dezember 1992 — wurde also gewahrt. Die archivierten Projektdaten aus dem Rechenzentrum wurden weit überwiegend dem Bundesarchiv übergeben. Dazu gehören so wichtige Datenbestände wie „Bestand der Inhaftierten", „Statistische Berichterstattung über den Arbeitseinsatz Strafgefangener" oder „Strafgefangenen- und Verhaftetendatei", aber auch der Datenbestand „Ordnungswidrigkeiten im Transitverkehr". Die Kriminalstatistik ist in Absprache mit den neuen Bundesländern an das Landeskriminalamt Sachsen abgegeben worden. Auch hier stand im Vordergrund, daß diese Datenbestände insbesondere noch für Rehabilitationsverfahren gebraucht werden könnten.

Problematisch ist, ob die maschinell lesbaren Datenträger überhaupt noch gelesen werden können: Die Daten sind seit Ende 1990 nicht mehr gepflegt, die Datenträger zum Teil unsachgemäß behandelt worden und die verwendete ESER-Technik (mit bulgarischen Plattenlaufwerken) steht voraussichtlich in Kürze nirgendwo mehr zur Verfügung. Auch gibt es nicht für alle Projekte brauchbare Beschreibungen, so daß verwendete Schlüsselungen dann nicht mehr „übersetzt", also in einen Klartext gebracht werden können. Gleichwohl halte ich es für richtig, die Projektdaten vorerst zu archivieren und erst in einigen Jahren über ihre weitere Aufbewahrung zu befinden. Der eigentliche Meldedatenbestand des ZER wurde nach meinen Informationen Anfang 1993 gelöscht.

2.2.1 Die Personenkennzahl

Im Einigungsvertrag ist vorgesehen, daß sämtliche Dateien im Beitrittsgebiet, die nach Personenkennzahlen geordnet sind, unverzüglich nach anderen Merkmalen umzuordnen sind. Die Personenkennzahlen müssen in allen Dateien zum frühestmöglichen Zeitpunkt gelöscht werden. Diese Forderung läßt sich nicht in jedem Falle buchstabengetreu umsetzen.

Insbesondere der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) benötigt die PKZ für die *eindeutige Identifizierung* von Betroffenen und für die *eindeutige Zuordnung von Unterlagen zu Personen.* Solange das ZER existierte, hat der BStU dort mit Hilfe von Personenkennzahlen angefragt und das ZER hat jeweils zum PKZ die benötigten Daten, vor allem Name und Anschrift, ergänzt. Das war aus meiner Sicht rechtlich zulässig. Um den BStU bei seiner Aufgabenerfüllung weiterhin unterstützen zu können, war es notwendig, vor Abwicklung des ZER einen verkürzten Meldedatenbestand aus dem eigentlichen Meldedatenbestand zu erzeugen, der folgende Daten umfaßt:

— PKZ

— Name (auch frühere), Vorname(n)

— Geburtsname, sonstige Namen

— Geburtsort

— letzte Anschrift

— Merkmal „verstorben".

Diese „PKZ-Datei" wurde erstellt und war bei Redaktionsschluß nach meinen Informationen noch — technisch gesichert — im Gebäude des ehemaligen ZER, einschließlich der Technik, die notwendig ist, damit diese Daten vom BStU genützt werden könne.

Zusammen mit dem Innenausschuß des Deutschen Bundestages und dem BMI bin ich der Auffassung, daß die Weitergabe der Daten aus dieser Datei an den BStU durch die Vorschriften des Einigungsvertrages gedeckt ist (s. u. 4.4.2). Rechtlich anders beurteilen die neuen Länder einschließlich der Landesbeauftragten für den Datenschutz die Zulässigkeit der Erstellung dieser PKZ-Datei und der Zurverfügungstellung dieser Datei an den BStU. Die Landesbeauftragten für den Datenschutz der neuen Länder und der Berliner Datenschutzbeauftragte fordern eine entsprechende Ergänzung des StasiUnterlagen-Gesetzes (StUG). Trotz meiner anderen Interpretation des Einigungsvertrages halte auch ich eine entsprechende Klarstellung im StUG für wünschenswert.

Ein Problem könnte werden, daß auch andere Stellen als der BStU diese PKZ-Datei nutzen wollen, z. B. die Zentrale Ermittlungsstelle von Regierungs- und Vereinigungskriminalität — ZERV — oder die BAfAM (s. u. 2.6.2) oder die ZEBWis (s. u. 2.6.3). Es liefe allerdings der Intention des Einigungsvertrages völlig zuwider, die PKZ nur aus Gründen der Praktikabilität „retten" zu wollen.

2.3 Datenspeicher „Gesellschaftliches Arbeitsvermögen der DDR" jetzt im Bundesarchiv

Der Datenspeicher „Gesellschaftliches Arbeitsvermögen der DDR" enthielt personenbezogene Daten über die Erwerbstätigen in der ehemaligen DDR (s. auch 13. TB S. 35).

Erfaßt waren Daten von Arbeitern und Angestellten, von berufstätigen Mitgliedern der Produktionsgenossenschaften und Rechtsanwaltskollegien, von Lehrlingen, Rentnern und handwerklich Beschäftigten, soweit letztere in Produktionsgenossenschaften tätig waren, sowie von Werktätigen, die Wehrdienst ableisteten. Nicht erfaßt waren vor allem die Daten von Selbständigen sowie von den bei ihnen Beschäftigten und von Mitarbeitern der Staatsorgane, insbesondere der Staatssicherheit, der Zollverwaltung und der Nationalen Verteidigung, von hauptamtlichen Mitarbeitern der Parteien und Massenorganisationen sowie ihrer Betriebe. Insgesamt waren die Daten von rd. 7,25 Mio. Berufstätigen der ehemaligen DDR erfaßt. Der umfangreiche Merkmalskatalog des Datenspeichers enthielt u. a. folgende Angaben: Personenkennzahl, Namen, Familienstand, Hauptwohnort, Anzahl der Kinder, Anzahl der pflegebedürftigen Familienangehörigen, Grad des Körperschadens, Rentenart, Rehabilitand, Schulbildung, ständiger Arbeits-/Ausbildungsort, Abbruch des Lehrverhältnisses mit Grund und Datum, Abgang vom Arbeitsplatz mit Grund, Datum und Form, Freistellung von der Arbeit.

Aufgrund der mangelnden Kapazität des zuständigen Rechenzentrums wurde jeweils nur der aktuelle Stichtagsdatenbestand gespeichert. Die Stichtagsdatenbestände vor dem 31. Dezember 1989 waren, soweit bekannt, gelöscht worden.

Eine zentrale Zusammenstellung derartiger personenbezogener Daten von Arbeitnehmern ist nach unserem Rechtsverständnis unzulässig.

Nach dem Einigungsvertrag habe ich deshalb auch zunächst die Löschung des Datenbestandes gefordert. Da die Datei allerdings von sozialhistorischem Interesse ist, habe ich in Auslegung des § 20 Abs. 8 BDSG schließlich einer Archivierung im Bundesarchiv zugestimmt (s. hierzu auch 2.1). Die in der Datei enthaltenen Angaben können im übrigen noch im Zusammenhang mit rentenrechtlichen oder anderen Nachweisen für Bürger hilfreich sein. Somit standen auch die mutmaßlichen Interessen Betroffener einer Löschung entgegen.

Die Datei „Gesellschaftliches Arbeitsvermögen" wurde im November 1991 an das Bundesarchiv abgegeben. Bis Redaktionsschluß war das Bundesarchiv allerdings wegen technischer Schwierigkeiten noch nicht in der Lage, die gespeicherten Informationen zu lesen und auszuwerten. Eine Nutzung der Datei für Auskünfte an Betroffene oder — in anonymisierter Form — für wissenschaftliche Zwecke wird aus diesem Grunde voraussichtlich nicht vor 1994 möglich sein.

2.4 Die Gesundheitsunterlagen aus der Urangewinnung SDAG Wismut — ein komplexes Datenschutzproblem —

Ein Industriegigant mit dem eher verschleiernden Namen Sowjetisch-Deutsche Aktiengesellschaft Wismut (SDAG Wismut) beutete nach 1945 die Uranerzvorkommen im östlichen Thüringen und im südlichen

Sachsen (Erzgebirge) aus. Aufgrund des Abkommens zwischen der Bundesrepublik Deutschland und der früheren UDSSR vom 16. Mai 1991 hat die SDAG Wismut zum 1. Januar 1991 ihre Tätigkeit eingestellt; der sowjetische Aktienanteil wurde unentgeltlich auf die deutsche Seite übertragen. Für die Stillegung und Abwicklung der Wismut-Bergbaubetriebe sowie die Sanierung und Rekultivierung der Bergbaulasten wurde die Wismut GmbH gegründet, die sich im alleinigen Bundesbesitz befindet. Diese GmbH ist im Besitz der Datenbestände der früheren SDAG Wismut, zu denen auch umfangreiche Sammlungen von Gesundheitsdaten gehören, die wegen der hohen Strahlenbelastung, der sowohl Mitarbeiter der SDAG Wismut als auch die Bevölkerung der gesamten Region ausgesetzt waren, auch heute noch von erheblicher Bedeutung sind, z. B. für Entschädigungsfragen und für Forschungsvorhaben.

Das Gesundheitswesen in der früheren SDAG Wismut war Teil des Gesundheitswesens der ehemaligen DDR mit einem besonderen regionalen Zuständigkeitsbereich nicht nur für die SDAG Wismut, sondern auch für die Bevölkerung im örtlichen Wirkungskreis der Wismut. Trotz der formalen Trennung von der SDAG Wismut nutzten die für diese zuständigen Gesundheitseinrichtungen Gebäude des Unternehmens. Das Gesundheitswesen Wismut verwaltete zuletzt Gesundheitsunterlagen von ca. 1 000 000 Personen, darunter z. B. die Daten aus ca. 40 000 Vorsorgeuntersuchungen, die noch 1989 durchgeführt worden waren. Etwa 40 % der Unterlagen betrafen Personen, die bei der SDAG Wismut beschäftigt waren. Die übrigen betrafen Familienangehörige sowie andere Personen, die das Gesundheitswesen Wismut nutzen konnten, bis ab 1990 die Einrichtungen unter der letzten DDR-Regierung abgewickelt wurden.

In den ersten Auflösungswirren der Wendezeit nahmen Ärzte der früheren Wismut-Polikliniken teils Unterlagen für ihre privatärztliche Tätigkeit mit. Teilweise händigten die Kliniken den Patienten deren Gesundheitsunterlagen mit dem Hinweis aus, sie könnten diese dem weiterbehandelnden Arzt zur Verfügung stellen. Im November 1990 hat die Generaldirektion der damaligen SDAG Wismut die Sicherung der Gesundheitsdaten ihrer früheren Mitarbeiter in ihre Hände genommen und eine Abteilung Gesundheitsdatensicherung als eigene Organisationseinheit gebildet, die nunmehr als Teil der Wismut GmbH weitergeführt wird.

Bei den vorhandenen Unterlagen ist zu unterscheiden zwischen:

— Daten von Polikliniken der Hauptstandorte der SDAG Wismut,

— Daten von Krankenhäusern und Sanatorien, die der Rehabilitation dienten,

— Daten aus arbeitsmedizinischen Vorsorgeuntersuchungen und Unterlagen der ehemaligen Betriebsambulatorien sowie aus den Ergebnissen von Röntgenreihenuntersuchungen,

— Befunde und Gutachten zur Entscheidung in Berufskrankheits-Verdachtsfällen.

Über die weitere Aufbewahrung und Verwaltung der Unterlagen habe ich Gespräche mit der Geschäftsleitung der Wismut GmbH sowie mit den beteiligten Bundesministerien für Wirtschaft, für Arbeit und Sozialordnung sowie für Umwelt, Naturschutz und Reaktorsicherheit geführt. Es bestand Einvernehmen, daß folgende Gesichtspunkte beachtet werden mußten:

— Die Gesundheitsdaten müssen bei Bedarf für den Patienten erreichbar sein.

  Deshalb wurden die Unterlagen in den weitergeführten Einrichtungen belassen, auch wenn die Trägerschaft gewechselt hatte. Daten aus nicht weitergeführten Einrichtungen hat die Abteilung Gesundheitsdatensicherung der Wismut GmbH übernommen. Kopien werden mit Einwilligung der Betroffenen an weiterbehandelnde Ärzte herausgegeben.

— Die betriebsbezogenen Daten müssen im Rahmen der Weiterbeschäftigung eines früheren Wismut-Mitarbeiters verfügbar sein.

  Dazu werden dem neu eingerichteten Berufsgenossenschaftlichen Arbeitsmedizinischen Dienst (BAD) die für ihn relevanten Teile aus den Betriebsambulatorien zur Verfügung gestellt.

— Die Berufsgenossenschaften benötigen Unterlagen für die Prüfung, welche bisher nicht als Folgen von Berufskrankheiten anerkannten Schäden nach neuem Recht anzuerkennen sind.

  Dazu müssen Ablehnungsfälle und neue Antragsfälle geprüft werden, wozu die arbeitsmedizinische Vorgeschichte gebraucht wird.

— Die Berufsgenossenschaften benötigen Daten zur nachgehenden Untersuchung und Betreuung gesundheitlich belasteter und möglicherweise geschädigter Mitarbeiter.

  Dazu ist im Frühjahr 1992 eine besondere Aktion zur Erfassung der Personaldaten durch die Zentrale Erfassungs- und Betreuungsstelle Wismut (ZEBWis) angelaufen (s. u. 2.6.3).

— Wesentliche Teile des Datenbestandes sind für Forschungsvorhaben über Strahlenschäden, insbesondere über den Zusammenhang zwischen Erkrankungen an Krebs und Belastungen durch Radioaktivität und Staub, von erheblicher Bedeutung.

Für die unter den letzten drei Punkten genannten Zwecke sind neben den Gesundheitsdaten auch die Personalunterlagen von ehemaligen Mitarbeitern der SDAG Wismut wichtig, soweit sie Angaben zur Beschäftigung und damit zur Belastung insbesondere durch Radon, Staub und Vibration enthalten.

Die Übernahme der Gesundheitsdaten durch die Wismut GmbH habe ich als einen richtigen Schritt ausdrücklich begrüßt. Dies gilt sowohl für die Akten aus den Gutachten-Bereichen als auch für die Unterlagen aus den Betriebsambulatorien, den Krankenhäusern und Polikliniken, soweit dort keine andere, sachgerechte Weiterführung der Patientenunterlagen gewährleistet werden kann. Im Interesse der Patienten habe ich es auch begrüßt, daß Unterlagen über kurative Behandlungen aus aufgelösten Einrichtun-

gen mit Einwilligung des Betroffenen weiterbehandelnden Ärzten in Kopie zur Verfügung gestellt werden. Ich konnte feststellen, daß die Unterlagen in der Abteilung Gesundheitsdatensicherung in Chemnitz angemessen gesichert sind. Dies gilt allerdings nicht für alle Stellen, die ehemalige Gesundheitsdaten aus dem Bereich Wismut verwahren. Die Wismut GmbH hat anläßlich meiner Kontrolle zugesagt, die erkannten Datensicherungsmängel so schnell wie möglich zu beseitigen.

Gegen Bestrebungen des Bundesministeriums für Wirtschaft, die gesamten Gesundheitsunterlagen des früheren Gesundheitswesens der SDAG Wismut dem Hauptverband der gewerblichen Berufsgenossenschaften (HVBG) zu überlassen, habe ich mich gewandt, weil dies der Verantwortung der Wismut GmbH für die Gesundheitsdaten der ehemaligen Mitarbeiter nicht entsprochen hätte. Die pauschale Übergabe dieser Unterlagen an den HVBG wäre rechtlich unzulässig gewesen.

Nachhaltig habe ich mich auch dafür eingesetzt, bei den notwendigen Forschungsvorhaben die Rechte der Betroffenen zu beachten. Das Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, in dessen Zuständigkeitsbereich bereits Forschungsvorhaben angemeldet wurden, habe ich gebeten, mich bei der Planung jeweils zu beteiligen.

Inzwischen erkennt die Wismut GmbH es nicht mehr als ihre Aufgabe an, Gesundheitsdaten, an denen ein Firmeninteresse nicht besteht, noch weiterhin zu verwalten. Solange es nicht gelingt, eine die Rechte der Betroffenen wahrende Lösung außerhalb der Wismut GmbH zu finden, muß sie diese Abwicklungsaufgabe aber als Rechtsnachfolgerin der SDAG Wismut weiterhin selbst wahrnehmen.

2.5 Kaderakten der Nomenklatura nicht auffindbar

— Personaldatenrechtliche Probleme aufgrund der Vereinigung —

Nach meinen Erkenntnissen sind für den Umgang mit Personaldaten in den neuen Bundesländern vor allem folgende Fragen von großer Bedeutung:

— Überprüfung der Verfassungstreue bei Bewerbern und bei Mitarbeitern, die in den öffentlichen Dienst übernommen werden wollen,

— Behandlung von Kaderakten und von Zweitakten der Kaderakten (Personalakten in der ehemaligen DDR)

Es ist leider nicht gelungen, Inhalt und Verfahren der Überprüfung der *Verfassungstreue* von Bewerbern aus dem Beitrittsgebiet einheitlich für Bund und Länder zu regeln. Auch hat der Bundesminister des Innern seinen Personalfragebogen, den einige oberste Bundesbehörden und viele Behörden der neuen Länder inzwischen als Muster zur Gestaltung ihrer eigenen Fragebögen übernommen haben, trotz meiner Bedenken (s. 13. TB S. 25) unverändert beibehalten. Er hat auch die Gegenvorschläge der Bundesregierung in deren Stellungnahme zu meinem Tätigkeitsbericht nicht verwirklicht.

Bei der Überprüfung der Verfassungstreue sind Fragen, die sich auf die Mitarbeit beim Ministerium für Staatssicherheit oder beim Amt für nationale Sicherheit sowie auf Funktionen in der SED, in Massenorganisationen/gesellschaftlichen Organisationen der DDR oder sonstigen herausgehobenen Funktionen im System der DDR erstrecken, unbedenklich; sie sind auf die Vorgaben des Einigungsvertrages abgestellt.

Beim Aufbau von Dienststellen im Beitrittsgebiet kann wegen des erheblichen Arbeitsaufwandes und des Zeitdruckes bei der Entscheidung über Einstellungen von Bewerbern aber wohl auch auf sensiblere Fragen, die eine Plausibilitätskontrolle der Antworten zu anderen Fragen zulassen, derzeit noch nicht verzichtet werden. Ich würde es allerdings begrüßen, wenn Fragen zur Verfassungstreue von Bewerbern erst in der zweiten Phase des Einstellungsverfahrens (vgl. hierzu 9.6) und abhängig von der angestrebten Funktion erörtert würden. Kommt nämlich ein Bewerber wegen fehlender persönlicher und fachlicher Qualifikation sowieso nicht in die engere Wahl für die angestrebte Stelle, ist auch die Antwort auf die oben angegebenen Fragen nicht mehr von Belang.

Ich halte auch eine Trennung besonders sensibler Daten, — die Daten aus der Verfassungstreueprüfung sind solche — zumal wenn auf sie nach Begründung des Dienstverhältnisses in aller Regel nicht mehr zurückgegriffen wird, von anderen Personaldaten für erforderlich.

Diese Trennung könnte auch in der Form erfolgen, die die Bundesregierung in ihrer Stellungnahme zu meinem 13. Tätigkeitsbericht selbst vorgeschlagen hat, daß nämlich Auskünfte zur Verfassungstreue, insbesondere solche des Bundesbeauftragten für die Unterlagen des ehemaligen MfS, in Teilakten zur Personalakte genommen und — vergleichbar wie ärztliche Gutachten — in einem verschlossenen Umschlag verwahrt werden. Wenn dies geschieht, sollten allerdings nicht nur Auskünfte über den Bediensteten, sondern auch dessen eigene Angaben zur Verfassungstreue in die verschlossene Teilakte genommen werden. Ein solches Verfahren setzt aber die Erhebung der Daten zur Verfassungstreue auf einem besonderen, von dem sonstigen Bewerbungsbogen oder dem Personalbogen getrennten Vordruck voraus. Ich empfehle daher nach wie vor dringend die Erhebung der Daten zur Verfassungstreue auf einem besonderen Vordruck.

Einschlägige Informationen gaben mir Veranlassung, dem Verbleib der Kaderakten des öffentlichen Dienstes der ehemaligen DDR nachzugehen.

Die Kaderakten (jetzt Personalakten) von Mitarbeitern, die vom BMI aus dem MdI der ehemaligen DDR übernommen wurden, werden in Bonn weitergeführt, die der nicht übernommenen befinden sich im Personalakten-/Kaderaktenarchiv in Berlin. Ein Teil der ehemaligen Kaderakten ist aufgrund organisatorischer Zuordnung bestimmter Dienstzweige zu Ländereinrichtungen an die entsprechenden Dienststellen der Länder abgegeben worden. Nach Auflösung der DDR-Ministerien für Kultur, Medienpolitik, für regionale, kommunale Angelegenheiten und für

Familie, Jugend und Sport hat das BMI außerdem die bei diesen vorhandenen Bestände an Kaderakten und sonstigen Personalunterlagen aller ehemaligen Mitarbeiter übernommen.

Die Kaderakten der sogenannten Nomenklaturkader (leitende Mitarbeiter vom Abteilungsleiter aufwärts) und des Kollegiums (oberstes Führungsorgan des Ministers) wurden in der ehemaligen DDR im Ministerbereich geführt. Wer für die Aktenführung verantwortlich war und wo diese Akten aufbewahrt wurden, unterlag auch ministeriumsintern strikter Geheimhaltung. Den Verbleib dieser Akten konnte ich bislang nicht klären.

Die noch vorhandenen Akten sind zu einem großen Teil allerdings nicht mehr vollständig, weil viele Mitarbeiter von der „Modrow-Verordnung" vom Februar 1990 Gebrauch gemacht und ihre Kaderakten „bereinigt" haben. Mir ist bekannt, daß auch einige Dienststellenleiter diese Bereinigung von Kaderakten bereits von sich aus vorgenommen hatten, bevor die Akten einzelnen Betroffen ausgehändigt wurden. Ebenso soll es vorgekommen sein, daß einzelne Betroffene, über das Ziel der Modrow-Verordnung hinaus, der Personalakte alles entnommen haben, was aus ihrer Sicht für sie nachteilig hätte werden können. Die stichprobenweise Durchsicht von Kaderakten bei einem Hauptzollamt ergab dagegen, daß dort die Kaderakten nahezu vollständig waren.

Mehrfach habe ich Hinweise bekommen, in der ehemaligen DDR seien — jedenfalls beim ehemaligen Ministerium des Innern — Kaderakten mindestens doppelt geführt worden. Nach meinen bisherigen Feststellungen, auch aufgrund übereinstimmender Angaben aller befragten Mitarbeiter der BMI — Außenstelle Berlin, kann ich dies für das ehemalige MdI bisher nicht bestätigen. Dennoch besteht Anlaß, dieser Frage weiter nachzugehen. Mir ist nämlich bekannt geworden, daß in der ehemaligen DDR Personalbögen in doppelter, Attestationen (dienstliche Beurteilungen) in dreifacher und Disziplinarvorgänge in sechsfacher Ausfertigung auszufüllen waren. Der Verbleib der Mehrfertigungen ist noch nicht geklärt. Die ehemaligen Mitarbeiter der Personalverwaltung sind seinerzeit davon ausgegangen, daß zumindest eine Ausfertigung an das Ministerium für Staatssicherheit (MfS) ging. Nach Auffassung der von mir um Auskunft gebetenen Mitarbeiter ist deshalb denkbar, daß der eingangs beschriebenen Annahme eine Verwechselung mit den beim MfS geführten Zweit-Personalakten zugrunde liegt; dies liegt deshalb nahe, weil das MfS in seinen Aktivitäten nach außen unter der Bezeichnung MdI in Erscheinung getreten ist. Ein weiteres Indiz dafür ist auch die Auskunft eines Mitarbeiters, es sei zu DDR-Zeiten unter anderem seine Aufgabe gewesen, dem MfS regelmäßig Blankoexemplare von MdI-Dienstausweisen zu übersenden.

Bei einer stichprobenweisen Einsicht konnte ich weder in den Suchkarteien, in der Hängeregistratur und in der Kaderkartei, noch in den vorgefundenen Archivakten Anhaltspunkte für eine doppelte Kaderaktenführung im ehemaligen MdI feststellen. Gespräche mit meinen Kollegen aus den neuen Bundesländern haben allerdings weitere Anhaltspunkte für die Führung von weiteren Personalunterlagen gebracht. So sollen bei Behörden in den neuen Bundesländern noch Magnetbänder vorhanden sein, auf denen sich Personaldaten von Arbeitnehmern befinden. Ich werde diesen Hinweisen weiterhin nachgehen.

Zur Vermeidung von Zweifeln weise ich darauf hin, daß es sich bei den möglicherweise noch vorhandenen Mehrfachpersonalakten oder -dateien nicht um den Datenspeicher „gesellschaftliches Arbeitsvermögen" handelt, der sich inzwischen im Bundesarchiv befindet (s. o. 2.3).

Bei Kontrollen in personalbearbeitenden Stellen werde ich häufig mit der Frage der *weiteren Verwendung und des Verbleibs von Kaderakten* der in den Dienst des Bundes übernommenen und der zwischenzeitlich ausgeschiedenen Mitarbeiter der ehemaligen DDR-Dienststellen konfrontiert.

Der Umgang mit Kaderakten wird innerhalb der Bundesregierung derzeit unterschiedlich gehandhabt. In einer Dienststelle im Geschäftsbereich des BMWi werden die Kaderakten — mit Zustimmung der Betroffenen — als besondere Teile Bestandteil der Personalhauptakte. Im Geschäftsbereich des Bundesministeriums der Finanzen werden aufgrund eines entsprechenden Erlasses aus der Kaderakte nur die Personenstandsurkunden und die Beschäftigungsnachweise in die aktuelle Personalakte übernommen. Die Kaderakte selbst wird als „Vorakte" gesondert abgelegt.

Die beschriebene Praxis im Umgang mit den Kaderakten durch öffentliche Stellen des Bundes begegnet erheblichen datenschutzrechtlichen Bedenken. Gegen die uneingeschränkte Einbeziehung der Kaderakte in die Personalhauptakte spricht vor allem, daß die ersteren eine Reihe von Daten enthalten, die zur Aufgabenerfüllung der Personalverwaltung des Bundes nicht erforderlich sind oder deren Erforderlichkeit zumindest fraglich ist und deren Erhebung nach Bundesrecht weitgehend unzulässig gewesen wäre. Als Beispiel möchte ich hier nur die Angaben über „soziale Herkunft", „soziale Stellung", „Parteimitgliedschaft mit Eintrittsjahr", „Vereinsmitgliedschaften", „Verwandte ersten und zweiten Grades im kapitalistischen Ausland/Westberlin", „Eltern mit Angabe über Parteizugehörigeit", „Geschwister mit Angabe ihrer Parteizugehörigkeit", „Lehrgänge bei Parteischulen" und „Angaben über Auszeichnungen" nennen.

Überzeugende Gründe für eine Übernahme der gesamten Kaderakte — also über die auf der Grundlage des § 90 BBG in die neue Personalakte übernommenen Bestandteile hinaus — sind nicht ersichtlich. Einerseits wird das Argument vorgebracht, daß Kaderakten bis zur Anerkennung von Vordienstzeiten und zur endgültigen Klärung von Fragen der Eingruppierung erforderlich seien. Andererseits — so die Argumentation des Bundesministeriums der Finanzen — seien Hinweise aus dem früheren sozialen Umfeld der Beschäftigten zur Wahrung berechtigter, schutzwürdiger Interessen der Betroffenen regelmäßig dann notwendig, wenn — wie im Bereich der Zollverwaltung geschehen — Bedienstete unter Hinweis auf entsprechende Vermerke in der Kaderakte

eine Rehabilitierung verlangen. Dieses Ziel wäre m. E. auch zu erreichen, wenn den Betroffenen die nicht mehr benötigen Unterlagen ausgehändigt würden. Der ebenfalls geäußerte Wunsch, die Kaderakte für das Verfahren zur Überprüfung der Verfassungstreue aufzubewahren, ist nur für die Dauer dieses Verfahrens begründet. Soweit Unterlagen aus den Kaderakten wirklich für die Prüfung der Verfassungstreue relevant sind, müßten sie zumindest in eine Teilakte „Verfassungstreue" genommen werden. Soweit ehemalige Arbeitnehmer der DDR zu Bundesbeamten ernannt worden sind, gelten für die Führung ihrer Personalakten die §§ 90ff BBG, somit auch § 90 Abs. 4 BBG, der bestimmt, daß der Dienstherr personenbezogene Daten über Bewerber und Beamte nur erheben darf, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen erforderlich ist. Soweit ehemalige Mitarbeiter der DDR als Beamte übernommen werden, dürfen daher nur solche Daten aus der ehemaligen Kaderakte übernommen werden. Bei der Beschäftigung als Angestellter oder Arbeiter im Bundesdienst gelten nach Arbeitsrecht die gleichen Grundsätze.

Die Behandlung von Kaderakten der ehemaligen DDR-Betriebe seitens der Treuhandanstalt bezüglich der Liquidation, des Verkaufs und des Konkurses dieser Betriebe wird in anderem Zusammenhang dargestellt (s. u. 2.12).

2.6 Schutz von Sozialdaten — Probleme beim Umgang mit ihnen —

Es kann nicht verwundern, daß die deutsche Einheit auch beim Schutz von Sozialdaten eine Reihe besonderer Fragen aufgeworfen hat, die teilweise Auswirkungen bis in das Gebiet der früheren Bundesrepublik Deutschland hinein hatten.

Als Beispiele nenne ich

— die ordnungsgemäße Unterbringung aus der ehemaligen DDR übernommener Akten mit Sozialdaten

— den Datenschutz bei der Bundesanstalt für Arbeitsmedizin (BAfAM)

— die Schaffung einer Zentralen Erfassungs- und Betreuungsstelle bei der Wismut GmbH i. A.

— die Datenerhebung im Rahmen des Anspruchs- und Anwartschaftsüberführungs-Gesetzes (AAÜG).

2.6.1 Übernommene Akten nicht ordnungsgemäß gesichert

Bei der Kontrolle der Bezirksverwaltung einer Berufsgenossenschaft im früheren Bundesgebiet habe ich festgestellt, daß in den Fluren des Dienstgebäudes zahlreiche Akten mit Sozialdaten gelagert waren. Eine Sicherung der Akten gab es lediglich dadurch, daß die Zwischentüren zu den betreffenden Fluren nach Dienstschluß verschlossen wurden. Besucher des in demselben Gebäude untergebrachten berufsgenossenschaftlichen arbeitsmedizinischen Dienstes konnten sich jedoch im Gebäude frei bewegen und auf die Akten zugreifen.

Diese Situation war dadurch veranlaßt worden, daß der Hauptverband der gewerblichen Berufsgenossenschaften e. V. aufgrund des Einigungsvertrages einen Verteilungsschlüssel für aus dem Beitrittsgebiet zu übernehmende Akten über Arbeitsunfälle/Berufserkrankungen erstellt und der kontrollierten Bezirksverwaltung ca. 25 000 Akten aus der ehemaligen DDR zugewiesen hatte. Infolge der Raummnot der Bezirksverwaltung mußten Akten vorübergehend nicht hinreichend gesichert auf den Fluren des Gebäudes in den verschiedenen Sitzungszimmern untergebracht werden.

Die Berufsgenossenschaft sagte bei der Kontrolle zu, Stahlschränke zur Aufnahme der Akten bis zum Umzug in erweiterte Büroräume zu beschaffen und das Volumen ihrer eigenen Altakten durch Vernichtung nicht mehr benötigter Unterlagen zu reduzieren.

Bei einer Nachkontrolle mußte ich jedoch feststellen, daß die dargestellten Mängel teilweise noch fortbestanden und neue Mängel hinzugetreten waren.

Daraufhin habe ich die unzureichende Sicherung der Akten mit Sozialdaten als Verstoß gegen die Pflicht zur Wahrung des Sozialgeheimnisses, sowie gegen die Verpflichtung zu technischen und organisatorischen Maßnahmen zur Sicherung der Daten (§ 35 SGB I, § 9 BDSG) beanstandet.

Die Berufsgenossenschaft hat die Mängel inzwischen behoben.

Da ich annehmen mußte, daß auch bei anderen Berufsgenossenschaften ähnliche Schwierigkeiten aufgetreten waren, habe ich die meiner Kontrollbefugnis unterliegenden Berufsgenossenschaften aufgefordert, mir über die Aufbewahrung übernommener Gesundheitsunterlagen und dabei aufgetretene Schwierigkeiten zu berichten.

Bei einigen Berufsgenossenschaften — drei weitere habe ich mit ähnlichem Schwerpunkt kontrolliert — zeigten sich leider ähnliche Schwierigkeiten, die aber inzwischen überwunden sind.

2.6.2 Bundesanstalt für Arbeitsmedizin hat arbeitsmedizinische Daten übernommen

Die Bundesanstalt für Arbeitsmedizin (BAfAM) hat die Datenbestände des früheren Zentralinstitutes für Arbeitsmedizin der ehemaligen DDR übernommen.

Die von der BAfAM weitergeführten Dateien und Akten enthalten oft als einziges Identifikationsmerkmal die Personenkennzahl (PKZ) des Betroffenen, die aber nach dem Einigungsvertrag in allen Dateien zum frühestmöglichen Zeitpunkt zu löschen ist. Dieser Zeitpunkt ist aber nicht erreicht, solange die Speicherung der PKZ noch erforderlich ist, z. B. weil schutzwürdige Interessen der Betroffenen an der Nutzung dieser Daten anders nicht gewährleistet werden kön-

nen. Es mußte somit für jede Datei mit PKZ festgestellt werden, ob und in welcher Weise diese Art der Personenbeziehbarkeit der gespeicherten Daten erhalten werden durfte. Die von mir über das Bundesministerium für Arbeit und Sozialordnung getroffenen Feststellungen führten u. a. zu folgenden Ergebnissen:

— *Datei über anerkannte Berufskrankheitenfälle*

Diese Datei wurde ursprünglich in zwei Versionen geführt, davon nur eine mit PKZ. Diese Datei wurde gesperrt, archiviert und für Anfragen Betroffener genutzt; bei Anfragen dritter Stellen nur insoweit, wie der Betroffene schriftlich in eine Auskunft aus der Datei an diese eingewilligt hatte. Jeder Zugriff auf diese Dateiversion wurde protokolliert.

Die zweite Version der Datei, die ohne PKZ geführt wurde, enthielt als Identifikationsmerkmal die Nummer des meldenden Bezirkes und die von diesem geführte Journalnummer.

Weil die bei der BAfAM gespeicherten Datensätze nur sehr pauschale und teilweise fehlerhafte Informationen enthielten, waren für die Entwicklung von Strategien zur Bekämpfung von Berufskrankheiten in Einzelfällen Recherchen in den Akten der gewerbeärztlichen Dienste der neuen Bundesländer insbesondere zur Frage, inwieweit Arbeitnehmer der Einwirkung von Schadstoffen ausgesetzt waren, notwendig. Dazu wurde die in den Datensätzen enthaltene Journalnummer verwendet, was offenbar ausreichte.

Inzwischen hat die BAfAM mir mitgeteilt, daß die in der Berufskrankheiten-Datei gespeicherten Daten bis Ende 1992 an die gewerbeärztlichen Dienste der neuen Bundesländer übergeben worden sind. Seitdem können Betroffene bei den gewerbeärztlichen Diensten der neuen Länder Auskunft über ihre Daten erhalten.

— *Begutachtungsfallakten*

In vielen Fällen führte das Zentralinstitut für Arbeitsmedizin der ehemaligen DDR Akten über die Begutachtungen in Berufskrankheitsfällen. Sowohl das BMA als auch die BAfAM teilen meine Auffassung, daß dem Betroffenen jederzeit die Einsichtnahme in seine bei der BAfAM geführte Begutachtungsfallakte zusteht. Demgemäß habe ich die BAfAM gebeten, technisch und organisatorisch sicherzustellen, daß dem Betroffenen die Möglichkeit eröffnet wird, jederzeit vom Inhalt seiner Begutachtungsfallakte Kenntnis zu nehmen.

Bei der Übermittlung von Daten aus den Begutachtungsfallakten an eine gewerbliche Berufsgenossenschaft sollen sog. Confounder-Daten (z. B. zu Rauchgewohnheiten des betroffenen Arbeitnehmers) nur mit Einwilligung des Betroffenen einbezogen werden.

— *Datei der arbeitsmedizinischen Vorsorgeuntersuchungen*

Die Datensätze sind in der Datei ohne Namen unter einer speziellen Probandennummer gespeichert. Daneben gibt es eine „Umsteigerdatei", die die Probandennummern der PKZ zuordnet. Die Umsteigerdatei stellt sicher, daß die BAfAM die Daten zur Vorbereitung von Forschungsvorhaben anderer Forschungsträger mit anderen Dateien jeweils personenbezogen zusammenführen kann. Vor der Weitergabe der zusammengeführten Daten an den Forschungsträger obliegt es der BAfAM in einem zweiten Schritt den neu entstandenen Datensatz wieder mit der Probandennummer zu versehen, d. h., für den Forschungsträger zu anonymisieren.

Zur Zeit erörtere ich mit dem Bundesministerium für Arbeit und Sozialordnung die Frage, unter welchen Voraussetzungen Daten aus der genannten Datei auch ohne Confounder-Daten an gewerbliche Berufsgenossenschaften übermittelt werden dürfen. Die Diskussion ist noch nicht abgeschlossen.

2.6.3 Wismut-Gesundheitsdaten für nachgehende Untersuchungen erfaßt

Die Wismut GmbH verwahrt in Aue und in Niederlassungen an anderen Orten eine große Menge von Personal- und Gesundheitsunterlagen über ehemalige und aktuell beschäftigte Mitarbeiter (s. auch oben 2.4).

Die gewerblichen Berufsgenossenschaften haben zur Bewältigung der gesundheitlichen Folgelasten des ehemaligen Uran-Erzbergbaues beim Hauptverband der gewerblichen Berufsgenossenschaften (HVBG) eine Zentrale Erfassung- und Betreuungsstelle Wismut (ZEBWis) errichtet. Die ZEBWis hat das primäre Ziel, ein Angebot nachgehender Untersuchungen bei — auch ehemaligen — Beschäftigten der Wismut zu steuern.

Die Wismut GmbH hat sich gegenüber dem HVBG vertraglich verpflichtet, unter Beachtung der datenschutzrechtlichen Bestimmungen den vom HVBG bestimmten Mitarbeitern die Unterlagen vorzulegen, aus denen die Daten des einvernehmlich abgestimmten Datenkatalogs erfaßt werden können. Dieser Katalog enthält nur Daten, die die Berufsgenossenschaften für ihre Aufgabenerledigung benötigen. Die zur Erfüllung der Aufgaben der ZEBWis erforderlichen Daten werden von Mitarbeitern des HVBG, aber nach alleiniger Weisung der Wismut GmbH auf Datenträger übernommen. Dieser Lösung habe ich zugestimmt, weil eine bessere, nämlich die Datenerhebung durch eigene Mitarbeiter der Wismut GmbH, aus wirtschaftlichen Gründen nicht realisierbar war.

2.6.4 Datenübermittlung für Rentenüberleitung korrekt

Das im Rahmen des Renten-Überleitungsgesetzes geschaffene Anspruchs- und Anwartschafts-Überführungsgesetz (AAÜG) sieht in bestimmten Fällen eine Leistungskürzung vor (§§ 6 und 7). Davon betroffen sind im wesentlichen Personen, die in der ehemaligen DDR eine bestimmte Tätigkeit ausgeübt oder einem bestimmten Versorgungssystem angehört haben.

Die BfA erhält die für diese Kürzungsentscheidungen erforderlichen Informationen im wesentlichen aus drei Unterlagen, nämlich

— dem ggf. im Original oder in Kopie vorzulegenden Ausweis für Arbeit und Sozialversicherung der ehemaligen DDR (§ 286 e SGB VI),

— den Angaben im Antrag auf Kontenklärung und

— aus Bescheinigungen, die von Arbeitgebern und Dienststellen sowie von sonstigen Einrichtungen mit Zusatzversorgungssystemen auszustellen sind.

Nach Angaben der BfA reichen nach den jetzigen Erkenntnissen diese Angaben im allgemeinen aus, um eine sachlich richtige Entscheidung treffen zu können. Nur in Einzelfällen wird es für notwendig erachtet, ergänzende Informationen einzuholen. Das ist z. B. dann der Fall, wenn Anhaltspunkte für eine verdeckte Tätigkeit als hauptberuflicher Mitarbeiter des Ministeriums für Staatssicherheit oder des Amtes für nationale Sicherheit bestehen (§ 7 Abs. 1 Satz 2 und Abs. 2 AAÜG).

Aus meiner Sicht bestehen gegen diese Vorgehensweise keine Bedenken.

2.7 Statistisches Material der ehemaligen DDR auf Statistisches Bundesamt und Landesämter für Statistik aufgeteilt

In der Staatlichen Zentralverwaltung für Statistik (SZS) der ehemaligen DDR, die noch am 8. März 1990 in das „Statistische Amt der DDR" umgewandelt worden war, sowie im fachlichen Berichtswesen, das im Auftrag der SZS von den Ministerien und ihren Institutionen durchgeführt wurde, ist in den letzten vierzig Jahren ein kaum überschaubares Datenmaterial angefallen. Das Statistische Amt der DDR wurde aufgrund des Einigungsvertrages zunächst in das Gemeinsame Statistische Amt der fünf neuen Bundesländer überführt. Dieses Gemeinsame Statistische Amt wurde dann mit Ablauf des Jahres 1991 aufgelöst. Die statistischen Daten wurden von den neugegründeten Landesämtern für Statistik der neuen Bundesländer übernommen.

Die Daten einer Reihe von Statistiken, die ihre Entsprechung in Bundesstatistiken haben, gingen an das Statistische Bundesamt. Dazu gehören etwa Datenaggregate aus den Volkszählungen der Jahre 1950, 1964, 1971 und 1981. Das Statistische Bundesamt hat sich zur Aufgabe gemacht, die statistischen Angaben aus der ehemaligen DDR zu sichern und — zurückgehend bis 1985, in Einzelfällen auch bis 1980 —, nach der Methodik und Systematik der Bundesstatistiken auszuwerten.

Anläßlich eines Besuches der Außenstelle des Statistischen Bundesamtes in Berlin hatte ich Gelegenheit, das Verwaltungs-, Volkszählungs- und Totenscheinarchiv der ehemaligen Staatlichen Zentralverwaltung für Statistik zu besichtigen und mit dem Statistischen Bundesamt gemeinsam die datenschutzrechtlichen Aspekte zu besprechen. Es bestand Einvernehmen darüber, daß die Personenkennzahl, nachdem sie zur Gewinnung von Erhebungsmerkmalen wie Alter, Geschlecht und Ausländerkennung für die Bevölkerungsstatistik und für die Statistik des Gesundheitspersonals gedient hat, unverzüglich gelöscht wird. Die Daten, die weder vom Bund noch von den Ländern benötigt werden, sollen vom Statistischen Bundesamt dem Bundesarchiv angeboten werden.

2.8 Soldaten und Wehrpflichtige der ehemaligen NVA

2.8.1 Unzulässige Daten auf den Wehrstammkarten der ehemaligen NVA werden nun doch gelöscht

Die ehemalige DDR hatte für Wehrpflichtige sog. Wehrstammkarten angelegt, auf denen in 120 Datenfeldern eine Fülle personenbezogener Daten gespeichert ist. Das Bundesministerium der Verteidigung hält es nach wie vor für erforderlich, diese Wehrstammkarten zu erhalten (s. 13. TB S. 34). Es war sich allerdings bald mit mir einig, daß eine Reihe von Daten, die nicht zur Aufgabenerfüllung der Bundeswehr erforderlich oder nicht nach rechtsstaatlichen Grundsätzen erhoben worden sind, nach §§ 12 Abs. 4, 35 Abs. 2 Satz 2 Nr. 1 und 3 BDSG grundsätzlich zu löschen, d. h. unkenntlich zu machen sind. Dies gilt vor allem für Eintragungen wie Parteizugehörigkeit (mit Eintrittsdatum) oder „Soziale Herkunft" (vgl. 13. TB S. 34).

Ich bin dem Bundesministerium der Verteidigung nicht gefolgt, als es allein unter Hinweis auf unverhältnismäßig hohen Aufwand lediglich eine Sperrung unzulässiger Daten nach § 35 Abs. 3 Nr. 3 BDSG auf allen, d. h. auf Millionen von Wehrstammkarten, vorsehen wollte. Um den Verwaltungsaufwand auf das unerläßliche Maß zu reduzieren, habe ich meine im 13. Tätigkeitsbericht erhobene Forderung nach Löschung der Daten auf die Fälle beschränkt, in denen eine Wehrstammkarte im Rahmen eines Verwaltungsvorgangs *bearbeitet* wird oder mit in die Bearbeitung gelangt. Dadurch wird vermieden, daß Wehrstammkarten nur zum Zweck der Löschung zu bearbeiten sind und ihr Inhalt damit zur Kenntnis des Bearbeiters gelangt; andererseits wird sichergestellt, daß die unzulässig gespeicherten Daten den Wehrpflichtigen oder Soldaten im Rahmen eines aktuellen Vorgangs nicht noch weiter begleiten. Die Betroffenen haben ein Recht darauf, daß auch bei Bearbeitung eines Vorgangs durch ein Kreiswehrersatzamt unzulässig gespeicherte Daten in Zukunft nicht mehr zur Kenntnis genommen werden können.

Das Bundesministerium der Verteidigung übernahm meinen *Kompromißvorschlag* zunächst nur insoweit, als es die Schwärzung bei Abgabe der Wehrstammkarten an Truppenteile oder Dienststellen (im Rahmen der Einberufung oder Einplanung) und an andere Bereiche außerhalb der Wehrersatzbehörden (z. B. Abgabe an das Bundesamt für den Zivildienst bei Anerkennung als Kriegsdienstverweigerer) verfügte. Für andere Fälle der Bearbeitung der Wehrstammkarten beließ das BMVg es unter Hinweis auf einen von ihm berechneten hohen Mehraufwand bei der Sperrung der Daten. Die Weigerung des Bundesministeriums der Verteidigung, meinem Vorschlag zu folgen, habe ich als Verstoß gegen das Löschungsgebot nach §§ 12 Abs. 4, 35 Abs. 2 Satz 2 Nr. 1 und 3 BDSG gewertet und eine *Beanstandung* ausgesprochen.

Maßgebend hierbei war für mich die Tatsache, daß sich der vom Bundesministerium der Verteidigung berechnete Mehraufwand bei Übernahme meines oben dargelegten Vorschlags in Wirklichkeit als wesentlich geringer darstellte und daher keinen, wie es § 35 Abs. 3 Nr. 3 BDSG voraussetzt, *unverhältnismäßig hohen Aufwand* erforderte. So hatte das Bundesministerium der Verteidigung auch Wehrpflichtige der Geburtsjahrgänge 1973 und 1974, die im Jahr 1993 einberufen werden, voll berücksichtigt, obwohl für diese keine Wehrstammkarten mehr angelegt waren, sondern die Erfassung und Musterung bereits durch die Bundeswehr erfolgte.

Der Deutsche Bundestag hat im Rahmen der Behandlung meines 13. Tätigkeitsberichts der Bundesregierung empfohlen, entsprechend meinem Vorschlag zu verfahren (s. BT-Drucksache 12/4094). Das Bundesministerium der Verteidigung beabsichtigt, dieser Empfehlung zu folgen. Sobald dessen Weisung durchgeführt ist, werden Soldaten und ehemalige Soldaten aus den neuen Ländern in bezug auf ihr informationelles Selbstbestimmungsrecht nicht mehr schlechter gestellt sein als Soldaten aus den alten Ländern.

2.8.2 Unzulässige Daten auf Wehrstammkarten der ehemaligen NVA werden auch beim Bundesamt für den Zivildienst gelöscht

Nach der nunmehr vom Bundesministerium der Verteidigung vorgesehenen Regelung (s. o. 2.8.1) erhält das Bundesamt für den Zivildienst in Zukunft von den Ausschüssen und Kammern für Kriegsdienstverweigerung und von den Verwaltungsgerichten mit den Personalunterlagen anerkannter Kriegsdienstverweigerer nur noch Wehrstammkarten mit den entsprechend gelöschten Datenfeldern. Im Bundesamt für den Zivildienst befinden sich aber aus der Zeit davor u. a. etwa 8 000 Personalunterlagen von gedienten Bausoldaten, die ebenfalls Wehrstammkarten enthalten (s. 2.8.3).

Ich habe das Bundesministerium für Frauen und Jugend gebeten, in gleicher Weise wie das Bundesministerium der Verteidigung die entsprechenden Daten auf den Wehrstammkarten zu löschen (s. 2.8.1). Das Bundesministerium für Frauen und Jugend ist meiner Empfehlung gefolgt. Einvernehmlich wurde jedoch das Datenfeld PKZ zunächst von der Löschung ausgenommen. Zwar hat die Bundeswehrverwaltung für alle gedienten Bausoldaten eine Personenkennziffer (PK) vergeben, die auch im Bereich der Zivildienstverwaltung Ordnungskriterium ist. Da aber eine entsprechende Benachrichtigung der Betroffenen nicht erfolgte, wenden sich diese bei Anfragen mit der ihnen allein bekannten PKZ an das Bundesamt für den Zivildienst. PKZ und PK enthalten als erste Ziffern das Geburtsdatum des Wehr- oder Zivildienstpflichtigen, so daß die Akte auch mit Hilfe der PKZ gefunden und die Identität des Anfragenden — anhand der Personenkennzahl auf der Wehrstammkarte — festgestellt werden kann. Dies dient der Verfahrensbeschleunigung.

Gegen eine vorübergehende Beibehaltung der PKZ für diesen Zweck habe ich, da sie zugunsten des Betroffenen erfolgt, keine Bedenken erhoben. Im Hinblick auf die Regelung des Einigungsvertrages, wonach dieses Datum zum frühestmöglichen Zeitpunkt zu löschen ist (Einigungsvertrag Anlage I Kapitel II Sachgebiet C Abschnitt III Nr. 3, Fußnote und Buchstabe c, BGBl. 1990 I S. 885, 917f.), werde ich allerdings mittelfristig prüfen, ob die Speicherung der PKZ noch erforderlich ist.

2.8.3 Unterlagen über ehemalige Bausoldaten noch nicht vollständig an das Bundesamt für den Zivildienst abgegeben

Seit 1964 bestand in der ehemaligen DDR die Möglichkeit, als Bausoldat in Baueinheiten der ehemaligen NVA den Wehrdienst ohne Waffe zu leisten. Die Erklärung, als Bausoldat dienen zu wollen, bedurfte der Schriftform.

Die von mir anläßlich eines Kontrollbesuchs in einem Kreiswehrersatzamt im Beitrittsgebiet Ende 1990 aufgeworfene Frage des Verbleibs dieser Erklärungen (s. 13. TB S. 34) und der damit verbundenen Personalunterlagen führte auf meine Empfehlung im Februar 1991 zu folgenden Regelungen des Bundesministeriums der Verteidigung, die im Einvernehmen mit dem für den Zivildienst zuständigen Bundesministerium für Frauen und Jugend ergingen:

— *Gediente* Bausoldaten gelten als anerkannte Kriegsdienstverweigerer; sie sind wie Zivildienstpflichtige zu behandeln, die bereits durch den Einigungsvertrag (Anlage I Kapitel X Sachgebiet C Abschnitt III Nr. 1, BGBl. 1990 I S. 885, 1072) den anerkannten Kriegsdienstverweigerern i. S. des Kriegsdienstverweigerungsgesetzes gleichgestellt wurden. Die Kreiswehrersatzämter in den fünf neuen Ländern wurden dementsprechend angewiesen, die Personalunterlagen der gedienten Bausoldaten an das Bundesamt für den Zivildienst abzugeben.

— *Ungedienten* Wehrpflichtigen, die eine Verwendung als Bausoldat lediglich beantragt oder sonst den Wehrdienst in der NVA schriftlich abgelehnt hatten, wurde anheimgestellt, bis zu einem bestimmten Termin einen schriftlichen Antrag nach dem Kriegsdienstverweigerungsgesetz zu stellen; ansonsten wurde davon ausgegangen, daß der Wehrpflichtige für den Wehrdienst zur Verfügung steht (zum Verbleib der Erklärungen s. 15.2).

Bei einer Kontrolle in einem weiteren Kreiswehrersatzamt in den neuen Ländern im Dezember 1991 habe ich festgestellt, daß die Abgabe der Personalunterlagen der gedienten Bausoldaten an das Bundesamt für den Zivildienst entgegen der eindeutigen Weisungslage nur zu einem geringen Teil tatsächlich erfolgt war. Daraufhin habe ich das Bundesministerium der Verteidigung dringend um entsprechende Maßnahmen gebeten. Bisher ist jedoch erst die Übergabe der Personalunterlagen der unter 32jährigen gedienten Bausoldaten erfolgt, die nach dem 3. Oktober 1990 nach und nach *als gediente Bausoldaten* von den Kreiswehrersatzämtern im aktuellen Bestand der Wehrdienstpflichtigen erfaßt worden sind. Anders

verhält es sich bei den Akten der über 32jährigen: Deren Unterlagen sind nicht durch ein äußeres Merkmal auf den Akten gekennzeichnet und befinden sich in der sog. „Ablagekartei". Darin werden die Unterlagen von ca. 2 Mio. nicht mehr der Wehrpflicht unterliegenden Personen geführt. Eine Aussortierung wäre daher nur bei Überprüfung des gesamten Aktenbestandes möglich. Nicht einmal die genaue Zahl dieser gedienten Bausoldaten steht fest; Angaben der ehemaligen NVA soll es nicht geben.

Ich bin mit dem Bundesministerium der Verteidigung und dem Bundesministerium für Frauen und Jugend wegen einer Lösung dieses Problems im Gespräch.

2.9 Das Sicherungsgesetz für das Nationale Krebsregister der ehemaligen DDR

Mit dem zum 1. Januar 1993 in Kraft getretenen Gesetz zur Sicherung und vorläufigen Fortführung der Datensammlungen des Nationalen Krebsregisters der ehemaligen Deutschen Demokratischen Republik (Krebsregistersicherungsgesetz) ist ein rechtlich kaum haltbarer Zustand beendet worden. Nach der Wiedervereinigung bestand für die fortdauernde Speicherung personenbezogener Daten im Nationalen Krebsregister keine ausreichende rechtliche Grundlage mehr (13. TB S. 32). Da auch die neuen Bundesländer und das Land Berlin keine entsprechenden Vorschriften erlassen haben, hätte der Datenbestand des Nationalen Krebsregisters der ehemaligen DDR eigentlich gelöscht werden müssen. Dies schien allen Beteiligten unvertretbar, so daß der Bund, die fünf neuen Bundesländer und das Land Berlin auf der Grundlage des Verwaltungsabkommens über die Verwaltung des Krebsregisters der ehemaligen DDR vom 31. Dezember 1991 die Daten befristet bis zum 31. Dezember 1992 in die Obhut des Bundesgesundheitsamtes gegeben haben.

Bei der Vorbereitung des Verwaltungsabkommens und den anschließenden Beratungen zum Entwurf des Krebsregistersicherungsgesetzes bin ich von Anfang an beteiligt gewesen. Meine Anregungen wurden aufgenommen.

Das Gesetz sieht vor, daß das Bundesgesundheitsamt als Organ der Länder die aufgrund des Verwaltungsabkommens vom 31. Dezember 1991 in Verwahrung genommenen Daten des Nationalen Krebsregisters der ehemaligen DDR sichert und das Krebsregister für die fünf neuen Bundesländer sowie das Land Berlin bis zum 31. Dezember 1994 fortführt. Es regelt die Trennung der epidemiologischen Daten (z. B. Geschlecht, Diagnose eines Tumors, Stadium der Tumorausbreitung, Wohnort, Monat sowie Jahr der Geburt und ggf. des Todes) von den Identitätsdaten (Name, Anschrift, Geburtsdatum) und ihre Nutzung für gesundheits- und umweltpolitische Maßnahmen sowie für wissenschaftliche Forschungszwecke, die von besonderer Bedeutung für die Krebsbekämpfung sind.

Nach § 8 Abs. 2 des Gesetzes darf das Bundesgesundheitsamt epidemiologische Daten mit Identitätsdaten für Zwecke eines bestimmten wissenschaftlichen Forschungsvorhabens vorübergehend wieder zusammenführen. Die Verarbeitung und Nutzung der zusammengeführten Daten ist dann aber nur nach Einwilligung des Patienten oder, wenn er verstorben ist, seines nächsten Angehörigen zulässig. Ich halte diese Forschungsregelung im Rahmen eines Sicherungsgesetzes, das zudem nur zwei Jahre gelten soll, zwar für sehr weitgehend, habe aber wegen der besonderen Bedeutung der Krebsforschung Bedenken zurückgestellt.

2.10 Besondere Gefahren für das Fernmeldegeheimnis im Telefonnetz der neuen Bundesländer

Die Abhöreinrichtungen des Ministeriums für Staatssicherheit der ehemaligen DDR spielen auch heute noch gelegentlich in Presseberichten eine Rolle. Die Bemühungen der dafür zuständigen Stellen — insbesondere der Deutschen Bundespost Telekom — haben jedoch inzwischen dazu geführt, daß solche Einrichtungen heute jedenfalls nicht mehr funktionsfähig bestehen und somit von ihnen keine Gefährdungen des Fernmeldegeheimnisses mehr zu befürchten sind.

Behörden und Betriebe in der ehemaligen DDR verfügen in der Regel über Telefonnebenstellenanlagen. Viele davon sind weiter im Gebrauch. Sie besitzen — wie auch in den alten Bundesländern — üblicherweise eine sogenannte Aufschaltmöglichkeit, die es dem Personal in der Telefonvermittlung erlaubt, sich in bestehende Telefonverbindungen einzuschalten, um den Teilnehmer zum Beispiel auf einen dringenden anderen Anruf aufmerksam zu machen. Beim Aufschalten wird ein akustisches Signal erzeugt, das alle Beteiligten auf den Vorgang aufmerksam macht.

Mich erreichten Hinweise, daß dieses Signal durch Eingriffe in einigen Telefonanlagen unterbunden ist oder werden kann, so daß sich das Vermittlungspersonal unbemerkt in Telefongespräche einschalten kann. Dies darf nicht hingenommen werden. Ich habe die zuständigen Stellen aufgefordert, entsprechende Prüfungen ihrer Telefonanlagen vorzunehmen und — falls erforderlich — den korrekten Zustand der Telefonanlage wieder herstellen zu lassen.

Insgesamt gesehen leidet — trotz der anerkennenswerten Anstrengungen der Deutschen Bundespost Telekom — die Telekommunikation in den neuen Bundesländern — besonders der Telefondienst — noch unter den Unzulänglichkeiten des von der ehemaligen Deutschen Post der DDR übernommenen Kabelnetzes und der dort vorhandenen Vermittlungsstellen, die aufgrund ihres Alters und ihres physisch-technischen Zustandes teilweise nicht mehr den Erfordernissen für eine sichere Nachrichtenübermittlung entsprechen. Die daraus resultierenden Mängel wirken sich im Störungsfall als „Nebensprechen" und Doppelverbindungen aus und gestatten in solchen Fällen das unbeabsichtigte Mithören von Telefonaten.

Durch die Eingabe einer Bürgerin aus Ostberlin wurde ich auf eine weitere — noch heute fortbestehende — Gefahr für das Fernmeldegeheimnis beim Telefonieren in den neuen Bundesländern aufmerksam gemacht. Die Petentin ist seit März 1989 im Besitz eines sogenannten Gemeinschaftsanschlusses („Zweieranschluss"), durch den unter Nutzung nur einer Fernsprechleitung zwei Teilnehmer an das Fernsprechnetz angeschlossen sind. Durch Zufall hatte sie erfahren, daß ihr Anschlußpartner ihre Gespräche unbemerkt mithören konnte. Die Telekom stellte fest, daß mit hoher Wahrscheinlichkeit ein Fehler bei Arbeiten am Leitungsnetz verantwortlich war; der Fehler wurde inzwischen behoben.

Gemeinschaftsanschlüsse in den neuen Ländern sind jedoch generell eine Gefahrenquelle. Aus Kostengründen hat die ehemalige Deutsche Post der DDR bevorzugt Gemeinschaftsanschlüsse gelegt. Zum Zeitpunkt der Fusion der beiden Telekom-Unternehmen gab es in den neuen Bundesländern ca. 750 000 Gemeinschaftsanschlüsse; das entsprach einem Anteil von 39 %. Die für die betriebstechnische Trennung erforderlichen elektronischen Weichen (Gemeinschaftsumschalter) sind in die ursprünglich verwendeten Telefonapparate eingebaut, können allerdings relativ einfach gezielt ausgeschaltet werden. Sie verlieren naturgemäß ihre Wirkung, wenn ein solcher Telefonapparat gegen ein „normales" Gerät ausgetauscht wird, wie dies immer häufiger geschieht, meist ohne daß den Teilnehmern die einschneidenden Konsequenzen — vom Mithören bis zu fehlerhafter Gebührenzuordnung — bewußt sind.

Die Telekom arbeitet seit 1991 intensiv daran, die Gemeinschaftsumschalter in den Netzabschluß („TAE-Dose") zu integrieren. Damit werden die Manipulationsmöglichkeiten weitgehend eingeschränkt. Langfristig sollen Gemeinschaftsanschlüsse im Zuge des Regelausbaus der Ortsnetze generell durch Einzelanschlüsse ersetzt werden.

Ich habe gefordert, bis dahin ergänzende Schutzmaßnahmen — wie zum Beispiel das Verplomben/Versiegeln der Telefonanschlußdosen oder der elektronischen Bauteile in den Telefonapparaten — zu ergreifen und vor allen Dingen die Inhaber von Gemeinschaftsanschlüssen über die damit verbundenen besonderen Risiken für das Fernmeldegeheimnis zu informieren.

2.11 Wohin mit Datenbeständen der ehemaligen DDR? — Bundesarchiv Potsdam —

Unter den Dateien und Akten der Verwaltung der ehemaligen DDR fanden sich viele Datenbestände, die zwar für die ursprünglichen Verwaltungszwecke nach der Vereinigung nicht mehr benötigt wurden, die aber auch nicht gelöscht werden durften. Die Gründe für eine weitere Aufbewahrung sind im wesentlichen die Notwendigkeit der Wiedergutmachung von Unrecht oder wenigstens die Beseitigung seiner Folgen, andere berechtigte Interessen der Betroffenen sowie das Interesse an der rechtlichen und historischen Aufarbeitung der aus den Unterlagen ersichtlichen Geschehnisse. Nicht immer gibt es jedoch eine Fachverwaltung, deren Aufgabe so mit den fraglichen Beständen zusammenhängt, daß die Daten dorthin übernommen werden können. Unter solchen Umständen ist die Abgabe der Bestände an das Bundes- oder ein Landesarchiv oft die noch am ehesten vertretbare Lösung. Eine entsprechende Regelung ist durch den Einigungsvertrag in das Bundesarchivgesetz aufgenommen worden.

Um das Bundesarchiv bei der Lösung der neuen Probleme und beim Umgang mit den neueren Beständen aus dem Staatsarchiv der DDR zu beraten, habe ich wiederholt die Außenstelle Postdam des Bundesarchivs besucht. Anlässe für datenschutzrechtliche Beanstandungen habe ich dabei nicht festgestellt. Ich habe aber angeregt, in einzelnen Bereichen die Einhaltung datenschutzrechtlicher Vorschriften durch den Erlaß von Dienstanweisungen sicherzustellen. Dies gilt im Bundesarchiv — Militärisches Zwischenarchiv Postdam, insbesondere für die Einsicht in Akten zum Zwecke der Durchführung von Strafverfahren, sowie für die Einsicht z. B. von Betroffenen in im Archiv liegende Akten über Strafverfahren. Ich habe zugesagt, das Bundesarchiv bei der Erarbeitung von Dienstanweisungen, die den Zugang zu den einzelnen Arten von Archivalien regeln, weiter zu unterstützen. Sehr hilfreich wäre es dabei, wenn das Bundesministerium des Innern die bisher immer noch nur im Entwurf vorliegende Benutzungsordnung für das Bundesarchiv in Kraft setzte.

Die Hauptstelle des Bundesarchivs, Abteilungen Potsdam, ist aus dem Zentralen Staatsarchiv der ehemaligen DDR hervorgegangen. Hier sind hauptsächlich Unterlagen archiviert, die bis zum Jahre 1933 bei öffentlichen Stellen des Deutschen Reiches, des Kaiserreiches und der damaligen deutschen Länder sowie bei nicht-öffentlichen Stellen angefallen waren. Im ehemaligen Zentralen Staatsarchiv waren allerdings auch Vorgänge der Reichsministerien für die während des Zweiten Weltkrieges besetzten Gebiete und anderer Dienststellen, z. B. Unterlagen des Reichssippenamtes, von den DDR-Behörden untergebracht worden.

Beim Besuch zweier Außenstellen in Berlin, deren Bestände mittlerweile in das Zwischenarchiv Berlin in Dahlwitz-Hoppegarten, übernommen wurden, habe ich einen guten Überblick über die Verwahrung und Nutzung der Archivalien erhalten. Eine dieser Stellen war die Außenstelle in Berlin, Freienwalder Straße, in der sich neben Unterlagen aus den Jahren 1933 bis 1945 auch Entnazifizierungsakten und Vorgänge aus Euthanasieprozessen befinden, die vom Ministerium für Staatssicherheit in den fünfziger und sechziger Jahren angelegt worden waren. Weil für wesentliche Teile dieser Unterlagen der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (BStU) zuständig ist, werden zur Zeit vom Bundesarchiv mit dem BStU Gespräche über die Übernahme von Unterlagen durch den BStU geführt.

Die Unterlagen, die bis zum 2. Oktober 1990 bei der Nationalen Volksarmee der ehemaligen DDR angefallen sind, wurden in das Bundesarchiv — Militärisches Zwischenarchiv Potsdam übernommen. Auch die Akten des Militärischen Oberstaatsanwaltes der

DDR (MOSTA) befinden sich dort. Das Bundesarchiv hat festgelegt, daß Gerichte, Staatsanwaltschaften und weitere Behörden von ihnen angeforderte Akten zur amtlichen Nutzung erhalten. Zum Schutz der Archivalien erhalten Betroffene grundsätzlich keine Akteneinsicht, können jedoch auf Antrag Kopien von Urteilen und Anklageschriften kostenlos erhalten. Lediglich Rechtsanwälte erhalten Akteneinsicht und auf Antrag Kopien der gesamten oder von Teilen der Akte: Diese Regelung halte ich für sachgerecht. Ich habe, wie vorstehend erwähnt, angeregt, das Verfahren in einer Dienstanweisung festzulegen.

Außer den Unterlagen aus der ehemaligen DDR lagern im Bundesarchiv — Militärisches Zwischenarchiv Potsdam auch militärische Archivalien und Unterlagen von Armeen im Gebiet des späteren Deutschen Reiches ab dem Jahr 1809 bis zum Jahr 1945. Dazu gehören auch ca. 50 000 Kriegsgerichtsakten aus dem Zweiten Weltkrieg und Personalakten der Heeresrichter. In den Kriegsgerichtsakten befinden sich naturgemäß personenbezogene Angaben über den Angeklagten und weitere Personen (Eltern, Zeugen, Anzeigeerstatter, Hinweisgeber etc.). Auch Feldpostbriefe, die den Empfänger nicht mehr erreicht haben, sind ebenso Teile der archivierten Unterlagen wie die Abschriften der Urteile, von denen der Verurteilte oft keine Kopie erhalten hat. Das Bundesarchiv — Militärisches Zwischenarchiv Potsdam verweist bei privaten Anfragen den Betroffenen stets an ein Gericht, das die Akten anfordern muß. Der Betroffene kann Auskunft durch das Gericht erhalten. Allerdings werden auf Antrag eines Betroffenen diesem oder seinem Anwalt auch Kopien der Anklageschrift und des Urteils zugesandt. Darüber hinaus kann der Anwalt des Betroffenen Akteneinsicht erhalten. Auch dieses Verfahren halte ich für sachgerecht. Es sollte ebenfalls in einer Dienstanweisung schriftlich festgelegt werden.

2.12 Treuhandanstalt

Nach mehreren vorangegangenen Informationsbesuchen habe ich im Mai 1992 bei der Treuhandanstalt den Umgang mit personenbezogenen Daten kontrolliert. Neben ihrer eigenen großen Personalverwaltung verarbeitet die Treuhandanstalt vor allem personenbezogene Daten von Grundstückseigentümern, Erwerbern und Interessenten sowie des Führungspersonals der Treuhandbetriebe. Nach meinen Erkenntnissen trägt die Treuhandanstalt den Erfordernissen des Datenschutzes Rechnung. Einige geringfügige Mängel sind auf meine Anregung hin weitgehend abgestellt worden.

Die Treuhandanstalt hat sich nach Inkrafttreten des neuen BDSG im Jahre 1991 mit meiner Unterstützung besonders der Aufgabe gewidmet, die Unternehmen mit Treuhandbeteiligung (zeitweise rd. 10 000) über das neue Bundesdatenschutzgesetz und die sich daraus ergebenden datenschutzrechtlichen Erfordernisse im Betrieb zu informieren. Die Reaktion auf ein entsprechendes Rundschreiben an alle Treuhandbetriebe war ausgesprochen positiv. Die meisten Unternehmen ernannten daraufhin betriebliche Datenschutzbeauftragte, die wiederum ein großes Interesse an weiterer Unterrichtung zeigten. Die Treuhandanstalt veranstaltete deshalb zwei Informationsveranstaltungen in Berlin und Leipzig zum Thema „Datenschutz im Unternehmen", an denen etwa 1 000 Datenschutzbeauftragte teilnahmen. Mein ständiger Vertreter hat auf diesen Veranstaltungen jeweils ein Referat über Grundsatzfragen des Datenschutzes gehalten.

Bei meinen ersten Informationsbesuchen stellte sich heraus, daß die Frage, wo die Unterlagen, insbesondere die Personalakten, aus den zahlreichen liquidierten oder geteilten Betrieben verbleiben sollen, dringend gelöst werden mußte.

Keine Probleme ergaben sich, wenn ein Betrieb von einem neuen Unternehmer übernommen worden war. Die juristische Person existierte dann als GmbH oder AG weiter und blieb in der Verantwortung für den ordnungsgemäßen Umgang mit den übernommenen Unterlagen.

Die Liquidierung oder Teilliquidierung von Betrieben hat dagegen zur Folge, daß *Unterlagen von Arbeitnehmern*, die u. a. für Rentennachweise wichtig sind, in noch nicht gekanntem Ausmaß „herrenlos" werden. Die Treuhandanstalt ist errichtet worden, um die kommunistische Staatswirtschaft in die Marktwirtschaft zu überführen. Aus diesem Auftrag folgt auch ihre Verantwortung, eine Verletzung des Persönlichkeitsrechts ehemaliger Mitarbeiter liquidierter oder teilliquidierter Betriebe zu verhindern und die vorhandenen Unterlagen für die Wahrung schutzwürdiger Interessen dieser Personen verfügbar zu halten.

Meine ersten Anregungen aufgreifend hat die Treuhandanstalt sich dieser Aufgabe inzwischen auch mit Nachdruck angenommen. Sie hat in Berlin und an den Standorten ihrer Niederlassungen (Schwerin, Potsdam, Magdeburg, Erfurt und Dresden) sechs *Depots* eingerichtet, die das Schriftgut aus den liquidierten Betrieben mit dem Ziel aufnehmen, die Personaldaten für die Wahrung der sozialversicherungsrechtlichen Belange der früheren Arbeitnehmer zu sichern und gesetzlichen Aufbewahrungspflichten zu genügen. Die Treuhandanstalt hat eine eingehende Arbeitsanweisung zur Archivierung des Schriftgutes erarbeitet, die Regelungen zur Zuständigkeit, Auskunftserteilung, Schriftgutaufbereitung, Formulargestaltung, Anlieferung und Vernichtung des Schriftgutes enthält. Die Arbeitsanweisung ist mit mir abgestimmt worden. Die Depotverantwortlichen der Treuhandanstalt fordern im Fall der Liquidation die Liquidatoren auf, die Akten vorgeordnet an das zuständige Depot zu übergeben. Schon in dieser Phase werden neben Fachleuten der Depots auch die Landesarchivare zur Beratung herangezogen. Archivwürdiges Schriftgut wird den Landesarchivaren unmittelbar ausgehändigt. Bis zum Abtransport in die Depots sind die Treuhandunternehmen, die sich in Liquidation befinden, gehalten, Bescheinigungen für die Sozialversicherung auszustellen.

Anläßlich meiner Kontrolle habe ich das seinerzeit im Aufbau befindliche Depot in Potsdam besichtigt und mir das Depotkonzept eingehend erläutern lassen. Meine Anregungen, insbesondere zur Aufbewahrung

und Akteneinsicht, wurden berücksichtigt und in das Konzept eingearbeitet. Die Depots haben inzwischen ihre Arbeit aufgenommen. Bei einem erneuten Besuch zusammen mit Vertretern der Landesbeauftragten für den Datenschutz der neuen Länder habe ich festgestellt, daß die Bewältigung der ungeheueren Aktenmengen schwierig ist. Gleichwohl habe ich keinen Anlaß für Beanstandungen gefunden.

Die Depots sind zur Zeit organisatorisch in die Treuhandanstalt eingegliedert. Es ist nicht auszuschließen, daß die Treuhandanstalt die Depots später von einer eigenen GmbH verwalten läßt. Angesichts der öffentlichen Aufgabe, die noch über Jahre hinaus erfüllt werden muß, habe ich auf die Pflicht der Treuhandanstalt hingewiesen, sich in diesem Fall den notwendigen Einfluß zu sichern. Sie oder ihr Rechtsnachfolger muß im Interesse aller betroffenen Arbeitnehmer nach wie vor das Verfahren zur ordnungsgemäßen Verwaltung der Akten vorgeben können und die Möglichkeit der Kontrolle behalten.

In meinem letzten Tätigkeitsbericht (13. TB S. 35) habe ich das Problem der *privatisierten Rechenzentren* angesprochen, die noch über früher erhobene staatliche Daten verfügten. Inzwischen hat ein weitgehend geordneter Übergang dieser Daten auf die jetzt zuständigen Stellen stattgefunden. In Absprache mit mir hat der Datenschutzbeauftragte der Treuhandanstalt im Zuge der Privatisierung der Rechenzentren die Verwahrung sämtlicher Daten, deren Verbleib ungeklärt war, in Sonderarchiven verfügt. Diese Sonderarchive befanden sich zwar noch räumlich innerhalb der Rechenzentren, für den Erwerber wurden aber die Verfügung und der Zugriff darauf vertraglich ausgeschlossen. Die Klärung des weiteren Verbleibs der Daten ist dann mit den zuständigen Landesbehörden erfolgt. Sie ist inzwischen in den meisten Bereichen abgeschlossen.

Die Treuhandanstalt hat einige ihrer Aufgaben auf zu diesem Zweck gegründete Gesellschaften mit beschränkter Haftung übertragen, so auch die Liegenschaftsgesellschaft der Treuhandanstalt mbH (TLG) und die Treuhand Osteuropa Beratungsgesellschaft mbH (TOB). Da auch von diesen Gesellschaften personenbezogene Daten verarbeitet werden, stellt sich die Frage, ob es sich um öffentliche Stellen des Bundes (§ 2 Abs. 1 BDSG) handelt. Nach meiner Auffassung (s. u. 31.1) ist dies der Fall, wenn die Stelle vom Bund beherrscht wird und öffentliche Aufgaben wahrnimmt.

Es handelt sich in beiden Fällen um 100 %ige *Tochtergesellschaften der Treuhandanstalt*, die Beherrschung durch den Bund ist also gegeben. Die TLG ist zuständig für die Veräußerung von Liegenschaften, die nicht für betriebliche Zwecke notwendig sind. Diese Aufgabe ist Teil des gesetzlichen Auftrags der Treuhandanstalt, das volkseigene Vermögen nach marktwirtschaftlichen Prinzipien zu privatisieren und zu verwerten, mithin eine öffentlich-rechtliche Aufgabe. Die Aufgabe der TOB ist die Beratung von Regierungen und Unternehmen beim Aufbau marktwirtschaftlicher Strukturen in ost- und mitteleuropäischen Ländern, ausgehend von den Erfahrungen der Treuhandanstalt. Über die Beratungsaufgabe hinaus übernimmt sie die Leitung modellhafter Projekte in diesen Ländern. Sie wird vom Bundesministerium der Finanzen über die einzelnen Projekte finanziert. Diese Aufgabe geht zwar über den eigentlichen Treuhandauftrag hinaus. Allerdings ist die Vollfinanzierung durch die öffentliche Hand ein Indiz dafür, daß der Staat darin auch eine eigene Aufgabe sieht. Für den Frieden in Europa, zumal mit den östlichen Nachbarn, ist es von ausschlaggebender Bedeutung, daß der Aufbau der Marktwirtschaft auch dort erfolgreich verläuft. Die aus der Tätigkeit der Treuhandanstalt gewonnenen Erfahrungen sollen hierzu einen Beitrag leisten. Dies zu unterstützen, ist eine öffentliche Aufgabe. Allerdings stufe ich die TOB als Wettbewerbsunternehmen ein (§ 27 Abs. 1 Nr. 2a BDSG), das meiner Kontrolle unterliegt, für das im übrigen aber die Vorschriften über nicht-öffentliche Stellen gelten.

3 Deutscher Bundestag

3.1 Welches Datenschutzrecht soll für den Deutschen Bundestag gelten?

Ob der Bundestag bei der Wahrnehmung seiner parlamentarischen Aufgaben als öffentliche Stelle i. S. des Bundesdatenschutzgesetzes anzusehen ist und dessen materiellrechtlichen Vorschriften unterliegt, kann zweifelhaft sein. Jedenfalls wurde in der 2. und 3. Lesung des Bundesdatenschutzgesetzes von seiten der Regierungskoalition ausgeführt, es sei davon auszugehen, daß für den Bundestag, soweit er *Verwaltung* ausübe, das Bundesdatenschutzgesetz gelte, nicht aber soweit er als *Legislativorgan* tätig werde. Im Hinblick auf Artikel 38 Abs. 1 Satz 2 GG, der die unabhängige Stellung der Abgeordneten garantiert, habe ich in diesem Zusammenhang stets die Auffassung vertreten, daß der Deutsche Bundestag einer datenschutzrechtlichen Kontrolle durch den BfD nur unterliegt, soweit er in Verwaltungsangelegenheiten tätig wird, nicht aber bei der Wahrnehmung seiner parlamentarischen Aufgaben.

Der Ausschuß für Wahlprüfung, Immunität und Geschäftsordnung des Deutschen Bundestages hat den Fraktionen und Gruppen einen Vorschlag zur Klärung der rechtlichen Zweifel unterbreitet. Er besteht aus einem Vorschlag für einen interfraktionellen Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes und einem Entwurf zur Ergänzung der Geschäftsordnung des Deutschen Bundestages durch eine *Datenschutzordnung*. Der Vorschlag zur Änderung des Bundesdatenschutzgesetzes sieht vor, daß sich der Deutsche Bundestag für die Datenverarbeitung im parlamentarischen Bereich eine Datenschutzordnung gibt. Hierbei sollen die §§ 5, 9 und der neu einzufügende § 26 Abs. 3 Satz 3 des Bundesdatenschutzgesetzes direkt Anwendung finden. Die letztere Vorschrift soll entsprechend der bisherigen Praxis bestimmen, daß der Bundesbeauftragte für den Datenschutz den Deutschen Bundestag im Rahmen seiner Beratungsaufgaben unterstützt. Der Entwurf der Datenschutzordnung selbst verweist auf eine Reihe von Vorschriften des Bundesdatenschutzgesetzes mit dem Vorbehalt, daß in der Datenschutzordnung getroffene abweichende Regelungen vorgehen,

um die Besonderheiten parlamentarischer Aufgaben zu berücksichtigen.

Bei der Vorbereitung beider Entwürfe war ich beteiligt; darüber hinaus bin ich von den Berichterstattern des Ausschusses gehört worden. Ich halte den Inhalt der vorgeschlagenen Entwürfe insgesamt für ausgewogen, vermisse allerdings eine Regelung für eine Haftung wegen Schadensersatzes ohne Verschulden entsprechend § 7 BDSG oder zumindest eine Beweislastregelung zugunsten des Geschädigten, wie sie § 8 BDSG für nicht-öffentliche Stellen vorsieht. Eine solche halte ich für unerläßlich. Wenn einem Bürger durch die unter Umständen auch automatisierte Verarbeitung seiner personenbezogenen Daten im parlamentarischen Bereich wirklich ein Schaden entsteht, ist nicht einzusehen, wieso er bei Geltendmachung eines Schadensersatzanspruches schlechter stehen soll als bei einem Schaden, der durch eine Datenverarbeitung im öffentlichen oder nicht-öffentlichen Bereich entsteht. Der Bundestag sollte sich nicht von einer Haftungsregelung freistellen, die er mit Recht jeder Behörde, ja selbst Privatpersonen, auferlegt.

Ich schlage deshalb vor, bei der in Aussicht genommenen gesetzlichen Regelung, auch den § 7 oder wenigstens den § 8 des Bundesdatenschutzgesetzes für eine Datenverarbeitung im parlamentarischen Bereich gelten zu lassen.

3.2 Steht der Datenschutz dem Fragerecht von Abgeordneten entgegen?

Ein Bundestagsabgeordneter stellte folgende Fragen an die Bundesregierung:

„1. In welche Aufsichtsräte, Verwaltungsräte, Rundfunkräte und vergleichbare Aufsichtsgremien privater oder öffentlicher Unternehmen und Einrichtungen entsendet der Bund Vertreter?

2. Welche Vertretungen des Bundes werden durch aktive oder ehemalige Regierungsmitglieder, Mandatsträger oder Beamte wahrgenommen?

3. In welchen Gremien und in welcher Höhe werden Vergütungen bezahlt und werden diese an die Bundeskasse abgeführt?"

Zur Frage 2 wurde nach Rückfrage ausdrücklich die Angabe der Namen sowie der Funktion der Mandatsträger erbeten.

Das zuständige Bundesministerium der Finanzen erhielt auf seine Umfrage bei allen Ressorts nur lückenhafte Anworten. Gegenüber der Aufforderung, Namen und Vergütungen zu nennen, erhoben viele Ressorts datenschutzrechtliche Bedenken. Daraufhin schaltete das BMF mich ein.

Es kommt gar nicht so selten vor, daß sich die Bundesressorts bei Anfragen aus dem Deutschen Bundestag auf den Datenschutz zurückziehen, auch Ressorts, die sonst den Belangen des Datenschutzes eher zurückhaltend gegenüberstehen. Angesichts der herausragenden Bedeutung der parlamentarischen Regierungskontrolle kann die Rolle des Datenschutzes jedoch keinesfall darin bestehen, die Verweigerung einer Antwort auf unbequeme Fragen zu begründen. Umgekehrt läßt sich freilich auch nicht sagen, daß Belange des Persönlichkeitsschutzes allein deswegen unbeachtlich sind, weil eine Frage von einem oder mehreren Abgeordneten in einer geschäftsordnungsmäßig vorgesehenen Form gestellt wird. Bei der gebotenen Abwägung zwischen beiden Rechtsgütern muß geprüft werden, ob eine personenbezogene Form der Beantwortung für die parlamentarische Regierungskontrolle erforderlich ist und welche Bedeutung diese Form für diese parlamentarische Funktion hat. Dabei ist zu prüfen, ob eine personenbezogene Antwort ohne wesentlichen Informationsverlust vermieden werden kann. Andererseits muß gefragt werden, welche Beeinträchtigungen der informationellen Selbstbestimmung oder anderer Grundrechte der Betroffenen mit einer solchen Antwort verbunden sind, insbesondere welcher Grad der persönlich-privaten Betroffenheit zu erwarten ist.

Im vorliegenden Fall habe ich auf Grund des Frage- und Kontrollrechts ein berechtigtes Interesse des Bundestages und seiner Mitglieder bejaht, über die Beteiligung des Bundes in Aufsichtsgremien öffentlicher und privater Unternehmen auch in personenbezogener Form informiert zu werden. Mitglieder des Parlaments müssen wissen können, wer den Bund in den oben angesprochenen Gremien vertritt, um beurteilen zu können, ob, in welchem Sinne und mit welcher Wirkung der Bund seinen Einfluß ausübt. Auch die Frage, ob ein Vertreter des Bundes aktives oder ehemaliges Mitglied der Regierung, Mandatsträger oder Beamter ist, ist durch das berechtigte Interesse gedeckt.

Zurückhaltung habe ich allerdings empfohlen, soweit aus der Antwort auch hervorgehen soll, welche Vertreter Vergütungen erhalten und in welcher Höhe sie diese an die Bundeskasse abführen. Hier habe ich eher ein überwiegendes schutzwürdiges Interesse der Betroffenen bejaht. Dies gilt insbesondere für diejenigen, die diese Bedingungen ihrer Mitgliedschaft in Aufsichtsräten, Verwaltungsräten und ähnlichen Gremien frei aushandeln. Die Antwort auf eine Anfrage eines Bundestagsabgeordneten wird in den Bundestagsdrucksachen veröffentlicht und kann weite Verbreitung durch die Medien erlangen. Eine Zweckbindung beim Empfänger, wie sie bei Übermittlung von personenbezogenen Daten im Bundesdatenschutzgesetz grundsätzlich vorgesehen ist, ist damit praktisch nicht erreichbar.

Im konkreten Fall habe ich daher empfohlen, die Frage 3 in nicht personenbezogener Form oder allenfalls in einem geeigneten Gremium, z. B. dem Haushaltsausschuß, zu beantworten. Das BMF ist dieser Empfehlung gefolgt.

4 Innere Verwaltung und Auswärtiger Dienst

4.1 Ausländerzentralregister weiter ohne ausreichende Rechtsgrundlage

Das Ausländerzentralregister (AZR) wurde 1953 eingerichtet. Es stellt die größte Sammlung personenbezogener Ausländerdaten in der Bundesrepublik

Deutschland dar, wird seit 1967 automatisiert betrieben und enthält Angaben über ca. 10 Millionen Ausländer. Bislang arbeitet das AZR auf der Grundlage des Gesetzes über die Errichtung des Bundesverwaltungsamts aus dem Jahr 1959, in dem es lediglich heißt: „Das Bundesverwaltungsamt führt das Ausländerzentralregister, das der Erfassung von im Bundesgebiet wohnenden Ausländern dient."

Seit Jahren besteht mit dem verantwortlichen Bundesministerium des Innern Einvernehmen über die Notwendigkeit einer umfassenden gesetzlichen Regelung für dieses Register, die den Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts genügt. Es fehlen normenklare Regelungen, die die aus Gründen überwiegenden Allgemeininteresses erforderlichen Einschränkungen des Rechts der Betroffenen auf informationelle Selbstbestimmung verbindlich festlegen.

In meinen Tätigkeitsberichten (3. TB S. 16, 5. TB S. 15f., 6. TB S. 9, 7. TB S. 10, 8. TB S. 10f., 9. TB S. 15f., 11. TB S. 16f., 12. TB S. 21f.) aber auch in zahlreichen Schreiben an das Bundesministerium des Innern habe ich immer wieder gesetzliche Vorschriften für die Datenverarbeitung in diesem sensiblen Bereich gefordert. Die Bundesregierung hatte nach langwierigen und schwierigen Vorbereitungen, an denen auch meine Dienststelle beteiligt war, im November 1989 beim Deutschen Bundestag den Entwurf eines Gesetzes über das AZR (BT-Drucksache 11/5828) eingebracht. In der 11. Legislaturperiode wurde dieser Entwurf allerdings nicht mehr abschließend beraten. Im Juli 1991 hat das Bundesministerium des Innern mir ein Arbeitspapier für einen Gesetzentwurf der Bundesregierung zugeleitet, in dem insbesondere die Änderungsvorschläge des Bundesrates aus der 11. Legislaturperiode, aber auch von mir gegebene Empfehlungen eingearbeitet sind.

Nach Beteiligung der Landesbeauftragten für den Datenschutz habe ich im Oktober 1991 zu diesem Gesetzentwurf gegenüber dem Bundesministerium des Innern Stellung genommen und dabei einige weitere datenschutzrechtliche Verbesserungen vorgeschlagen. Trotz meiner wiederholten Hinweise auf die dringend notwendige Verabschiedung eines AZR-Gesetzes hat das Bundesministerium des Innern — bedingt offenbar durch personelle und organisatorische Probleme — erst Ende 1992 den Dialog über den Gesetzentwurf wieder aufgenommen.

Das Bundesministerium des Innern hat im Juni 1990, zu einem Zeitpunkt, in dem mit der Verabschiedung des im November 1989 eingebrachten Gesetzentwurfs noch zu rechnen war, im Rahmen der Einführung der dv-technischen Neukonzeption des AZR eine „Vorläufige Richtlinie für die Registerbehörde und für den Verkehr mit dem AZR" erlassen. Sie wurde dem Innenausschuß des Deutschen Bundestages vorgestellt und sollte — unter Inanspruchnahme eines rechtlichen Übergangsbonus — bis zum Inkrafttreten des AZR-Gesetzes gelten. Nach dieser Richtlinie wird noch heute verfahren.

Im Herbst 1992 habe ich beim AZR kontrolliert, ob und inwieweit die Richtlinie von der Registerbehörde und den mit dem AZR zusammenarbeitenden Behörden beachtet wird.

Zu berücksichtigen war dabei allerdings, daß die Richtlinie vor dem Hintergrund eines Gesetzentwurfs (Stand: November 1989) entstanden war, der zum Zeitpunkt der Kontrolle bereits wieder fortentwickelt worden war (Stand: Juli 1991). Mir schien es daher geboten, bei der datenschutzrechtlichen Bewertung der Datenverarbeitung im Register die in dem fortentwickelten Entwurf enthaltenen Wertungen und Regelungen zur Konkretisierung des „Übergangsbonus" mit heranzuziehen. Nach den unter diesem Begriff vom Bundesverfassungsgericht entwickelten Prinzipien kann das ohne ausreichende Rechtsgrundlage praktizierte gegenwärtige Verfahren im Rahmen des Unerläßlichen nur insoweit hingenommen werden, als ein Zustand, der der verfassungsmäßigen Ordnung noch ferner stünde, vermieden werden muß.

Mein Kontrollbesuch gab mir auch Gelegenheit, den fortentwickelten Gesetzentwurf mit Blick auf seine Praxiseignung einer ersten Wertung zu unterziehen.

Dabei bin ich in vielen Punkten zu positiven Ergebnissen gelangt. Gleichwohl ist zu bedauern, daß sich das Bundesministerium des Innern an meinen Gesprächen mit dem Bundesverwaltungsamt nicht beteiligt hat. Zu einzelnen Punkten des Gesetzentwurfs habe ich nämlich festgestellt, daß dieser nicht nur unter Gesichtspunkten des Datenschutzes, sondern auch aus Gründen der Praktikabilität überarbeitet werden sollte. Hierzu möchte ich einige Beispiele nennen:

Dem zugelassenen Benutzer des AZR, d. h. auch jeder online angeschlossenen Stelle außerhalb des AZR, werden die zu den Anfragepersonalien im Register gefundenen Personalien auf dem Bildschirm angezeigt. Falls vorhanden umfaßt diese Anzeige auch frühere Namen, Aliasnamen etc. Oft, insbesondere bei lückenhaften Anfragepersonalien, werden in einer Übersichtstabelle auch Personendatensätze von mehreren Personen sichtbar gemacht, die als der Angefragte in Betracht kommen. Die Anzeige nur möglicherweise in Betracht kommender Personalien in einem solchen Umfang bereits in diesem Stadium des Verfahrens vor genauer Identitätsfeststellung ist jedoch weder mit den Vorschriften der Richtlinie noch mit denen des Gesetzentwurfs vereinbar. Danach soll die auskunftsuchende Stelle, solange die Identitätsprüfung nicht abgeschlossen ist, lediglich die sog. *Grundpersonalien* erfahren, zu denen der Familienname, der Vorname, Tag und Ort der Geburt, das Geschlecht und die Staatsangehörigkeiten, nicht aber frühere Namen, Aliaspersonalien etc. gehören.

Ich habe den Eindruck gewonnen, daß die unmittelbare Anzeige eines Aliasnamens und möglicherweise auch weiterer Personalien zusammen mit den Grundpersonalien sinnvoll ist, da mit diesen Daten Zugriffe ermöglicht werden, die die Person betreffen können, um die es in der Anfrage geht. Ich würde daher einer entsprechenden Regelung nicht widersprechen.

Meine Kontrolle befaßte sich auch mit dem sog. Visaverfahren, in dem einem besonderen Referat des Bundesverwaltungsamts (sog. Visareferat) Daten aus dem AZR zur Prüfung der Frage übermittelt werden,

ob zu den von deutschen Auslandsvertretungen benannten Personen Erkenntnisse vorliegen, die einer Visumerteilung entgegenstehen (s. auch 4.10.2).

Auch in diesem Verfahren spielt die Identitätsfeststellung eine entscheidende Rolle. Erkennt der Bearbeiter, daß Personengleichheit zwischen Anfrage- und Registerdaten besteht, ruft er die Erkenntnisdaten aus dem Register ab, stellt fest, ob sie einer Visumerteilung entgegenstehen und teilt das Ergebnis der anfragenden Auslandsvertretung mit. Werden zu den Anfragedaten Personendatensätze von mehreren im Register erfaßten Personen, sog. ähnlichen Personen, angezeigt, ruft der Bearbeiter diese Daten mit den jeweiligen Erkenntnisdaten ab, um festzustellen, ob Erkenntnisse gegen eine Visumerteilung sprechen und der Auslandsvertretung mitzuteilen sind. Eine weitere Identitätsprüfung erübrigt sich dann, wenn derartige Erkenntnisse bei keiner der in Betracht kommenden „ähnlichen Personen" gespeichert sind.

Auch hier ist die Vorgehensweise durchaus betroffenenfreundlich und datenschutzrechtlich akzeptabel, steht aber nicht im Einklang mit den bislang konzipierten Regelungen des Gesetzentwurfs, der zuerst eine Identitätsentscheidung fordert. Erfreulicherweise hat das Bundesministerium des Innern meine Anregungen für eine Korrektur inzwischen aufgegriffen.

Ich begrüße die vom Deutschen Bundestag am 5. Februar 1993 beschlossene Aufforderung an die Bundesregierung, den Entwurf einer gesetzlichen Grundlage für die Verarbeitung personenbezogener Daten im Ausländerzentralregister so schnell wie möglich einzubringen, und hoffe sehr, daß dem Parlament bald ermöglicht wird, ein datenschutzgerechtes AZR-Gesetz zu verabschieden (s. Anlage 1).

4.2 Asylverfahren

Am 1. Juli 1992 ist ein neues Asylverfahrensgesetz (AsylVfG) in Kraft getreten. Es enthält Rechtsgrundlagen für die Erhebung und Übermittlung personenbezogener Daten, die den Besonderheiten des Asylverfahrens Rechnung tragen. Meiner Empfehlung, Auskünfte beim Verfolgerstaat nur mit Zustimmung des Betroffenen einzuholen, ist der Gesetzgeber nicht gefolgt. Ich hoffe jedoch, daß die statt dessen getroffene Regelung, die die Datenerhebung bei ausländischen Behörden nur zuläßt, wenn keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden, ausreicht, um die Belange des Betroffenen und etwa zurückgelassener Angehöriger zu schützen. Ich werde die Praxis entsprechend beobachten.

Auf meine Initiative wurde auch eine Regelung zur Datenübermittlung vom Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) an den Hohen Flüchtlingskommissar der Vereinten Nationen (UNHCR) aufgenommen. Nachdem ich bei einer im September 1987 beim BAFl durchgeführten Kontrolle festgestellt hatte, daß die Praxis der Datenübermittlung zu extensiv war, habe ich Regelungen gefordert, die präzis auf die internationalen Vereinbarungen zugeschnitten sind. Der UNHCR überwacht als Einrichtung der Vereinten Nationen seit 1949 die Durchführung der Genfer Konvention. Deren Unterzeichnerstaaten sind verpflichtet, ihn zu unterstützen und ihm die erforderlichen Auskünfte zu erteilen (Artikel 35 f.). Eine Übermittlung von Entscheidungen des BAFl einschließlich ihrer Begründungen ist daher „auf Ersuchen" des UNHCR vorgesehen; die Übermittlung sonstiger Angaben, außer in anonymisierter Form, wird nur noch erlaubt, wenn der Ausländer sich an den UNHCR gewandt hat oder seine Einwilligung anderweit nachgewiesen ist (§ 9 AsylVfG).

Schwerpunkt der datenschutzrechtlichen Diskussion um den Gesetzentwurf war die Regelung über die „Sicherung der Identität" des Asylbewerbers (§ 16). Auf die hierzu gefaßte Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, abgedruckt in Anlage 5, nehme ich Bezug. Wesentliche Neuerung ist, daß Asylbewerber nicht mehr nur bei Identitätszweifeln erkennungsdienstlich zu behandeln sind, sondern generell zur Identitäts-Sicherung, um eine etwaige Identitäts-Täuschung bei einem Zweitantrag erkennen zu können und damit zugleich eine mehrfache Inanspruchnahme von Sozialleistungen auszuschließen.

Meine Beratung betraf vor allem die Frage, ob die zur Sicherung der Identität im Asylverfahren erhobenen erkennungsdienstlichen Daten auch für Zwecke der Strafverfolgung genutzt werden dürfen. Ein überwiegendes Allgemeininteresse an einer solchen zweckändernden Nutzung sehe ich durchaus. Zu beachten ist jedoch der Grundsatz der Verhältnismäßigkeit: Nicht nur, daß nunmehr Fingerabdrücke von nahezu *allen* Asylbewerbern gefertigt werden, sondern auch daß das Bundeskriminalamt bei seiner Amtshilfe bei der Auswertung das von ihm neu eingeführte Verfahren AFIS (s. u. 24.3) anwendet. Dieses Verfahren bietet für eine zweckändernde Nutzung dieser Daten durch Zuordnung von Fingerabdruck-Spuren zu den Fingerabdruck-Daten von Asylbewerbern Möglichkeiten, die in diesem Umfang bisher — vornehmlich aus technischen Gründen — nicht bestanden haben. Der von der großen Mehrheit der Datenschutzbeauftragten von Bund und Ländern unterbreitete Vorschlag, durch einen *abschließenden Katalog schwerer Straftaten* ein normatives Korrektiv zu setzen, die Fingerabdrücke von Asylbewerbern also nicht auch zur Verfolgung von Bagatelldelikten zur Verfügung zu stellen, hat sich nicht durchgesetzt. Immerhin sind nach der jetzt getroffenen Regelung die erkennungsdienstlichen Unterlagen über Asylbewerber vom Bundeskriminalamt getrennt von anderen erkennungsdienstlichen Unterlagen aufzubewahren und gesondert zu kennzeichnen. Eine zweckändernde Nutzung ist nur im Einzelfalle zugelassen, „wenn bestimmte Tatsachen die Annahme begründen, daß dies zur Aufklärung einer Straftat führen wird, oder wenn es zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist".

Parallel zu den Bemühungen um die gesetzliche Neuregelung habe ich das BAFl Mitte November 1991 erneut kontrolliert und hierbei eine große Zahl von

ungeordneten Fingerabdruckblättern gefunden, die auf der Basis des alten § 13 AsylVfG angelegt worden waren. Im alten manuellen Verfahren konnte das Bundeskriminalamt nur etwa 10 000 bis 12 000 Fingerabdruckblätter pro Jahr verarbeiten. Was darüber hinaus anfiel, wurde beim BAFl ungeordnet gelagert. Da die Leitung des BAFl mitteilte, daß die Unterlagen für die Durchführung der Asylverfahren nicht erforderlich waren, habe ich empfohlen, die Unterlagen zu vernichten und damit die überflüssigerweise erhobenen gespeicherten Daten zu löschen. Aufgrund einer Weisung des Bundesministeriums des Innern vom März 1992 ist dies dann geschehen.

4.3 Notwendige Verwaltungsvorschriften zum Ausländergesetz fehlen

Nach § 104 des am 1. Januar 1991 in Kraft getretenen neuen Ausländergesetzes erläßt das Bundesministerium des Innern allgemeine Verwaltungsvorschriften zu diesem Gesetz und den aufgrund dieses Gesetzes erlassenen Rechtsverordnungen. Zu den Datenschutzbestimmungen des § 75ff. hat es bislang keine Initiative ergriffen, obwohl Präzisierungen gerade hier dringend notwendig sind, worauf ich wiederholt hingewiesen habe (vgl. 13. TB S. 37).

Auch die Landesbeauftragten für den Datenschutz beklagen die erhebliche Rechtsunsicherheit bei der Anwendung dieses Teils des Gesetzes durch die Länder. Einzelne Länder beabsichtigen inzwischen, eigene Verwaltungsvorschriften zu erlassen. Ich habe dem Bundesministerium des Innern meine Besorgnisse nochmals dargelegt.

4.4 Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR

4.4.1 Stasi-Unterlagen-Gesetz

Am 29. Dezember 1991 ist das Stasi-Unterlagen-Gesetz — StUG — in Kraft getreten (BGBl. I 2272). In Anwendungsbereich, Struktur und wesentlichen Bestimmungen sind zahlreiche meiner Empfehlungen (siehe bereits 13. TB S. 23) berücksichtigt. Im großen und ganzen trägt die nunmehr geschaffene Rechtslage den Anforderungen des Persönlichkeitsrechtsschutzes angemessen Rechnung. Eine bessere Beurteilung wird möglich sein, wenn der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik — BStU — am 1. Juli 1993 seinen ersten Tätigkeitsbericht präsentiert hat.

Vor dem Hintergrund meiner Aufgabe, den Gesetzgeber beim Schutz des Persönlichkeitsrechts zu beraten, möchte ich rückblickend einige aus meiner Sicht besonders wichtige Punkte hervorheben:

Dem informationellen Selbstbestimmungsrecht entspricht es, daß in einem näher bestimmten Umfang allen betroffenen Personen — bei Vermißten oder Verstorbenen für bestimmte Zwecke auch nahen Angehörigen — Ansprüche auf Auskunft, Einsichtnahme und Herausgabe von Kopien zustehen. Dabei stehen die Opfer — im Sprachgebrauch des StUG: „Betroffene" — im Vordergrund, die Personen nämlich, „zu denen der Staatssicherheitsdienst aufgrund zielgerichteter Informationserhebung oder Ausspähung einschließlich heimlicher Informationserhebung Informationen gesammelt hat". Die Einschränkungen, die das im August 1990 noch von der Volkskammer der ehemaligen DDR verabschiedete Gesetz für den Auskunftsanspruch der Bürger vorsah und die ich im 13. TB kritisiert hatte, wurden erfreulicherweise nicht übernommen.

Rechtsstaatlichen Prinzipien entspricht es, daß auch den ehemaligen Mitarbeitern des Staatssicherheitsdienstes ein Recht auf Auskunft über ihre personenbezogenen Informationen zusteht, die in den zu ihrer Person geführten Unterlagen enthalten sind; der Zugang zu ihren Berichten über Betroffene wurde allerdings zu deren Schutz mit Recht beschränkt.

Die in den Gesetzesentwürfen vorgesehene zu enge Definition der anspruchsberechtigten „Dritten" wurde auf meine Empfehlung während der parlamentarischen Beratung erweitert. „Dritte" sind neben Betroffenen, Mitarbeitern und Begünstigten nunmehr alle „sonstigen Personen, über die der Staatssicherheitsdienst Informationen gesammelt hat". Für „Betroffene" und „Dritte" sind Auskunft und Einsichtnahme kostenfrei.

Zu begrüßen ist, daß der BStU die Unterlagen vor der Gewährung einer Einsicht darauf durchsehen muß, ob sie Informationen zu anderen „Betroffenen" oder „Dritten" enthalten und ob deren schutzwürdige Interessen gebieten, die Einsicht nur in Kopien zu gewähren, in denen diese Angaben unkenntlich gemacht sind. Es wäre sicherlich nicht angemessen, wenn z. B. eine ausgespähte Person anhand der Protokolle über den Lauschangriff auf ihre Wohnung vom Ehebruch ihres Ehegatten erfahren würde.

Der BStU bearbeitet Fälle besonderer Eilbedürftigkeit (hohes Alter — erlittene Haft — andauernde Beeinträchtigungen) bevorzugt. Daß dabei Prominente priviligiert würden, kann ich nicht bestätigen.

Wenig befriedigend ist die Regelung über den Anspruch „Betroffener" und „Dritter" auf Anonymisierung und Löschung ihrer personenbezogenen Daten. Solche Ansprüche können nämlich überhaupt erst ab dem 1. Januar 1997 geltend gemacht werden.

Das auf meine Anregung zurückgehende Gegendarstellungsrecht gibt jeder Person, die durch konkrete Tatsachenbehauptungen betroffen ist, die sich in den Stasi-Unterlagen finden, die Möglichkeit, dem eine eigene Darstellung entgegenzusetzen. Diese ist den Unterlagen beizufügen und auch bei Mitteilungen an andere Stellen zu berücksichtigen.

Einen wesentlichen Mangel sehe ich bei den Rechten betroffener Personen in bezug auf „Justizakten". Dabei handelt es sich um vom BStU verwahrte Akten von Gerichten und Staatsanwaltschaften der ehemaligen DDR. Wenn das StUG die Betroffenen insoweit auf die „jeweiligen gesetzlichen Verfahrensordnungen" verweist, berücksichtigt es nicht den Umstand, daß es sich durchweg um Unterlagen aus Strafverfahren

handelt, in denen der Staatssicherheitsdienst die Untersuchungen geführt hat und die daher mit gewöhnlichen Justizakten nicht vergleichbar sind. Das sehr beschränkte Einsichtsrecht nach der Strafprozeßordnung ist keine angemessene Lösung. Eine Korrektur sollte bei nächster Gelegenheit erfolgen.

Über die Verwendung der Unterlagen des Staatssicherheitsdienstes durch öffentliche und nicht-öffentliche Stellen enthält das StUG besondere Vorschriften. Unterschieden ist zwischen Einschränkungen des Persönlichkeitsrechts einerseits für Forschungszwecke und Medien, andererseits für andere Stellen. Die Bestimmungen für die letztgenannten Stellen sind im wesentlichen sachgerecht. Zu begrüßen ist, daß ein abschließender Katalog der zulässigen Verwendungszwecke aufgestellt wurde. Nicht unproblematisch erscheint mir allerdings die in den parlamentarischen Beratungen über das im Entwurf Vorgesehene hinaus erfolgte Ausweitung dieses Katalogs: Muß beispielsweise der ehrenamtliche Kirchenorganist wirklich „Stasi-überprüft" werden können? Als nach wie vor problematisch betrachte ich auch, daß entgegen meinem Rat und der ursprünglichen Entwurfsfassung für den öffentlichen Dienst die Regelüberprüfung eröffnet worden ist; d. h., die Verwaltung hat zwar keine Verpflichtung, aber die Möglichkeit zur Überprüfung in jedem Fall. Auf die Bedeutung der ausgeübten Tätigkeit und vorliegende Verdachtstatsachen kommt es nicht an. Damit hat der Gesetzgeber es der Verwaltung überlassen, das Wesentliche selbst zu entscheiden, nämlich in welchen Fällen und unter welchen Voraussetzungen Überprüfungsverfahren betrieben werden. Leider haben sich auch meine Befürchtungen bestätigt, daß diese breite Regelung zu einer Überlastung des BStU führt, die zur Folge haben kann, daß die wirklich wichtigen Überprüfungskategorien in Bearbeitungsqualität und -dauer beeinträchtigt werden.

Die im Gesetz getroffene strenge Zweckbindung der Auskünfte des BStU ist zu begrüßen. Ihre praktische Einhaltung wäre freilich besser gewährleistet, wenn — entsprechend meinen Anregungen — konkrete organisatorische Sicherungssysteme, vor allem die gesonderte Verwahrung, vorgeschrieben worden wären.

Bewährt hat sich die „Jugendsündenregelung", wonach Stasi-Tätigkeiten von Personen bis 18 Jahren nicht mitzuteilen sind. Heranwachsende bis 21 Jahre wurden leider nicht einbezogen.

Auch eine Regelung zur „Zugangsverjährung" fehlt bisher. Andere Informationssysteme, die zu Eignungsprüfungen abgefragt werden, sehen ausnahmslos angemessene Resozialisierungselemente vor. Selbst eine Verurteilung wegen Totschlags wird nach fünfzehn Jahren im Bundeszentralregister getilgt. Für die Mitteilung einer Stasi-Belastung bleibt dementgegen nach dem StUG der Zeitablauf seit Beendigung der Mitarbeit ohne Belang, so daß selbst noch nach dreißig Jahren unbedeutende Details mitzuteilen sind. Eine Korrektur ist dringend notwendig.

Zur Verfolgung im einzelnen genannter schwerer Straftaten sowie von Straftaten im Zusammenhang mit dem Regime der ehemaligen DDR, insbesondere mit dem Staatssicherheitsdienst, gilt eine Ausnahme von dem sonst mit Recht besonders betonten Grundsatz, daß Informationen aus Stasi-Unterlagen nicht zum Nachteil des jeweiligen Betroffenen oder Dritten verwendet werden dürfen. Diese Ausnahmeregelung ist problematisch, da die Verwertung bei Berücksichtigung von Herkunft und Art der Daten im Einzelfalle unzumutbar sein kann, so etwa, wenn — um die Glaubwürdigkeit eines Zeugen zu erschüttern — Stasi-Unterlagen herangezogen würden, die die Homosexualität des Zeugen aufgrund der Ausforschung seiner Intimsphäre durch die Stasi dokumentieren. Die Voraussetzungen zur Verwertung von Informationen über Betroffene und Dritte aus Stasi-Unterlagen im Strafverfahren sollten daher durch eine an § 81 c Abs. 4 StPO angelehnte Zumutbarkeitsklausel ergänzt werden.

Ich begrüße, daß das Gesetz meinem Vorschlag gefolgt ist, dem BStU eine sog. Nachberichtspflicht aufzuerlegen: wenn nachträglich Umstände bekannt werden, die die früher übermittelten Daten unrichtig erscheinen lassen, so sind die jeweiligen Empfänger zu benachrichtigen.

Was die sog. Spontanmitteilungen, d. h. die dem BStU auferlegten Pflicht zu Mitteilungen *ohne Ersuchen* an öffentliche und an nicht-öffentliche Stellen anbelangt, so werde ich mit kritischem Interesse verfolgen, wie die Vorschriften sich in der Praxis bewähren. Meine Bedenken hinsichtlich ihrer Praktikabilität und letztlich im Ergebnis auch hinsichtlich der Gerechtigkeit der dadurch herbeigeführten Folgen sind noch nicht ausgeräumt.

Seit der Vereinigung gibt es immer wieder Probleme mit Stasi-Unterlagen, die von Medien genutzt, im Fernsehen gezeigt, von Unbekannten erläutert, gar als deren Privatarchiv bezeichnet werden. Nach Einrichtung der Behörde des BStU und Inkrafttreten des StUG wurde auch immer wieder versucht, dort die Schuld für das Bekanntwerden dieser Unterlagen zu sehen. Das ist auch nach meinen Erkenntnissen falsch: Die gesetzlichen Vorschriften sind streng und die Behörde arbeitet korrekt. Ursache für diesen Zustand ist, daß in der Wende-Phase in erheblichem Umfang Unterlagen abhanden gekommen sind und nunmehr auf einem grauen Markt feilgeboten werden. In diesem Zusammenhang ist darauf hinzuweisen, daß von anderer Seite erlangte Unterlagen dem BStU anzuzeigen sind und die Verletzung der Anzeigepflicht mit einer Geldbuße bis zu 500 000 DM geahndet werden kann.

Bedauerlicherweise ist die Strafvorschrift des StUG aufgrund einer mißverständlichen Diskussion in den Medien in der Schlußphase der parlamentarischen Beratung des Entwurfs noch zur Bedeutungslosigkeit entleert worden. Die getroffene Regelung stellt eine drastische Absenkung des strafrechtlichen Datenschutzstandards gegenüber vergleichbaren Regelungen dar, obwohl die in Stasi-Unterlagen enthaltenen Informationen im Interesse der betroffenen Personen doch gerade umgekehrt eine Verschärfung des Strafrechtsschutzes nahegelegt hätten.

Ich gehe davon aus, daß das Bundesministerium des Innern den ersten Tätigkeitsbericht des BStU zum

Anlaß nimmt, Verbesserungen des StUG vorzubereiten. Neben den vorstehend angesprochenen Punkten werden dabei sicherlich auch weitere Punkte zu diskutieren sein. Bereits jetzt kann aber festgehalten werden, daß sich die Grundentscheidung bewährt hat, die Stasi-Unterlagen nicht zu vernichten, sondern insbesondere dem Betroffenen zu ermöglichen, anhand „seiner" Stasi-Unterlagen die Einflußnahme des Staatssicherheitsdienstes auf sein persönliches Schicksal aufzuklären.

4.4.2 Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR widmet Datenschutz große Aufmerksamkeit

Bei meinen ersten Kontrollen in den Außenstellen und in der Zentrale der Behörde, die damals noch Sonderbeauftragter der Bundesregierung für die personenbezogenen Unterlagen des ehemaligen Staatssicherheitsdienstes hieß, galten für deren Arbeit noch die Vorläufigen Regelungen des Vertrages über die Herstellung der Einheit Deutschlands (Anlage I Kapitel II Sachgebiet B Abschnitt II Nr. 2 Buchstabe b des Einigungsvertrages); das Stasi-Unterlagen-Gesetz war noch nicht verabschiedet. Insofern habe ich damals schwerpunktmäßig die datenschutzgerechte Organisation der Arbeitsabläufe und die Sicherung der Unterlagen, z. B. deren Verwahrung in den Diensträumen, den Botenverkehr mit den Außenstellen, die Papiervernichtung und die Abschirmung gegenüber dem Publikumsverkehr, kontrolliert und Verbesserungen empfohlen. Auch die Abläufe bei der Bearbeitung von Auskunftsersuchen gehörten dazu. Hier war — und ist — von Bedeutung, daß nur die dazu berechtigten Mitarbeiter Zugriff auf die Unterlagen erhalten und daß jederzeit nachvollziehbar sein muß, wer wann welche Akte des Staatssicherheitsdienstes eingesehen hat.

Die Auskunftserteilung an öffentliche Stellen zur Überprüfung von Bewerbern und Mitarbeitern auf eine etwaige Tätigkeit für den Staatssicherheitsdienst stand damals noch mehr als jetzt im Vordergrund. In einem aus meiner Sicht wichtigen Detailpunkt gab es einen Dissens mit der Behörde: Ich habe festgestellt, daß der Sonderbeauftragte bei Auskunftsersuchen den öffentlichen Stellen Hinweise auf das Vorliegen eines vom Staatssicherheitsdienst angelegten „Sicherungsvorgangs" in Fällen gab, in denen weitere Unterlagen zu der Person nicht aufgefunden oder nicht ausgewertet waren. Zwar fügte der Sonderbeauftragte dieser Mitteilung die Erläuterung bei, daß sich aus dem Vorliegen eines Sicherungsvorgangs keine Rückschlüsse auf eine Tätigkeit für den Staatssicherheitsdienst ziehen ließen, da derartige Vorgänge von diesem aus einer Vielzahl von Gründen angelegt wurden. Gegen diese Mitteilung erhob ich gleichwohl Bedenken. Der Text der Erläuterung schien mir geeignet für Spekulationen, der Sonderbeauftragte hätte Indizien für eine Stasi-Tätigkeit festgestellt, die lediglich nicht hinreichend verfestigt seien, um auf sie ausdrücklich hinzuweisen. Gerade weil sich aus dem Vorliegen eines Sicherungsvorgangs keine Rückschlüsse auf eine Stasi-Tätigkeit ziehen ließen, war die Mitteilung nicht geeignet, dem in den Rechtsvorschriften genannten Auskunftszweck der Feststellung einer Tätigkeit für den Staatssicherheitsdienst zu dienen. Eine Befugnis zur Übermittlung dieses personenbezogenen Datums bestand demnach nicht. Da der Sonderbeauftragte trotz meiner Bedenken und meiner Ankündigung einer formellen Beanstandung für den Fall, daß diese Mitteilungen weiterhin erfolgen sollten, zunächst an seinem Verfahren festhielt, habe ich im Dezember 1991 eine formelle Beanstandung gemäß § 25 BDSG wegen des Verstoßes gegen § 2 und § 5 der Anlage I Kapitel II Sachgebiet B Abschnitt II Nr. 2b Einigungsvertrag in Verbindung mit § 15 Abs. 1 Nr. 1 BDSG ausgesprochen. Daraufhin hat die Behörde zu Beginn des Jahres 1992 die Hinweise auf vorhandene Sicherungsvorgänge eingestellt.

Bei einem weiteren Informations- und Kontrollbesuch im Sommer 1992, also nach Inkrafttreten des StUG, in der Zentralstelle des BStU war der Aufbau der Behörde bereits weit vorangeschritten. So waren von den endgültig vorgesehenen rd. 3 400 Mitarbeitern rd. 2 500 eingestellt worden. Die hohe Zahl der monatlichen Neueinstellungen von 200 bis 300 Personen schaffte allerdings, was nicht verwundert, erhebliche Probleme bei deren Einarbeitung und Schulung. Bei meinem Besuch überprüfte ich vor allem die automatisierte Datenverarbeitung. Insbesondere der Ablauf der Bearbeitung eines an den BStU gerichteten Antrags von seinem Eingang bis zu seiner Erledigung wurde kontrolliert. Erfreulicherweise ergab sich dabei nur wenig Anlaß zu Kritik. Meine Empfehlungen wurden durchweg angenommen. Einige wichtige Punkte möchte ich herausheben:

1. Jeder Antragsteller hat seinem Antrag auf Auskunft, Einsicht oder Herausgabe von Kopien eine amtliche Identitätsbescheinigung beizufügen. Dies kann durch eine amtlich beglaubigte Ablichtung des Personalausweises oder auch dadurch erfolgen, daß sich der Antragsteller die Angaben zur Person auf der Rückseite des Antragsvordrucks von der zuständigen Landesbehörde bestätigen läßt. Auf dem Antragsvordruck wird neben den Angaben zur Person jedoch eine Vielzahl weiterer zum Teil hochsensibler personenbezogener Daten, wie z. B. die Gründe für eine besondere Eilbedürftigkeit der Bearbeitung, abgefragt. Es ist mehr als verständlich, wenn ein Antragsteller nicht möchte, daß der Mitarbeiter der zuständigen Landesbehörde von solchen Gründen wie „Entlastung vom Vorwurf einer Zusammenarbeit mit dem Staatssicherheitsdienst" oder „Politische Verurteilung des Antragstellers" Kenntnis erhält. Der BStU wird nicht nur bei der Neuauflage der Antragsvordrucke den Hinweis aufnehmen, daß die Antragsteller vor Einholen der Identitätsbestätigung *nur* die Angaben zur Person und erst danach den übrigen Antrag ausfüllen sollten, sondern hat auch alle bereits gedruckten Antragsformulare durch Stempelaufdruck mit einem entsprechenden Hinweis versehen.

2. Angesichts beim BStU vorhandener Personendatensätze zur Auffindung von Stasi-Unterlagen in Millionenhöhe und einer Zahl von „angefragten Personen" in Auskunftsanträgen, die ebenfalls die

Millionenzahl längst überschritten hat, stellt die richtige Zuordnung der angefragten Person zu der Person, über die Unterlagen vorhanden sind (Identifikation) ein besonderes Problem dar, wie sich auch bei anderen Datensammlungen vergleichbarer Größenordnung gezeigt hat. Erfreulicherweise ist noch kein Fall einer Verwechslung bekannt geworden. Ich sehe darin die Wirkung der großen Anstrengungen des BStU gerade in diesem Bereich, die ich weiterhin unterstütze. Dies bezieht sich auch auf die weitere Verwendung der durch die ehemalige DDR vergebenen Personenkennzahl. Die PKZ ist nicht nur in den Stasi-Unterlagen einschließlich der überkommenen Dateien zu erhalten, sie sollte auch weiterhin in den Anträgen erfragt und wie bisher in der Datei der Personen, zu denen ein Antrag gestellt wurde, gespeichert werden. Der BStU verfügt über Unterlagen, die keinen Namen, sondern nur eine PKZ enthalten. Eine Identifizierung ist in diesen Fällen nur mit Hilfe der Datenspeicher des Zentralen Einwohnerregisters der ehemaligen DDR möglich, welches im Oktober 1992 auf Beschluß der neuen Länder, aufgelöst wurde (s. o. 2.2).

Ich habe den BStU darin unterstützt, weiterhin über die PKZ und einige wenige weitere Daten zur Identifikation von Personen verfügen zu können und begrüße die zwischenzeitlich vom Bund und von den zuständigen Ländern hierzu unternommenen Schritte (s. o. 2.2.1).

3. Besonderer Aufmerksamkeit bedürfen Fälle, in denen die PKZ — sei es im Antrag, sei es in den vorhandenen Findmitteln — nicht zur Verfügung steht. Bei einem Vergleich der Daten auf dem Antragsvordruck mit denen aus der Namens-Kartei (F 16) des Staatssicherheitsdienstes habe ich festgestellt, daß dort der Geburtsort durchweg als Identitätsmerkmal eingetragen ist, während er auf dem Antragsvordruck fehlt. Da der Geburtsort ein recht selektives Identitätsmerkmal ist, habe ich empfohlen, diese Angabe in den Antragsvordruck aufzunehmen. Der BStU will dem bei der nächsten Auflage der Formulare entsprechen.

4. Mit dem BStU besteht Einvernehmen, daß eine Veränderung oder Berichtigung (sei es auch nur in Form einer Ergänzung) von Stasi-Unterlagen nicht vorgenommen werden darf. Beim Staatssicherheitsdienst der ehemaligen DDR entstandene, d. h. von ihm angelegte, Karteien sind Unterlagen des Staatssicherheitsdienstes im Sinne des StUG und somit Gegenstand der Erfassung, Verwahrung, Verwaltung und Erteilung von Auskünften. Die Tatsache, daß vom Staatssicherheitsdienst angelegte Karteien zugleich auch dem Auffinden von Unterlagen und der dazu notwendigen Identifizierung von Personen dienen und dienen dürfen, ändert hieran nichts. Unzulänglichkeiten, die sich in der Erfüllung dieser Funktion herausstellen, dürfen nicht durch Veränderung, Berichtigung oder Umordnung dieser Karteien behoben werden. Vielmehr weist § 41 StUG auf die Befugnis des BStU hin, sich als Hilfsmittel zur Erfüllung seiner Aufgaben *eigene* Dateien (die nicht Stasi-Unterlagen sind) zu schaffen.

   In mehreren Außenstellen des BStU waren in der Anfangsphase der Arbeit der Behörde auf den Stasi-Karteikarten von Mitarbeitern des BStU Registriernummern oder Archivnummern nachgetragen worden, die durch die hinzugefügten Jahreszahlen indessen eindeutig als nachträgliche Hinweise erkennbar sind. Der BStU teilt meine Auffassung, daß in dieser Frage ein Höchstmaß an Klarheit gewährleistet sein muß: Auf meine Initiative hin wurden sämtliche Außenstellenleiter angewiesen sicherzustellen, daß Veränderungen jedweder Art von Stasi-Unterlagen unterbleiben.

   Für neu aufgefundenes Material hat sich der BStU Findmittel durch das Anlegen eigener Karteikarten geschaffen. Ich habe gegenüber der Behördenleitung klargestellt, daß eine Einstellung dieser Karteikarten in die vom Staatssicherheitsdienst angelegten Karteien nur dann erfolgen darf, wenn die vom BStU erstellten Karteikarten vom Aussehen her (z. B. pinkfarben mit BStU-Aufdruck und Bundesadler) eine Verwechslung mit Stasi-Unterlagen absolut ausschließen. Nur unter diesen Voraussetzungen wäre eine Einstellung in die vom Staatssicherheitsdienst angelegten Karteien datenschutzrechtlich vertretbar.

5. Gemäß § 4 Abs. 3 des StUG hat der BStU eine sog. „Nachberichtspflicht" wenn sich eine Auskunft im nachhinein als unrichtig erweist. Wenn z. B. im Jahr 1992 einer öffentlichen Stelle auf Ersuchen mitgeteilt wurde, daß über ihren Mitarbeiter keine Unterlagen vorhanden sind, im Jahr 1993 jedoch Unterlagen aufgefunden werden, die diese Person als ehemaligen Inoffiziellen Mitarbeiter (IM) des Staatssicherheitsdienstes ausweisen, hat der BStU nachzuberichten. Nachdem der BStU dieser Verpflichtung bis zum Sommer 1992 wegen der immensen Arbeitsbelastung durch aktuelle Auskunftsersuchen nicht nachkommen konnte, wird mittlerweile eine automatisiert geführte Datei „Nachrecherche" aufgebaut, mit deren Hilfe Erstauskünfte bei der Gewinnung neuer Erkenntnisse aktualisiert werden.

Im Berichtszeitraum erschienen zahlreiche Presseveröffentlichungen mit hochsensiblen, offenkundig aus den Archiven der Stasi stammenden Angaben über mögliche Stasi-Verbindungen von Politikern und Kirchenvertretern; Listen mit den Namen und Dienststellen angeblicher hauptamtlicher Mitarbeiter und Offiziere im besonderen Einsatz der Stasi wurden abgedruckt. Dies veranlaßte mich, den BStU um Prüfung zu bitten, ob etwa aus seiner Behörde Informationen an die Presse gelangt sein könnten. Dies hat sich erfreulicherweise nicht bestätigt.

Auch das Bundeskriminalamt, der Bundesnachrichtendienst, das Bundesamt für Verfassungsschutz und der Militärische Abschirmdienst gelangten in der Zeit des Zusammenbruchs des SED-Regimes in der ehemaligen DDR in den Besitz von Stasi-Unterlagen. Ich habe mich der Problematik der Herausgabe dieser Unterlagen, an den BStU in zahlreichen Schreiben sowie auch in einem Gespräch mit dem Bundesnachrichtendienst angenommen. Mittlerweile sind alle

Sicherheitsbehörden ihrer Verpflichtung nach dem StUG nachgekommen, alle Unterlagen herauszugeben, die personenbezogene Daten Betroffener enthalten.

In bezug auf den Umgang mit Stasi-Unterlagen hat mich auch eine Reihe von Eingaben erreicht. Ein Bürger gab an, IM der Stasi gewesen aber schon vor vielen Jahren in die Bundesrepublik geflohen zu sein und sich den bundesdeutschen Sicherheitsbehörden offenbart zu haben. Ein Mann, den er seinerzeit bespitzelt hatte, hatte als Betroffener (im Sinne des StUG) beim BStU Einsicht in seine Unterlagen genommen und Kopien daraus erhalten. Er fand darin auch rein persönliche Angaben über den Petenten und versuchte, diesen mit diesem Wissen zu erpressen. Die auf meine Initiative hin beim BStU angestellten Nachforschungen ergaben, daß die Bearbeiterin dem Betroffenen nicht nur, wie es § 13 StUG vorsieht Auskunft über die *zu seiner Person* vorhandenen und erschlossenen Unterlagen erteilt, sondern auch Duplikate von Unterlagen herausgegeben hatte, die nur den Petenten persönlich betrafen. Der BStU hat dies gegenüber dem Petenten bedauert und den Betroffenen um Beachtung des Persönlichkeitsrechts des Petenten gebeten.

Zusammenfassend kann ich sagen, daß Kontrolle und Beratung des BStU parallel zum Ausbau dieser Behörde in erfreulicher Weise abgelaufen sind, nicht zuletzt weil die Leitung der Behörde stets eine enge Zusammenarbeit mit dem Datenschutz gesucht hat. Angesichts der Sensibilität der Materie bleibt der BStU für mich eine mit Priorität zu betreuende Einrichtung.

4.5 Umgang mit brisanten Daten aus dem Geschäftsbereich des früheren Bundesministers für innerdeutsche Beziehungen und des ehemaligen Ministeriums des Innern der DDR

4.5.1 Unterlagen über Familienzusammenführung bleiben erhalten

Im Januar 1991 wurden das Bundesministerium für innerdeutsche Beziehungen (BMB) aufgelöst und der überwiegende Teil der Fachaufgaben sowie des Personals vom BMI übernommen. Eine Aufgabe des ehemaligen BMB, die nach dem Zusammenbruch des SED-Regimes in der ehemaligen DDR glücklicherweise entfiel, war die Zusammenführung von Familien aus den ehemaligen beiden deutschen Staaten. Dennoch werden die seinerzeit für diesen Zweck angelegte Kartei und die dazu gehörenden Akten über die Personen, deren Übersiedlungswunsch der BMB seinerzeit unterstützt hat, weiter benötigt, z. B. für Auskünfte an Betroffene und an die Arbeitsgruppe „Regierungskriminalität" bei der Staatsanwaltschaft des Kammergerichts Berlin. Den Umgang mit diesen Daten habe ich in der Außenstelle Berlin des BMI kontrolliert. Dabei ergaben sich weder Beanstandungen noch sonstige Mängel.

4.5.2 Unterlagen in Häftlingsangelegenheiten

Eine weitere brisante Aufgabe des BMB vor der Herstellung der deutschen Einheit war der Freikauf politischer Häftlinge. Während die im Zusammenhang mit dieser Aufgabe angefallenen Aktenvorgänge im BMB geführt wurden und sich nun im Besitz des BMI, Außenstelle Berlin, befinden, wurde die Häftlingskartei in der Berliner Abteilung der dem BMB nachgeordneten Bundesanstalt für gesamtdeutsche Aufgaben (BfgA) geführt und nach deren Auflösung am 1. Januar 1992 vom Bundesarchiv übernommen.

Die beim ehemaligen BMB entstandenen Unterlagen sind für die Arbeitsgruppe „Regierungskriminalität" bei der Staatsanwaltschaft des Kammergerichts Berlin und für den Ersten Untersuchungsausschuß des Deutschen Bundestages für den Bereich kommerzielle Koordinierung (Koko-Ausschuß) von Interesse. Auch beim Umgang mit diesen Unterlagen habe ich keine datenschutzrechtlichen Verstöße oder Mängel festgestellt. An die erwähnten Stellen werden entweder nur Kopien, in denen die personenbezogenen Daten Dritter geschwärzt wurden, herausgegeben oder die Unterlagen werden als Verschlußsache „VS-Vertraulich" oder „Geheim" eingestuft, so daß nur besonders ermächtigte Personen darauf zugreifen dürfen. Auskunftsersuchen ehemals Betroffener, etwa zum Zwecke der Rehabilitierung oder zur Erlangung von Leistungen nach dem Häftlingshilfegesetz, werden aus diesen Unterlagen ebenso wie aus der Häftlingskartei nur sehr vereinzelt beantwortet, da die gewünschten Bestätigungen meist unmittelbar aus der Zentralen Gefangenenkartei des ehemaligen Ministeriums des Innern der DDR erteilt werden können (s. u. 4.5.3).

4.5.3 Sicherung der Daten von Strafgefangenen der ehemaligen DDR unbefriedigend

Das Bundesarchiv hat aus der ehemaligen Bundesanstalt für gesamtdeutsche Aufgaben (BfgA) deren Häftlingskartei (s. o. 4.5.2) und aus dem Ministerium des Innern der DDR die Zentrale Gefangenenkartei übernommen. Zwischenzeitlich erhielt es aus dem aufgelösten Rechenzentrum des Zentralen Einwohnerregisters auch den „Strafgefangenen- und Verhafteten-Datenspeicher" der einschließlich statistischer Aufbereitungen fast 600 Magnetbänder umfaßt. Mit Hilfe der auf Magnetbändern vorliegenden Strafgefangenen- und Verhafteten-Daten hofft das Bundesarchiv, den Datenbestand aus der Zentralen Gefangenenkartei, der ihm bis zum Jahr 1975 in Form von Filmen und ab 1976 in Form von Karteikarten vorliegt, vervollständigen zu können, um auf dieser Grundlage die Anfragen Betroffener in Rehabilitierungs- und Wiedergutmachungsverfahren beantworten zu können. Das Bundesarchiv erhält derzeit monatlich ca. 1 000 Anfragen von Betroffenen, Gerichten, Staatsanwaltschaften und anderen Landesbehörden, die zum Zweck der Rehabilitierung, zur Durchführung des Häftlingshilfegesetzes oder zum Nachweis von Versicherungszeiten Auskünfte erhalten wollen. Wie bei allen anderen Magnetbändern der ehemaligen DDR

hat das Bundesarchiv zur Zeit allerdings noch technische und finanzielle Probleme mit dem Umschreiben der Daten in eine für Lesegeräte mit West-Technik geeignete Form.

Da die Daten der Zentralen Gefangenenkartei teilweise mit denen des Strafregisters des Generalstaatsanwalts der DDR identisch sind, habe ich das Bundesarchiv darauf hingewiesen, daß nach den einschlägigen Regelungen des Bundeszentralregistergesetzes (BZRG) sowie des Ersten SED-Unrechts-Bereinigungsgesetzes der Zugang zu den Daten des Strafregisters der DDR im Interesse der Betroffenen beschränkt ist. Zwar sollen die Daten der Zentralen Gefangenenkartei zum Zweck der Rehabilitierung und für Leistungen nach dem Häftlingshilfegesetz zugänglich sein. Vermieden werden muß aber, daß Dritte — und sei es auf dem Weg über den Betroffenen — Informationen erlangen, die ihnen bei inhaltlich gleichen Auskunftsersuchen an das Bundeszentralregister nicht zustehen. Deshalb habe ich das Bundesarchiv gebeten, sich bei seiner Auskunftspraxis an den Regelungen des BZRG und des Ersten SED-Unrechts-Bereinigungsgesetzes zu orientieren und mit Auskünften zurückhaltend zu sein, bei denen Anhaltspunkte für das Risiko eines Mißbrauchs bestehen. Auch ist darauf zu achten, daß nur die zur Erreichung des jeweiligen Auskunftszweckes erforderlichen Daten übermittelt werden. Bei Anfragen von Landesversorgungsämtern und Arbeitsämtern ist beispielsweise der Haftgrund nicht mitzuteilen.

Hinsichtlich der Verwendung der Zentralen Gefangenenkartei zu Forschungszwecken habe ich die Ansicht vertreten, daß eine Übermittlung personenbezoger Daten für diese Zwecke derzeit nicht zulässig ist. Denn nach § 5 BArchG darf das Archivgut grundsätzlich erst 30 Jahre nach dem Tod des Betroffenen genutzt werden. Um die Betroffenen durch die Speicherung ihrer Daten im Bundesarchiv nicht unangemessen zu benachteiligen, dürfen deshalb für Forschungszwecke derzeit grundsätzlich nur anonymisierte Daten zur Verfügung gestellt werden.

Da die Sicherung der Zentralen Gefangenenkartei gegen unbefugte Zugriffe ebenso unbefriedigend war wie die Unterbringung der Häftlingskartei der ehemaligen BfgA, habe ich dem BMI und dem Bundesarchiv Anregungen zur sichereren Verwahrung der Datenträger in den Arbeitsräumen gegeben und empfohlen, auch die Türen zu diesen Räumen zu verstärken, weil der Zutritt zum Gebäude nicht wirksam kontrolliert werden kann. Eine Reaktion darauf lag mir bei Redaktionsschluß noch nicht vor.

4.6 Nicht mehr benötigte Daten aus der Aufnahme von Übersiedlern vernichtet — Heimatortskartei Gießen —

Ein anderer durch die deutsche Teilung veranlaßter Datenbestand, dem meine besondere Aufmerksamkeit auch im Berichtszeitraum galt, betraf die Übersiedlung von Bürgern der ehemaligen DDR in die Bundesrepublik Deutschland. Die entsprechenden Akten waren bei der Dienststelle des Bundesnotaufnahmeverfahrens in Gießen entstanden und sind nun auf das Bundesverwaltungsamt übergegangen. Im Berichtszeitraum hat mich besonders die sog. Heimatortskartei Gießen beschäftigt. Die Dienststelle des Bundesnotaufnahmeverfahrens in Gießen hat in dieser Datei seit etwa 1966 Daten über Übersiedler aus der ehemaligen DDR — geordnet nach ihren ehemaligen Wohnsitzen — gesammelt. Die Datei diente nach meinen Erkenntnissen in erster Linie Zwecken der Ausgleichsverwaltungen, die mit Hilfe dieser Daten Personen, z. B. ehemalige Nachbarn, die Auskunft zu von Übersiedlern angemeldeten, in der ehemaligen DDR erlittenen Vermögensschäden geben konnten, feststellen wollten.

Schon vor der Herstellung der Deutschen Einheit habe ich wiederholt auf das Fehlen einer klaren gesetzlichen Grundlage für diese Datei hingewiesen und unter Gesichtspunkten der Erforderlichkeit Zweifel an ihrer Zuverlässigkeit geltend gemacht. Im Hinblick auf die politische Entwicklung hat das Bundesministerium des Innern Anfang 1990 auf meine erneuten Fragen zur weiteren Notwendigkeit der Heimatortskartei zunächst eine Übergabe an das Bundesarchiv oder eine Abgabe an das Bundesausgleichsamt erwogen. Dort sollte wiederum geprüft werden, ob eine Abgabe an das Bundesamt zur Regelung offener Vermögensfragen zweckmäßig sei. Meine Fragen nach der Erforderlichkeit und nach der Rechtsgrundlage blieben jedoch unbeantwortet. Im Sommer 1992 erklärte dann der Präsident des Bundesausgleichsamtes, daß er seine Bedenken gegen eine Vernichtung der Heimatortskartei nicht mehr aufrechterhalte. Mit der durch das Bundesverwaltungsamt vollzogenen Anordnung des Bundesminsteriums des Innern, diese Kartei zu vernichten, hatten meine Bemühungen endlich Erfolg.

4.7 54-seitiger Fragebogen wird mindestens halbiert — Aussiedleraufnahmeverfahren —

Im Juli 1990 ist das Gesetz zur Regelung des Aufnahmeverfahrens für Aussiedler (Aussiedleraufnahmegesetz) in Kraft getreten (vgl. 13. TB S. 37f.).

Um zu überprüfen, wie sich das Aussiedleraufnahmegesetz unter Aspekten des Datenschutzes bewährt, habe ich im Sommer 1991 eine große Außenstelle des Bundesverwaltungsamtes, das für die Durchführung des Aussiedleraufnahmeverfahrens zuständig ist, kontrolliert.

Das Aussiedleraufnahmeverfahren gliedert sich in ein schriftliches Aufnahmeverfahren und in ein mündliches Verfahren, das sogenannte Erstaufnahmeverfahren. Durch das schriftliche Aufnahmeverfahren, das der Aussiedler von seinem bisherigen Wohngebiet aus betreiben muß, soll sichergestellt werden, daß nur solche Personen als Aussiedler in die Bundesrepublik Deutschland einreisen, die mit hoher Wahrscheinlichkeit den Anforderungen des Gesetzes entsprechen. Um dies feststellen zu können, hat der Betroffene einen 54seitigen Aufnahmeantrag auszufüllen, mit

dem eine Fülle von personenbezogenen Daten erhoben wird.

Bei näherer Prüfung hat sich gezeigt, daß ein nicht unbeträchtlicher Teil dieser Angaben für die Feststellung der Rechtsstellung als Deutscher nicht erforderlich ist. Ich habe daher eine deutliche Reduzierung gefordert. Für die GUS-Staaten wird vom Bundesministerium des Innern im Zusammenwirken mit dem Bundesverwaltungsamt derzeit eine Reduzierung des Umfangs des Aufnahmeantrages auf — je nach Einzelfall — 17 bis 28 Seiten vorbereitet. Eine Überarbeitung der Aufnahmeanträge für weitere Herkunftsgebiete soll folgen. Ich hoffe, daß diese Bemühungen, die nicht nur dem Schutz des Persönlichkeitsrechts sondern auch der Verwaltungsvereinfachung dienen, nunmehr zügig voranschreiten.

Nach der Einreise durchläuft der Aussiedler das mündliche Verfahren, in dessen Verlauf die im schriftlichen Verfahren gemachten Angaben des Aussiedlers in dessen Anwesenheit nochmals überprüft werden. Als Ergebnis dieses Verfahrens erhält der Aussiedler den Registrierschein, der Voraussetzung für die Gewährung bestimmter Vergünstigungen, zum Beispiel des Überbrückungsgeldes, ist.

In einer vom Bundesverwaltungsamt entwickelten Laufkarte werden dem Aussiedler die Stationen benannt, die er während seiner Anwesenheit in der Aufnahmeeinrichtung aufsuchen muß. Dazu zählen zum Beispiel die Arbeitsverwaltung, aber auch Stellen der Sicherheitsbehörden. Diese verfolgen eigene Zwecke, die mit dem Aufnahmeverfahren nichts zu tun haben. Die Laufkarte, die dem Aussiedler durch Angehörige des Bundesverwaltungsamtes übergeben wird, suggeriert diesem aufgrund ihrer Gestaltung allerdings, daß alle aufgeführten Stationen Verfahrensschritte im Aussiedleraufnahmeverfahren seien. Dazu kommt, daß die Nachrichtendienste weder auf der Laufkarte noch nach der Ausschilderung unter ihrer Behördenbezeichnung aufgeführt sind, sondern neutrale, nichtssagende Bezeichnungen, wie z. B. „HBW" (d. i. Hauptstelle für Befragungswesen), tragen. Ich habe das Bundesministerium des Innern gebeten, hier für mehr Transparenz für den Betroffenen zu sorgen. Es hat mir mitgeteilt, daß die Abstimmung zwischen den beteiligten Behörden noch nicht abgeschlossen sei.

Eine besondere Rolle im Verfahrensablauf nimmt das Deutsche Rote Kreuz ein, das damit beauftragt ist, die Fahrt- und Gepäckbeförderungskosten sowie die Kosten für die Beschaffung von Pässen und Sichtvermerken des Aussiedlers abzurechnen. Im Rahmen der Kontrolle haben meine Mitarbeiter festgestellt, daß dem Deutschen Roten Kreuz jedoch mehr Daten zur Verfügung gestellt wurden, als es dafür benötigt. Die notwendige Korrektur ist inzwischen erfolgt.

Das Deutsche Rote Kreuz erhält darüber hinaus für seinen in Hamburg betriebenen Suchdienst aus dem Aussiedleraufnahmeverfahren eine Vielzahl personenbezogener Daten, die es nach eigenen Angaben für Zwecke der Familienzusammenführung und für die Betreuung von Aussiedlern in ihren derzeitigen Wohngebieten benötigt und nutzt (s. auch 4.8).

4.8 Suchdienst des Deutschen Roten Kreuzes

Das Deutsche Rote Kreuz (DRK) unterhält als unselbständigen Teil seiner Organisation einen Suchdienst nach Kriegs- und Zivilgefangenen, Wehrmachtsvermißten und Zivilverschleppten des Zweiten Weltkrieges. Aufgrund einer Vereinbarung mit dem damaligen Bundesminister für Vertriebene, Flüchtlinge und Kriegsgeschädigte aus dem Jahre 1958 nimmt es als beliehener Unternehmer Aufgaben der Bundesrepublik Deutschland wahr, wird vom Bundesministerium des Innern finanziert und unterliegt damit als öffentliche Stelle im Sinne von § 2 Abs. 4 Satz 2 BDSG meiner datenschutzrechtlichen Kontrolle. Bei der Überprüfung des Aussiedleraufnahmeverfahrens (s. o. 4.7) habe ich festgestellt, daß das DRK unter der Bezeichnung „Suchdienst des DRK" dabei Hilfe leistet und daß ihm auch in diesem Verfahren erhobene Daten für Zwecke des Suchdienstes übermittelt werden. Ich habe dies zum Anlaß genommen, die beiden Zentralstellen des Suchdienstes in Hamburg und München zu kontrollieren.

Der Suchdienst in Hamburg widmet sich mit etwa 460 Mitarbeitern der Familienzusammenführung von Deutschen aus osteuropäischen Ländern sowie der humanitären Hilfe für im Ausland lebende und dort verbleibende Deutsche. Ein Teil seiner Aktivitäten steht in engem Zusammenhang zum Aussiedleraufnahmeverfahren, so die Beratung potentieller Aussiedler, gutachterliche Tätigkeit, die Unterstützung des Antragstellers im Anerkennungsverfahren, die Organisation und Abrechnung der Ausreise aus dem Herkunftsland sowie die Hilfe bei der Erstaufnahme in der Bundesrepublik Deutschland.

In München arbeiten noch etwa 77 Mitarbeiter an der Aufklärung von Verschollenenschicksalen, dem traditionellen Tätigkeitsschwerpunkt des Suchdienstes. Die besseren Informationsbeziehungen mit den Staaten der ehemaligen Sowjetunion haben in den letzten Jahren in diesem Aufgabenbereich neue Möglichkeiten eröffnet. Derzeit werden Listen von Verschollenen für die automatisierte Datenverarbeitung erfaßt, um sie mit aus der Gemeinschaft Unabhängiger Staaten gelieferten oder noch erwarteten Aufstellungen von Todesfällen Kriegsgefangener abgleichen zu können und so Verbleib oder Grabstätten Vermißter zu finden. Auch heute kommt es noch zu zahlreichen Suchanfragen, die oft mit Hilfe der aus Anlaß der DRK-Hilfeleistungen angelegten umfangreichen Personenkartei des Suchdienstes oder aufgrund eigener Recherchen beantwortet werden können. Sieht der Suchdienst eine Chance, daß die Vermittlung des Kontakts zu einer von ihm festgestellten Person (sei es der Gesuchte selbst, sei es eine dritte Person) zur Aufklärung beitragen könnte, so wird diese von der Anfrage benachrichtigt und ihr Gelegenheit gegeben, mit dem Suchenden Kontakt aufzunehmen. Äußert sie sich ablehnend oder gar nicht, wird dem Suchenden mitgeteilt, daß sie kein Interesse an einer Kontaktaufnahme bekundet hat und ihre Anschrift daher nicht mitgeteilt werden kann.

Der Suchdienst hat seine Ursprünge in vorkonstitutioneller Zeit. Er ist nicht aufgrund staatlicher Organisa-

tionsentscheidung und definierter Aufgabenzuweisung entstanden; er wuchs vielmehr als Teil der Aufgaben, die das Deutsche Rote Kreuz im Spannungsfeld zwischen Ost und West den jeweiligen Gegebenheiten entsprechend mit einer gewissen Staatsferne und orientiert an seinem humanitären Anliegen zu bewältigen hatte. Gleichwohl muß sich der Suchdienst des DRK mit seinen so gewachsenen Strukturen an den Maßstäben des Persönlichkeitsrechtsschutzes messen lassen. Hierbei habe ich besonders auf § 29 des Bundesvertriebenengesetzes (BVFG) in der Fassung des Aussiedleraufnahmegesetzes vom 28. Juni 1990 hingewiesen. Danach dürfen *„im Aufnahmeverfahren mitwirkende Behörden"* — soweit es zur Feststellung der Voraussetzungen nach § 27 BVFG, d. h. zur Feststellung der Anspruchsvoraussetzungen für einen Aufnahmebescheid, erforderlich ist — bei ihnen vorhandene personenbezogene Daten nutzen, beim Betroffenen erheben und — hilfsweise — auch von anderen öffentlichen oder nicht-öffentlichen Stellen beziehen. Die im Aufnahmeverfahren gesammelten Daten dürfen grundsätzlich *„nur für Zwecke dieses Verfahrens"* genutzt und übermittelt werden. Ich halte es für vertretbar, bei der Auslegung dieser Gesetzesnormen davon auszugehen, daß das DRK insoweit rechtmäßiger Empfänger der ihm durch das Bundesverwaltungsamt übermittelten personenbezogenen Daten ist und darüber hinaus eine gesetzliche Befugnis zur Erhebung personenbezogener Daten beim Betroffenen insoweit hat, als es mitwirkende Funktionen oder Hilfsfunktionen im Aussiedleraufnahmeverfahren übernommen hat und die Daten ausschließlich diesem Zweck dienen. Notwendig ist daher zu definieren, welche der vom DRK übernommenen Aufgaben zum Aussiedleraufnahmeverfahren gezählt werden können. Der historische Begriff des „Suchdienstes" ist für die Abgrenzung dieser Funktionen kaum hilfreich. Vielmehr hat sich ergeben, daß es — wie schon beschrieben — Funktionen im Aufnahmeverfahren gibt, die bei genauer Betrachtung schwerlich als „Suchdienst" bezeichnet werden können; umgekehrt gibt es Funktionen des „Suchdienstes", die auch bei großzügiger Auslegung nicht dem Aussiedleraufnahmeverfahren zugerechnet werden können. Als noch zu diesem Verfahren gehörend betrachte ich bestimmte Arbeiten des DRK schon vor dem Ergehen eines Aufnahmebescheides, so bestimmte Archivfunktionen und die Beratung und Hilfe im Anerkennungsverfahren, Abwicklungshilfe bei der Ausreise aus dem Herkunftsland und die Hilfe nach der Einreise in die Bundesrepublik. Die Mitwirkung am Aussiedleraufnahmeverfahren kann jedoch erst dann einsetzen, wenn tatsächlich ein „Aussiedler" auftritt: Sie kann sich mithin nur auf Personen beziehen, die das in der Einreise in die Bundesrepublik mündende Verfahren betreiben oder zumindest konkret in nächster Zeit beabsichtigen.

Keine Beziehung zum Aufnahmeverfahren vermag ich hingegen dort zu erkennen, wo es um die Auslandshilfe des DRK für im Ausland Verbleibende geht. Dies gilt auch für die traditionellen Aufgaben des Suchdienstes, wie sie mir in München erläutert wurden. Ich begrüße daher, daß das Bundesverwaltungsamt Daten aus dem Aussiedleraufnahmeverfahren nicht mehr an den Suchdienst München übermittelt. Generell ist zu beachten, daß in der Suche nach einer bestimmten anderen Person keine Einwilligung liegt, daß die eigenen Daten für eine Suche Dritter zur Verfügung stehen und zu diesem Zweck gespeichert werden. Die Zweckänderung sehe ich auch nicht durch § 14 Abs. 2 BDSG gerechtfertigt; insbesondere ist mir — wie es Absatz 2 Nr. 3 verlangt — nicht offensichtlich, daß die Zweckänderung in jedem Fall im Interesse des Betroffenen liegen soll — gerade auch weil es immer wieder vorkommt, daß Gesuchte die Kontaktaufnahme zu Suchenden ablehnen. Mit Rücksicht auf die gewachsenen Strukturen des Suchdienstes erscheint mir eine Datenspeicherung allenfalls unter dem Gesichtspunkt hinnehmbar, daß — wie mir als Praxis des Suchdienstes in München erläutert wurde — bei Vorliegen einer weiteren Suchnachfrage der Betroffene nachträglich um Einwilligung in die Verwendung seiner Daten zur Herstellung des Kontaktes mit den suchenden Dritten gebeten wird. In diesem Zusammenhang habe ich angeregt, das Verfahren des Suchdienstes den zu ihm in Kontakt Tretenden besser transparent zu machen.

4.9 Darf ein Bundesministerium eine Eingabe stets an eine andere — zuständige — Behörde abgeben?

Die Gemeinsame Geschäftsordnung der Bundesministerien — Allgemeiner Teil (GGO I) bestimmt, daß ein Vorgang unverzüglich an eine andere oberste Bundesbehörde abzugeben ist, wenn diese offensichtlich zuständig ist (§ 20 Abs. 3 GGO I). Zur Frage, ob der Betroffene dem zugestimmt haben muß, enthält die Geschäftsordnung keine Aussage. Durch die Eingabe eines Bürgers bin ich auf die Frage aufmerksam geworden, ob damit eine Regelung getroffen ist, die als „andere Rechtsvorschrift des Bundes" nach § 1 Abs. 4 BDSG dem Bundesdatenschutzgesetz vorgeht, so daß bei der Abgabe immer auf die Zustimmung des Betroffenen verzichtet werden könnte.

In dem von mir überprüften Fall hatte das Auswärtige Amt eine an dessen damaligen Minister *vor allem* in seiner Eigenschaft als „Delegationsleiter der KSZE-Konferenzen" gerichtete Petition, mit der der Bürger die Verletzung „seiner Grund- und Menschenrechte" durch eine andere oberste Bundesbehörde geltend machte, eben dieser zur weiteren Bearbeitung übersandt. Das Auswärtige Amt berief sich dabei auf § 20 Abs. 3 GGO I, weil es den materiellen Gehalt der Eingabe, die behauptete Beeinträchtigung des Bürgers, — zutreffend — als eine Frage ansah, die die Zuständigkeit der anderen obersten Bundesbehörde berührte. Es hatte aber nicht ausreichend berücksichtigt, daß eine Abgabe hier nicht im Sinne des Bürgers war: Dieser hatte sich gerade deshalb an den damaligen Bundesminister des Auswärtigen gewandt, weil er bei der anderen obersten Bundesbehörde, an deren Verhaltensweise er in seiner Petition nachdrücklich Kritik geübt hatte, mit seinem Anliegen — trotz mehrerer Versuche — nach seiner Auffassung ohne Erfolg geblieben war.

Hier wäre es erforderlich gewesen, anhand des materiellen Gehalts der Petition zu prüfen, ob die Abgabe

an die andere oberste Bundesbehörde ohne ausdrückliche Zustimmung des Betroffenen zulässig war. Dies ergibt sich aus § 15 BDSG, der von § 20 Abs. 3 GGO I nicht verdrängt wird. Die GGO I ist kein Gesetz und daher keine Rechtsgrundlage zur Einschränkung des informationellen Selbstbestimmungsrechts. Sie weist auch nicht die besondere Rechtsqualität auf wie die nach Artikel 65 Satz 4 GG von der Bundesregierung beschlossene Geschäftsordnung der Bundesregierung. Vielmehr ist die GGO I lediglich eine aus der Organisationsgewalt der Bundesregierung abgeleitete Verwaltungsvorschrift. Selbst wenn man auch die GGO I als eine Geschäftsordnung des Staatsorgans Bundesregierung und damit als autonomes Recht einstuft, handelt es sich doch nur um sogenanntes Binnenrecht, d. h. ein Recht ohne Auswirkung auf einzelne Bürger, das nur für die Mitarbeiter der Bundesministerien verbindlich ist (s. § 1 Abs. 3 Satz 1 GGO I). § 20 Abs. 3 GGO I regelt also für den Fall der Unzuständigkeit einer obersten Bundesbehörde ein bestimmtes Verfahren, bietet aber keine Grundlage für die Übermittlung personenbezogener Daten von einem Ministerium an ein anderes.

Ich habe das Auswärtige Amt unter Darlegung dieser Gesichtspunkte gebeten, Eingaben künftig sorgfältig daraufhin zu überprüfen, ob die nach dem Wortlaut von § 20 Abs. 3 GGO I vorgeschriebene Abgabe an eine andere oberste Bundesbehörde mit der Intention des Bürgers übereinstimmt und im Zweifel die Einwilligung des Betroffenen einzuholen.

Dieser Empfehlung ist das Auswärtige Amt durch Rundschreiben an alle Organisationseinheiten in seinem Hause und Erlaß an alle diplomatischen und berufskonsularischen Vertretungen gefolgt.

4.10 Auslandsvertretungen

4.10.1 Diskretionszonen eingerichtet

Bei den Auslandsvertretungen der Bundesrepublik Deutschland wurden im Berichtszeitraum Diskretionszonen eingerichtet. Der Auswärtige Dienst entspricht damit einer Tendenz, die sich seit etwa fünf Jahren in weiten Bereichen des öffentlichen und privatwirtschaftlichen Dienstleistungssektors auch in Deutschland durchgesetzt hat.

Durch Wartelinien auf dem Fußboden und entsprechende Hinweise kann ein ausreichender Abstand zwischen dem bedienten Besucher und dem hinter ihm oder seitlich vor einem Schalter wartenden anderen Besucher erreicht und das Mithören von Gesprächen sowie das Einsehen in Unterlagen weitgehend ausgeschlossen werden. Auf meine Empfehlung hin hat das Auswärtige Amt die Auslandsvertretungen bereits Anfang 1989 auf die schutzwürdigen Belange der betroffenen Besucher hingewiesen und nach dem erfolgreichen Versuch im Bereich der Post (s. 11. TB S. 36) Ende 1990 die Auslandsvertretungen unter Vorgabe genauer Kriterien angewiesen, Diskretionszonen einzurichten, falls die entsprechenden räumlichen Gegebenheiten vorhanden sind. In dem Runderlaß heißt es außerdem, das Auswärtige Amt werde bei künftigen Neubauten und bei der erstmaligen Herrichtung von angemieteten Gebäuden Diskretionszonen *grundsätzlich* einplanen.

Durch die Eingabe eines Bürgers bin ich Anfang 1992 darauf hingewiesen worden, daß im Generalkonsulat Istanbul im Rechts- und Konsularbereich noch keine entsprechenden Maßnahmen ergriffen worden waren. Auf meine Nachfrage hin habe ich vom Auswärtigen Amt erfahren, daß dies jedoch kurz darauf geschehen ist.

Es ist erfreulich, daß das Auswärtige Amt die dargestellten Maßnahmen getroffen hat. Ein besserer Schutz vertraulicher Gespräche wäre allerdings durch bauliche Maßnahmen wie Sprechkabinen oder sogenannte Schalterzimmer zu erreichen. Ich würde es daher begrüßen, wenn das Auswärtige Amt, wie in einigen Auslandsvertretungen geschehen, in weiterem Umfang als bisher entsprechende Maßnahmen träfe.

4.10.2 Unverschlüsselte Übermittlungen empfindlicher Informationen an und von Auslandsvertretungen sind riskant

Bei der Mitwirkung des Bundesverwaltungsamtes (BVA) am automatisierten Visaverfahren zwischen den Auslandsvertretungen und dem BVA werden bestimmte Daten *unverschlüsselt* per Telex übermittelt.

Nach Kontrollbesuchen bei den Botschaften in Ankara und Moskau sowie beim Generalkonsulat Istanbul habe ich bereits 1990 diese Datenübertragungen kritisiert und das Auswärtige Amt aufgefordert, angemessene Maßnahmen der Datensicherheit im Fernschreibverkehr, d. h. kryptographische Verschlüsselung, einzuführen. Das Auswärtige Amt hat daraufhin „erwogen", den Fernschreibverkehr des Visaverfahrens in das *geplante, weltweite Kommunikationsnetz der Bundesregierung* einzubeziehen, für das eine vollständige Kryptierung vorgesehen war. Dieses Netz wäre nach Darstellung des Auswärtigen Amtes ohne „nennenswerten, zusätzlichen Aufwand mitbenutzbar gewesen". Nach Auskunft des Auswärtigen Amtes ist dieses Projekt jedoch in absehbarer Zeit nicht realisierbar. Die in Betracht kommende *Ersatzlösung*, nämlich die Beschaffung von Ver- und Entschlüsselungsgeräten für die Auslandsdienststellen, verursacht nach Darlegung des Auswärtigen Amtes einen hohen Aufwand an Sach- und Personalkosten.

Das Auswärtige Amt hat mir inzwischen aber auch mitgeteilt, es wolle mit dem BVA in Kürze über die künftigen Übertragungs- und Verschlüsselungsmodalitäten sprechen. Dieses Vorhaben begrüße ich, da eine Verschlüsselung des Telexverkehrs von und zu den Auslandsvertretungen besonders in Visa-Angelegenheiten insbesondere zum Schutz der Betroffenen — aber nicht nur deshalb — geboten ist. Auch die Einrichtung des Schengener Informationssystems (SIS) zwingt noch im Jahr 1993 (s. 24.1.2) dazu, die geforderten Verbesserungen durchzuführen. Über das SIS wird im Rahmen des Visaverfahrens nämlich auch auf Daten der Partner-Staaten des Schengener Abkommens zugegriffen. Die Verpflichtung der Bun-

desregierung nach dem Schengener Durchführungsübereinkommen, für ihren „nationalen Teil" des SIS die Maßnahmen zu treffen, die *verhindern*, daß personenbezogene Daten bei der Übermittlung unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Artikel 118 Abs. 1 lit. h), erstreckt sich auch auf personenbezogene Daten, die durch Zugriffe nach Artikel 101 Abs. 2 des Übereinkommens, wie sie im Visaverfahren erfolgen, erlangt worden sind. Gerade auch wegen dieser völkerrechtlichen Verpflichtung aus dem Schengener Durchführungsübereinkommen halte ich es für dringend geboten, die Datensicherheit im Visaverfahren zu verbessern.

Um die Frage der Datensicherheit ging es auch, als ich die Verarbeitung personenbezogener Daten auf Arbeitplatzcomputern in einer Auslandsvertretung kontrollierte. Ich hatte bereits anläßlich früherer Informations- und Kontrollbesuche bei anderen Auslandsvertretungen auf Sicherheitsmängel im Zusammenhang mit dem Betrieb von Arbeitsplatzcomputern hingewiesen. Nachdem mir notwendige Sicherheitsmaßnahmen damals zwar in Aussicht gestellt, aber immer noch nicht durchgeführt worden waren und nur auf die Abschreibung der derzeit eingesetzten PC sowie deren Ersatz durch Geräte neueren Typs verwiesen wurde, habe ich die Mängel beanstandet. Das vom Auswärtigen Amt in seiner Antwort vor allem aufgeführte Argument, die von mir empfohlene Installation von Sicherheitssoftware (ggf. mit Hardwarezusatz) bei den vorhandenen Geräten sei wegen der hierfür erforderlichen umfangreichen Reisetätigkeit von Fachpersonal und dessen damit verbundener häufiger Abwesenheit von der Zentrale unverhältnismäßig aufwendig, überzeugt mich bisher nicht. Ich gehe der Frage weiter nach.

5 Rechtswesen

5.1 Änderungen des Strafverfahrensrechts

5.1.1 Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG)

Mitte September 1992 ist nach langen Vorbereitungen das Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG) in Kraft getreten. Wer meinte, mit der Schaffung der hierin enthaltenen neuen und besonders tiefgreifenden Eingriffsbefugnisse für die Strafverfolgungsbehörden sei der Ruf namentlich von prominenten Vertretern der Polizei nach weitergehenden Befugnisnormen einstweilen verhallt, sieht sich indessen getäuscht.

Um meine wichtigste Aussage vorweg zu nehmen: Ich gehöre nicht zu denen, die das Gesetz und damit den Gesetzgeber schelten. Wenn auch meine zum Schutze der Persönlichkeitsrechte der Bürger gegebenen Empfehlungen nicht alle berücksichtigt wurden, trete ich dafür ein, den in schwieriger Abwägung zwischen dem Schutz des Persönlichkeitsrechts und der Privatsphäre einerseits sowie dem staatlichen Strafverfolgungsinteresse andererseits gefundenen Kompromiß zu akzeptieren, mit weiteren Forderungen an den Gesetzgeber — sei es in dieser oder jener Richtung — einstweilen innezuhalten und zunächst einmal mit dem neugeschaffenen gesetzlichen Instrumentarium Erfahrungen zu sammeln.

Angesichts immer wieder aufkommender Vorwürfe, der Datenschutz beeinträchtige die Bemühungen um die innere Sicherheit, wiederhole ich, was ich schon in meinem 13. Tätigkeitsbericht (S. 38f.) gesagt habe: Die zunehmenden Herausforderungen, denen die Bürger unseres Staates durch die Organisierte Kriminalität, insbesondere durch die Drogenkriminalität, ausgesetzt sind, machen es notwendig, den Strafverfolgungsorganen weitergehende Befugnisse einzuräumen, auch wenn damit Eingriffe in die Freiheitsrechte der Bürger verbunden sind. Der Datenschutz hat sich deshalb von Anfang an nicht den Bemühungen entgegengestellt, die notwendigen Vorschriften zur Bekämpfung des illegalen Rauschgifthandels und der Organisierten Kriminalität zu schaffen. Wie in der — gegen die Stimme Bayerns — gefaßten Entschließung der Konferenz der Datenschutzbeauftragten vom 25. Juni 1991 (Anlage 2) zum Ausdruck kommt, war für mich und die Mehrzahl meiner Kollegen in den Ländern aber nicht einzusehen, daß unter dem Deckmantel dieser Zwecke in das Strafverfahrensrecht weit über die Bekämpfung solcher Straftaten hinaus neue Ermittlungsmethoden eingeführt werden sollten, die tief in die Privatsphäre auch unverdächtiger und unbeteiligter Bürger eingegriffen hätten (vgl. auch die Entschließung der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juni 1990 — gegen die Stimme Bayerns —, 13. TB Anlage 5 Seite 103).

Vor diesem Hintergrund läßt sich mit Blick auf das verabschiedete Gesetz unter dem Vorbehalt notwendiger Erfahrungen bei seiner Anwendung aus meiner Sicht eine insgesamt akzeptable Bilanz für das Ergebnis meiner Beratung des Gesetzgebers ziehen. Einige Punkte möchte ich nennen:

— Das Gesetz (wie schon der in dieser Legislaturperiode neu eingebrachte Gesetzentwurf des Bundesrates — BR-Drucksache 12/989 —) bedient sich des konturlosen Begriffs der „Straftat von erheblicher Bedeutung" als Anknüpfungspunkt für besondere Eingriffsmaßnahmen deutlich in geringerem Umfang, als das noch in dem in der vorherigen Legislaturperiode eingebrachten Bundesratsentwurf der Fall war (zur Kritik vgl. 13. TB S. 38f.). Dies kommt meiner Forderung entgegen, zum Schutze der Persönlichkeitsrechte der Bürger klare Rechtsgrundlagen zu schaffen; es trifft sich auch mit den Forderungen der Rechtsanwender, ihnen das Verständnis der Rechtsvorschriften möglichst leicht zu machen. Ein erfreulicher Schritt ist daher die Einführung der Straftatenkataloge für die Rasterfahndung (§ 98a StPO) und für den Einsatz eines Verdeckten Ermittlers (§ 100a StPO), auch wenn dieser Schritt zugleich für den Einsatz technischer Observationsmittel (§ 100c Abs. 1 Nr. 1b StPO) und die polizeiliche Beobachtung (§ 163e StPO) nicht getan worden ist.

— Nicht Gesetz geworden ist der vom Bundesrat vorgeschlagene sog. kleine Lauschangriff in die Wohnung, d. h. das Abhören oder Aufzeichnen des

in einer Wohnung nichtöffentlich „im Beisein eines nicht offen ermittelnden Beamten" gesprochenen Wortes sowie das unter diesen Voraussetzungen erfolgende Herstellen von Lichtbildern und Bildaufzeichnungen in einer Wohnung (§ 100 c Abs. 2 StPO i. d. F. BT-Drucksache 12/989). Auf die damit noch nicht abgeschlossene generelle Diskussion um den Lauschangriff gehe ich nachfolgend (unter 5.1.3) besonders ein.

— Sogenannte Subsidiaritätsklauseln sind in die Gesetzesfassung zusätzlich eingeführt oder gegenüber den Entwurfsvorschlägen verbessert worden: So sind z. B. die Herstellung von Lichtbildern und Bildaufzeichnungen als Maßnahmen gegen „andere Personen" als Beschuldigte nicht schon — wie ursprünglich vorgesehen — immer zulässig, wenn sie zur Erforschung des Sachverhalts „geeignet" sind. Hinzu kommen muß nunmehr, daß die Erreichung dieses Zweckes „auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre" (§ 100c Abs. 2 Satz 2 StPO).

— Auch die Verfahren, in welchen die besonderen Maßnahmen angeordnet werden, wurden im Vergleich mit dem Entwurf der vorherigen Legislaturperiode verbessert. Die Hilfsbeamten der Staatsanwaltschaft (Polizei) sind nicht mehr zur Anordnung der Rasterfahndung (§ 98b Abs. 1 StPO) befugt. Die Anordnung der polizeilichen Beobachtung (§ 163e Abs. 4 StPO) steht nunmehr unter dem Vorbehalt richterlicher Entscheidung. Nicht durchgesetzt hat sich dagegen meine Empfehlung, auch beim Einsatz eines Verdeckten Ermittlers (§ 110b Abs. 1 und 2) auf eine Eilkompetenz jedenfalls der Hilfsbeamten der Staatsanwaltschaft zu verzichten. Ebenso wie bei der Rasterfahndung sind hier regelmäßig gründliche Vorbereitungen für einen erfolgreichen Einsatz nötig, so daß ich ein Bedürfnis für eine Eilkompetenz nach wie vor nicht zu erkennen vermag.

— Bei Maßnahmen, die — wie die Rasterfahndung und die polizeiliche Beobachtung — unter Richtervorbehalt stehen, hätte ich mir auch eine klare gesetzliche Aussage gewünscht, was geschehen soll, wenn die richterliche Bestätigung ausbleibt oder der Richter es ablehnt, eine im Rahmen der Eilkompetenz getroffene Maßnahme zu bestätigen. Nach vorherrschender Auffassung steht dies einer Verwertung der erlangten Erkenntnisse grundsätzlich nicht entgegen — so wenn der Täter bereits vor der Bestätigung ermittelt worden ist und die Staatsanwaltschaft auf einen Antrag verzichtet oder der Richter die Bestätigung mit der Begründung der Zweckerreichung ablehnt. Dementsprechend geht offenbar auch das Gesetz davon aus, die Eilanordnung bedürfe nicht der Bestätigung ihrer Rechtmäßigkeit, wenn sie innerhalb von drei Tagen vollzogen wird, und ein Verwendungsverbot werde nur durch die richterliche Feststellung ausgelöst, daß die Eilmaßnahme von vornherein rechtswidrig war. Ich hätte es begrüßt, wenn die Verwertung der Daten im jedem Fall von einer richterlichen Bestätigung der Rechtmäßigkeit der Maßnahme abhängig gemacht worden wäre.

— Als Merkposten für eine künftige Überprüfung der Erfahrungen mit dem OrgKG betrachte ich auch die Thematik der Zweckbindungen und Verwertungsverbote für die mit Hilfe besonderer Eingriffsmaßnahmen (wie §§ 98b Abs. 3, 100b Abs. 5, 100d Abs. 2 und 110e StPO) gewonnenen Daten. Es liegt nahe, eine Verwertung solcher Daten nur für die Verfolgung von anderen Straftaten von *ähnlicher Schwere* zuzulassen. Unter Gesichtspunkten der Verhältnismäßigkeit halte ich eine Orientierung an dem Rahmen für geboten, für den der Gesetzgeber die besonderen Ermittlungsbefugnisse gewährt hat.

— Mit der Verbesserung des Zeugenschutzes (§ 68 StPO) wurde einer alten Forderung des Datenschutzes entsprochen.

— Als ein besonders wichtiger Punkt ist schließlich hervorzuheben, daß das Gesetz den Vorschlag des Bundesrates nicht aufgegriffen hat, durch Änderung des Fernmeldeanlagengesetzes eine Überwachung und Aufzeichnung des Fernmeldeverkehrs für bestimmte Zwecke der Gefahrenabwehr zuzulassen (Artikel 9 des Bundesrats-Entwurfs). Die Notwendigkeit einer solchen Regelung konnte im Gesetzgebungsverfahren nicht überzeugend dargelegt werden. Der Gesetzgeber ist zutreffend der Überlegung gefolgt, daß es neben den vorhandenen Befugnissen der Überwachung des Fernmeldeverkehrs zu Zwecken der Strafverfolgung (§§ 100a und 100b StPO) solcher zusätzlicher präventivpolizeilicher Befugnisse nicht bedarf.

5.1.2 Gewinnaufspürungsgesetz

In Ergänzung des OrgKG soll das Gewinnaufspürungsgesetz die Weiterverwendung von Straftatgewinnen unterbinden und damit dem organisierten Verbrechen die Triebfeder nehmen. Unter Gesichtspunkten des Datenschutzes ist das Gesetz von einschneidender Bedeutung:

Über die herkömmlichen in der Strafprozeßordnung geregelten Möglichkeiten der Strafverfolgungsbehörden, personenbezogene Daten bei Dritten zu erheben, führt es insofern hinaus, als es nicht lediglich bei diesen Dritten vorhandene, von diesen für ihre eigenen Zwecke erhobene personenbezogene Daten den Zwecken der Strafverfolgung zugänglich macht. Vielmehr werden diesen Dritten über ihre eigenen Interessen hinausgehende Pflichten zur Datenerhebung auferlegt, die allein strafprozessualen Erfordernissen dienen. Banken und andere Gewerbetreibende werden unter bestimmten Voraussetzungen verpflichtet, ihre Kunden zu identifizieren sowie die Identifizierungsangaben aufzuzeichnen und aufzubewahren. Hinzu tritt die Pflicht zur Meldung von Fällen des Verdachts einer Geldwäsche. Damit werden nichtöffentliche Stellen in einem Umfang für Zwecke der Bekämpfung und Verfolgung von Straftaten in die Pflicht genommen, der über das bisherige Maß (Zeug-

nispflicht, Pflicht zur Anzeige bestimmter geplanter Straftaten nach § 138 StGB) weit hinausgeht.

Ich habe mich dennoch der Erkenntnis nicht verschlossen, daß die Bekämpfung der Organisierten Kriminalität an der Weiterverwendung der Straftatgewinne ansetzen muß und daher im überwiegenden Allgemeininteresse zumindest auf absehbare Zeit Maßnahmen der genannten Art unausweichlich sind. Um so mehr habe ich begrüßt, daß ich bei der Vorbereitung des Gesetzentwurfes in einem frühen Stadium beteiligt worden bin. Mir kam es vor allem darauf an, die den Banken und anderen Gewerbetreibenden auferlegten Pflichten so präzise wie möglich zu bestimmen und Eingriffe in die Rechte Nicht-Verdächtiger möglichtst gering zu halten. Positiv bewerte ich namentlich die in § 10 Abs. 1 erreichte enge Zweckbindung für die Heranziehung und Verwendung der erhobenen Daten: Straftaten, die mit Geldwäschevorgängen nichts zutun haben, dürfen danach mit diesen Daten nicht verfolgt werden — ein absolutes Verwendungsverbot, das auch für die weitere Diskussion des Strafverfahrensänderungsgesetzes wegweisend sein könnte. Auch § 10 Abs. 2 des Gesetzes, der für Mitteilungen nach § 116 Abgabenordnung für Zwecke der Nachbesteuerung eine rechtskräftige Verurteilung voraussetzt, verdient datenschutzrechtlich eine positive Bewertung.

Auch in diesem Gesetz, das — wie schon gesagt — Neuland betritt, sehe ich einen schwierigen Kompromiß, mit dem zunächst einmal Erfahrungen gesammelt werden sollten, bevor zu späterer Zeit über seine Bewährung entschieden wird. Die Praxis bei Anwendung dieses Gesetzes und die damit erzielten Erfolge werden daher mit besonderer Aufmerksamkeit zu verfolgen sein.

5.1.3 Lauschangriff

Bei der Verabschiedung des OrgKG ist der Gesetzgeber dem Vorschlag des Bundesrates nicht gefolgt, auch nur den „kleinen Lauschangriff" in die Wohnung zuzulassen (s. o. 5.1.1). Das Abhören und Aufzeichnen des in einer Wohnung nicht-öffentlich gesprochenen Wortes und das Herstellen von Lichtbildern und Bildaufzeichnungen in einer Wohnung wurde damit — entsprechend einem Votum der Bundesregierung — auch für den Fall nicht zugelassen, daß es „im Beisein eines nicht offen ermittelnden Beamten" geschieht. Die weiterhin vielfach erhobene Forderung, der Polizei in bestimmten Fällen das heimliche Abhören und Herstellen von Bild- und Tonaufzeichnungen in und aus Wohnungen zu ermöglichen, ist damit freilich nicht vom Tisch. Wie seiner am 4. Juni 1992 verabschiedeten Entschließung zu entnehmen ist, hat der Deutsche Bundestag die mit dem Einsatz technischer Mittel in Wohnungen im Sinne des Artikel 13 GG verbundenen schwierigen rechtlichen — insbesondere auch verfassungsrechtlichen — Fragen im Rahmen der Beratungen des Gesetzentwurfs nicht mit der erforderlichen Sorgfalt klären können und beabsichtigt, die Beratung fortzuführen.

Ich habe in diesem zentralen Punkt der Diskussion von Anfang an betont, daß es eine Wahrheitsfindung mit allen Mitteln und um jeden Preis für Zwecke der Strafverfolgung nicht geben darf. Dem Bürger muß ein privates Refugium, eine persönliche Sphäre, bleiben, die obrigkeitlicher, insbesondere heimlicher Ausforschung zumindest für diesen Zweck entzogen ist.

Ich wende mich gegen die verharmlosende Bezeichnung des Lauschangriffes als „akustisches Beweissicherungsmittel" und versuche bewußt zu machen, daß es sich dabei um einen fundamentalen Eingriff in die Privatsphäre handelt. Bei aller Sorgfalt, die bei einer entsprechenden Anordnung angewandt wird, wird ein solcher in der überwiegenden Mehrzahl doch unschuldige Bürger treffen.

Der Lauschangriff greift in einen Grundrechtsbereich ein, dem das Grundgesetz besondere Bedeutung beimißt. Das Bundesverfassungsgericht betont in ständiger Rechtsprechung, schon lange vor dem Volkszählungsurteil von 1983, nach der Werteordnung des Grundgesetzes dürfe der Staat „durch keine Maßnahme, auch nicht durch ein Gesetz, die Würde des Menschen verletzen oder sonst über die in Artikel 2 Abs. 1 GG gezogenen Schranken hinaus die Freiheit der Person in ihrem Wesensgehalt antasten" (BVerfGE 27/1,6). Es erläutert dazu: „Damit gewährt das Grundgesetz dem einzelnen Bürger einen unantastbaren Bereich privater Lebensgestaltung, der der Einwirkung der öffentlichen Gewalt entzogen ist". Dieser Grundsatz leitet sich aus der Menschenwürde ab. Ob ein solcher Bereich wirklich „unantastbar" für jeden Menschen sein muß, ist in der Rechtsprechung zwar nicht völlig eindeutig. Klar ist aber, daß in diesen allenfalls zum Schutz der Existenz und Menschenwürde anderer eingedrungen werden darf. Hier ist ein sehr schwieriger Abwägungsprozeß vorzunehmen. Ich habe nie Bedenken dagegen erhoben, in einem eng begrenzten Bereich auch ein Eindringen in den Schutzbereich der Wohnung zuzulassen, wenn damit das Ziel verfolgt wird, erhebliche Gefahren für die Existenz und die Menschenwürde anderer abzuwehren.

Wenn zwei gleichwertige Rechtsgüter auf dem Spiel stehen, ist zu verantworten, daß das Rechtsgut des Schutzes der Wohnung gegenüber dem Leben und der Menschenwürde anderer zurücktritt. Die Polizeigesetze der Länder lassen daher nach meiner Überzeugung im Grundsatz durchaus mit Recht den Einsatz von Abhör- und Videogeräten in Wohnungen zu, wobei allerdings im Einzelfall fraglich ist, ob der Einbruch in das Grundrecht nicht in zu weitgehendem Maß zugelassen wird.

Bei aller Bedeutung, die der Verwirklichung des staatlichen Strafanspruchs zukommt, halte ich einen Eingriff in das durch die Menschenwürde geschützte private Refugium eines Menschen allein für den Zweck der Strafverfolgung mit dem Menschenbild des Grundgesetzes nicht für vereinbar.

In der Diskussion waren die Mehrzahl meiner Kollegen und ich selbst bereit, den Erfordernissen der Bekämpfung schwerer Kriminalität noch ein weiteres Stück entgegenzukommen. Wir haben keine Einwände dagegen erhoben, entsprechend einer bei der Anhörung vor dem Rechtsausschuß des Deutschen

Bundestages zum OrgKG gegebenen Anregung zu prüfen, ob z. B. Unterkünfte, die der Prostitution oder dem Glücksspiel dienen, wirklich als Wohnungen im Sinne der Vorschriften der Strafprozeßordnung angesehen werden müssen. Dafür, den vor Lauschangriffen zu Zwecken der Strafverfolgung geschützten Wohnungsbereich enger zu bemessen als er bisher in Artikel 13 GG verstanden wird, sprechen gute Gründe.

Die Forderung nach dem Lauschangriff wird vor allem auf die vom Präsidenten des Bundeskriminalamtes bei der öffentlichen Anhörung zum OrgKG aufgestellte und seitdem kritiklos immer wieder wiederholte Behauptung gestützt, in den USA würden 80 % der Aufklärungserfolge in der Organisierten Kriminalität über den Einsatz technischer Mittel erzielt. Ich habe dies zum Anlaß genommen, das Bundeskriminalamt um die Übersendung einschlägigen Materials, das diese Behauptung stützt, zu bitten.

Das Bundeskriminalamt hat mir in seiner Antwort nicht eine einzige Unterlage übermittelt, sondern erklärt, die Prozentangabe beruhe „auf Referenzen der amerikanischen Bundespolizei FBI". Ergänzend erklärte das BKA: „In einschlägigen Ermittlungsverfahren konnte die Polizei in der Vergangenheit die Erkenntnis gewinnen, daß gerade in Hinterzimmern von Gastätten, Spielcasinos, Hotels, Saunaclubs und Bordellen, schwerste Straftaten geplant und abgesprochen werden." Daraus schließe ich, daß ein Einsatz technischer Mittel in diesen Räumen den größten Teil der praktischen Erfordernisse abdecken würde. Ich habe deshalb für die weitere Rechts- und Sachdiskussion eine Differenzierung zwischen der eigentlichen Privatwohnung des Bürgers, deren Unverletzlichkeit garantiert bleiben muß, einerseits und Räumen, die allgemein zugänglich sind oder beruflicher oder geschäftlicher Tätigkeit der vom Bundeskriminalamt genannten Art dienen, andererseits empfohlen. In bezug auf Räume dieser letztgenannten Art sollte in den weiteren Beratungen geklärt werden, von welchen konkreten rechtlichen Voraussetzungen und Begrenzungen der Einsatz von Abhör- und Videoaufzeichnungsgeräten abhängig gemacht werden soll und gegen welchen Personenkreis solche Maßnahmen gezielt eingesetzt werden dürfen. Mindestvoraussetzungen für eine solche Lösung wären ein eng begrenzter abschließender Straftatenkatalog, die Verwendung der gewonnen Erkenntnisse ausschließlich zur Verfolgung dieser Straftaten, ein strikter Richtervorbehalt sowie die Wahrung besonderer Amts- und Berufsgeheimnisse.

Faßt man die nach meiner dargestellten Auffassung gegebenen Möglichkeiten für den Einsatz von Ton- und Bildaufzeichnungsgeräten durch die Polizei zusammen, so ergibt sich die Zulässigkeit des Lauschangriffs sogar im engsten Wohnungsbereich zur Abwehr schwerster Gefahren sowie die Möglichkeit zum Einsatz dieser Mittel zur Strafverfolgung mit Ausnahme der eigentlichen Privatwohnung. Damit würden nach meiner Überzeugung die wichtigsten Bedürfnisse zum Einsatz dieser Mittel abgedeckt. Andererseits würde der Gesetzgeber deutlich machen, daß er das private Refugium entsprechend der Rechtsprechung des Bundesverfassungsgerichts achtet und in diese für ein Leben in Würde so wichtige Sphäre nur einbricht, wenn es für die Wahrung eines gleichwertigen Rechtsguts unerläßlich ist. Sollte dann doch der eine oder andere Fall übrigbleiben, bei dem ein Einsatz von Abhör- und Videogeräten im engsten Wohnungsbereich ausscheidet, gilt der vom Bundeskanzler in seiner Rede vor dem Juristentag 1992 ausgesprochene Satz:

„Wir müssen immer wieder Verständnis dafür wekken, daß dem Rechtsstaat Grenzen gesetzt sind, die dem spontanen Rechtsempfinden vieler nicht immer entsprechen. Wir müssen akzeptieren, daß der Rechtsstaat mit dieser Selbstbindung auch diejenigen schützt, die es moralisch vielleicht gar nicht verdienen. Diese Beschränkung schützt uns alle, und sie schützt den Rechtsstaat selbst: Ohne sie ist Rechtssicherheit und damit Rechtsstaatlichkeit nicht denkbar."

Zum praktischen weiteren Vorgehen habe ich empfohlen jetzt nach Erlaß des OrgKG keinen Schnellschuß mit einer einschlägigen Grundgesetzänderung abzugeben. Beim Bundesverfassungsgericht sind zwei Verfahren gegen die Regelungen über den Lauschangriff im Polizeigesetz des Landes Baden-Württemberg und im hamburgischen Gesetz über die Datenverarbeitung der Polizei anhängig. Es kann erwartet werden, daß das Bundesverfassungsgericht in diesen Verfahren sich darüber äußern wird, ob und unter welchen Voraussetzungen ein Lauschangriff in eine Wohnung hinein mit dem Grundgesetz vereinbar ist. Nach einer solchen Entscheidung dürfte es mehr Sicherheit für den vorzunehmenden schwierigen Abwägungsprozeß als bisher geben. Alle Beteiligten hätten dann Gelegenheit, die von ihnen eingenommene Position noch einmal zu überprüfen. Ich selbst nehme mich davon nicht aus.

5.1.4 Strafverfahrensänderungsgesetz

Zu einem Teil der Regelungsinhalte des vom Bundesministers der Justiz im Juni 1989 zur Erörterung gestellten Entwurfs eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts — Strafverfahrensänderungsgesetz 1989 — StVÄG — (s. 12. TB S. 25) sind durch das OrgKG (s. o. 5.1.1) Rechtsvorschriften geschaffen worden. Dies gilt namentlich für die Rasterfahndung, für den Einsatz Verdeckter Ermittler und für die polizeiliche Beobachtung. Andere wichtige Regelungsinhalte des damaligen Entwurfs sind bis jetzt leider noch nicht einer gesetzgeberischen Entscheidung zugeführt worden.

Dies in Ergänzung des OrgKG zu tun, ist — nach meiner Kenntnis schon seit Herbst 1991 — das Vorhaben des Bundesministers der Justiz. Unter dem Arbeitstitel eines „Rest-StVÄG" sollen in einer Reihe von seit langem als regelungsbedürftig erkannten Punkten die im Interesse des Schutzes des Persönlichkeitsrechts der Bürger, im Interesse der Rechtssicherheit und Rechtsklarheit sowie aus strafprozessualsystematischen Gründen notwendigen präzisen Rechtsgrundlagen geschaffen werden. Zu nennen sind insbesondere

- die Fahndung, insbesondere in der Öffentlichkeit und durch Inanspruchnahme von Publikationsorganen, einschließlich der Unterrichtung der Öffentlichkeit nach einer erfolgreichen solchen Fahndung
- die längerfristige Observation,
- die Erteilung von Aktenauskünften und Akteneinsicht für Gerichte, Staatsanwaltschaften, Behörden und Privatpersonen sowie die Übermittlung von Erkenntnissen für wissenschaftliche Zwecke,
- die Verwendung von für Zwecke der Strafverfolgung erhobenen personenbezogenen Daten für präventiv-polizeiliche Zwecke,
- die Unterrichtung der Polizei über den Ausgang des Strafverfahrens,
- die Verarbeitung von in einem Strafverfahren erhobenen personenbezogenen Daten in Dateien sowie die Verwendung dieser Daten,
- die Einrichtung eines zentralen staatsanwaltschaftlichen Verfahrensregisters,
- der Auskunftsanspruch desjenigen, dessen Daten in einer Datei gespeichert sind.

Die Bemühungen, hierfür Regelungen zu schaffen, habe ich seit Jahren mit Empfehlungen begleitet. In einem Schreiben an das Bundesministerium der Justiz vom Oktober 1992 habe ich meiner Sorge über den schleppenden Fortgang der Arbeiten Ausdruck gegeben. In seiner Antwort hat das Bundesministerium der Justiz darauf hingewiesen, daß insbesondere mit den Dateiregelungen für die Strafverfolgungsbehörden und die Gerichte Neuland betreten werde. Das Gesetzgebungsvorhaben werde mit größtem Nachdruck mit dem Ziel weiterverfolgt, die fortbestehenden Meinungsunterschiede in den sich schwierig und kompliziert gestaltenden Einzelabstimmungen zu überwinden und alsbald einen Regierungsentwurf vorzulegen. Ich wiederhole meinen Hinweis auf die dringende Notwendigkeit der Schaffung geeigneter gesetzlicher Regelungen und hoffe, daß es nunmehr zügig vorangeht. Geschieht dies nicht, muß der Eindruck entstehen, daß der Gesetzgeber zwar schnell bei der Hand ist, wenn es darum geht, zusätzliche Eingriffsbefugnisse für Staatsanwaltschaften und Polizei zu schaffen, daß er sich aber sehr viel Zeit läßt, wenn die Rechte Betroffener auf sorgfältigen Umgang mit ihren oft sehr sensiblen personenbezogenen Daten in Rede stehen.

5.1.5 Genomanalyse im Strafverfahren

In meinem 13. Tätigkeitsbericht (S. 39ff.) war Kernaussage meiner eingehenden Ausführungen zum Thema Genomanalyse im Strafverfahren die dringende Empfehlung an den Gesetzgeber, in der laufenden Legislaturperiode die unter Gesichtspunkten des Datenschutzes unerläßlichen Regelungen über den Einsatz gentechnischer Methoden im Strafverfahren zu schaffen. Inzwischen ist meine Befürchtung gewachsen, daß es in dieser Legislaturperiode dazu nicht mehr kommt.

Im Januar 1992 hat das Bundesministerium der Justiz endlich einen „Referentenentwurf einer gesetzlichen Regelung zum genetischen Fingerabdruck" vorgelegt, der einen Anfang 1990 verteilten Diskussionsentwurf ablöst (s. auch 13. TB S. 39 ff.). Der deutlichste Unterschied zum früheren Entwurf ist, daß auf eine gentechnische Untersuchung in bezug auf *„äußerlich sichtbare Körpermerkmale"* verzichtet werden soll. Damit ist erfreulicherweise eine Reihe von grundlegenden Problemen ausgeräumt, die ich schon in meinem 13. Tätigkeitsbericht (a. a. O. S. 40) dargestellt habe. Ich hoffe, daß es hierbei bleibt. In meiner Stellungnahme zu dem Referentenentwurf habe ich empfohlen, darüber hinausgehend zu verdeutlichen, daß genetisches Untersuchungsmaterial nicht als *selbständig* aussagekräftige Informationsquelle genutzt werden darf: Als Ergebnis einer *vergleichenden* Untersuchung sollte das „Untersuchungsziel" der „Feststellung der Abstammung oder der Tatsache, ob aufgefundenes Spurenmaterial von dem Beschuldigten stammt" ausdrücklich und abschließend im Gesetz definiert werden. Zur verfahrensmäßigen Sicherung des Kernsatzes des Referentenentwurfs: „Feststellungen über genetische Anlagen dürfen nicht erfolgen" habe ich zudem empfohlen, ausdrücklich im Gesetz zu formulieren, daß es sich um Untersuchungen „des hochvariablen, nicht-kodierenden Bereichs" der Desoxyribonukleinsäure handelt. Diese Beschränkung muß vom Gesetzgeber selbst ausgesprochen werden; Hinweise in der Gesetzesbegründung reichen in dieser wichtigen Frage nicht aus.

Durch die keineswegs abgeschlossene wissenschaftliche Methodendiskussion zum genetischen Fingerabdruck sehe ich meine Empfehlung bestätigt, es nicht allein den mit der Durchführung der Untersuchung beauftragten Stellen zu überlassen, durch technische und organisatorische Maßnahmen zu gewährleisten, daß unzulässige molekulargenetischen Untersuchungen oder unbefugte Kenntnisnahme Dritter ausgeschlossen sind, wie es der Referentenentwurf vorsieht. Das Bundesministerium der Justiz sollte mit Zustimmung des Bundesrates durch Rechtsverordnung Vorschriften zur Durchführung dieser technischen und organisatorischen Maßnahmen und im Einvernehmen mit dem Bundesministerium für Forschung und Technologie über die zulässigen Untersuchungsmethoden erlassen.

Die Notwendigkeit baldiger gesetzgeberischer Reaktion belegt nach meiner Überzeugung auch das Urteil des Bundesgerichtshofs vom 12. August 1992 (5 StR 239/92 — JZ, 1992, 102 —): Das Gericht beanstandet Mängel in der Klärung, „aus welcher Datenbasis der Sachverständige die Häufigkeit der untersuchten Merkmale in der Population hergeleitet hat". Es spricht von einem rechtsfehlerfreien Vorgehen dann, wenn das Landgericht „den Angeklagten als durch die DNA-Analyse stark belasteten Tatverdächtigen angesehen und sich unter Berücksichtigung der weiteren Indizien von der Täterschaft überzeugt hätte". Letztlich erklärt der Bundesgerichtshof, der DNA-Analyse komme der hohe Beweiswert, wie ihn das Landgericht voraussetzte, nicht zu.

Ich hoffe, daß der Gesetzgeber auch diese Entscheidung zum Anlaß nimmt, den Gesetzgebungsentwurf

mit Nachdruck zu betreiben, damit wenigstens in der nächsten Legislaturperiode rechtliche Klarheit in diesem für das Strafverfahren immer wichtiger werdenden Bereich geschaffen wird.

5.1.6 Weitere Empfehlungen für den Persönlichkeitsschutz im Strafverfahren

Schon seit langem deutlich ist die Notwendigkeit, der routinemäßigen öffentlichen Erörterung so sensibler personenbezogener Informationen, wie der Einkommens- und Vermögensverhältnisse des Beschuldigten — und damit oft auch seines Ehe- oder Lebenspartners — zumindest in den Fällen entgegenzuwirken, in denen diese Datenerhebung mit dem eigentlichen Gegenstand des Strafverfahrens (Strafvorwurf) nichts zu tun hat. Schon in meinem 5. Tätigkeitsbericht (S. 20) habe ich auf die Möglichkeit verwiesen, in geeigneten Fällen verstärkt von dem in § 249 Abs. 2 StPO geregelten sogenannten Selbstleseverfahren Gebrauch zu machen, d. h. die schriftliche Darstellung der Einkommens- und Vermögensverhältnisse anheim zu geben und im Einvernehmen der Verfahrensbeteiligten von der Verlesung eines solchen Schriftstückes abzusehen. Die Stellungnahme des Bundesministeriums der Justiz, mein Vorschlag würde durch die Zielrichtung der Vorschrift, die auf Prozeßwirtschaftlichkeit und Verfahrensbeschleunigung ausgerichtet sei, nicht gedeckt, hat mich nicht zu befriedigen vermocht. In einer rechtstaatlichen Verfahrensordnung, in der der Angeklagte nicht bloßes Verfahrensobjekt ist, vermag ich es mit der Wertordnung des Grundgesetzes nicht in Einklang zu bringen, Transparenzeinbußen zwar im Hinblick auf prozeßwirtschaftliche Vorteile hinzunehmen, nicht aber im Hinblick auf die Gewährleistung des grundrechtlich verbürgten Persönlichkeitsschutzes. Einen gewissen Fortschritt in dieser Diskussion sehe ich darin, daß das Bundesministerium der Justiz nunmehr einen von mir erarbeiteten Vorschlag für eine gesetzliche Klarstellung im Dialog mit den Landesjustizverwaltungen zur Diskussion gestellt hat.

Die wachsende Bedeutung des Persönlichkeitsschutzes im Strafverfahren illustriert auch der Grundsatzbeschluß des Bundesgerichtshofs vom 27. Februar 1992 (5 StR 190/91). Danach führt das Unterlassen der polizeilichen Belehrung eines Beschuldigten über das ihm zustehende Aussageverweigerungsrecht, darüber nämlich, daß es ihm freisteht, sich zu der Beschuldigung zu äußern oder nicht zur Sache auszusagen (§ 136 Abs. 1 Sastz 2 i. V. m. § 163a Abs. 4 Satz 2 StPO) nunmehr zu einem Verwertungsverbot: Äußerungen, die der Beschuldigte in dieser Vernehmung gemacht hat, dürfen nicht verwertet werden. Ich schließe mich gern den zahlreichen Stimmen an, die diesen Beschluß als „einen wirklichen Durchbruch" begrüßen und „zu den bedeutensten strafprozeßrechtlichen Entscheidungen des Bundesgerichtshofs" zählen. Die in ihm zum Ausdruck kommende Änderung der bisherigen Rechtssprechung trägt dem Umstand Rechnung, daß niemand gegen sich selbst aussagen muß. Die Freiwilligkeit, sich zu einer Beschuldigung zu äußern, ist damit als ein aus hochrangigen Verfassungsgrundsätzen abzuleitendes, international geltendes Prinzip des Strafprozeßrechts erkannt worden, dessen Geltung im Falle der Nichtbeachtung durch ein Verwertungsverbot geschützt werden muß.

In einem Punkte jedoch bedarf die vom Bundesgerichtshof festgestellte Rechtslage einer Weiterentwicklung: Der Satz nämlich: „Läßt sich nicht klären, ob der Hinweis gegeben worden ist oder nicht, so darf der Tatrichter den Inhalt der Vernehmung verwerten." entspricht — darin bin ich mir mit anderen Kommentatoren einig — den Prämissen der Entscheidung nicht. Bleibt unklar, ob eine Belehrung des Beschuldigten über sein Aussageverweigerungsrecht erfolgt ist, so ist die Möglichkeit offen geblieben, daß keine Belehrung stattgefunden hat. Dann aber steht die Verwertung mit der Menschenwürde und den Erfordernissen eines fairen Verfahrens nicht im Einklang. Der Gesetzgeber sollte die Lücke dadurch schließen, daß er dem Verwertungsverbot auch für den zitierten Zweifelsfall durch normative Regelungen Geltung verschafft.

5.2 Persönlichkeitsschutz im Rehabilitierungsverfahren — Erstes SED-Unrechtsbereinigungsgesetz —

Nach dem Vertrag über die Herstellung der Einheit Deutschlands (Einigungsvertrag) blieben zwar Strafurteile der DDR-Justiz grundsätzlich wirksam, es war jedoch unverzüglich eine gesetzliche Grundlage dafür zu schaffen, daß alle Personen rehabilitiert werden können, die Opfer einer politisch motivierten Strafverfolgungsmaßnahme geworden waren. Diesem Auftrag an den gesamtdeutschen Gesetzgeber folgend hat das Erste Gesetz zur Bereinigung von SED-Unrecht (1. SED-UnBerG) die Grundlage dafür geschaffen, strafgerichtliche Entscheidungen auf Antrag für rechtsstaatswidrig zu erklären und aufzuheben, „soweit sie mit wesentlichen Grundsätzen einer freiheitlichen rechtsstaatlichen Ordnung unvereinbar" sind, und soziale Ausgleichsleistungen zu gewähren.

Im Rechtsetzungsverfahren konnte ich in einigen Punkten zu einer datenschutzgerechten Gestaltung des Entwurfs beitragen: Die Rechtsstellung des Betroffenen bei der Antragstellung wurde verbessert. Der Rehabilitierungsantrag, der Antrag also auf gerichtliche Aufhebung der rechtsstaatswidrigen Entscheidung, kann nicht nur von dem unmittelbar in seinen Rechten Betroffenen (bzw. nach seinem Tode durch bestimmte Angehörige), sondern auch von der Staatsanwaltschaft gestellt werden. Unter Gesichtspunkten des Persönlichkeitsschutzes erscheint dies durchaus sachgerecht. In der Regel nämlich dürfte die Aufhebung rechtsstaatswidriger DDR-Verurteilungen sowohl im öffentlichen Interesse als auch im Interesse des Betroffenen liegen. Mit Blick auf das Persönlichkeitsrecht war jedoch auch an diejenigen Betroffenen zu denken, die das anders sehen. Auf meinen Vorschlag wurde ergänzend eingefügt, daß die Staatsanwaltschaft den Antrag nicht stellen kann, „soweit der unmittelbar in seinen Rechten Betroffene widersprochen hat". Damit wird den Interessen derje-

nigen genüge getan, die mit ihrem in der Vergangenheit liegenden Schicksal nicht in einem erneuten Verfahren konfrontiert werden wollen.

Eine weitere wichtige Verbesserung, die auf meine Vorschläge zurückgeht, betrifft die Frage der Auskunftserteilung durch den Generalbundesanwalt über in das Bundeszentralregister übernommene strafgerichtliche Verurteilungen, namentlich die Frage, in welchem Stadium des Rehabilitierungsverfahrens die angefochtene Entscheidung in einem Führungszeugnis nicht mehr erscheint. Der Gesetzentwurf sah ursprünglich vor, dem Bundeszentralregister lediglich rechtskräftige Entscheidungen über eine Rehabilitierung mitzuteilen. Konsequenz hieraus wäre gewesen, daß Eintragungen über Strafurteile der DDR, die im Bundeszentralregister gespeichert sind, erst nach erfolgreichem rechtskräftigem Abschluß des Rehabilitierungsverfahrens hätten entfernt werden können. Die nunmehr getroffene Regelung stellt sicher, daß eine dem Rehabilitierungsantrag stattgebende Entscheidung des Gerichts nicht erst dann, wenn sie rechtskräftig geworden ist, sondern schon dann, wenn sie — durch Beschwerde angefochten — noch nicht rechtskräftig ist, dem Bundeszentralregister mitzuteilen ist. Ausdrücklich ist nunmehr geregelt, daß ein entsprechender Vermerk im Bundeszentralregister bewirkt, daß die angefochtene Entscheidung *nicht* in das Führungszeugnis aufgenommen wird. Damit ist eine erfreuliche Annäherung an die Regelungen erreicht, die bislang schon nach der Strafprozeßordnung für das strafprozessuale Wiederaufnahmeverfahren gelten: Dort bewirkt bereits die Wiederaufnahmeentscheidung und nicht erst die Aufhebung des angefochtenen Urteils eine entsprechende Vergünstigung bei Auskünften aus dem Bundeszentralregister.

5.3 Auch Funktionsträger der früheren DDR müssen amtlich bekannt gewordene Privatgeheimnisse wahren

Ehemalige Mitarbeiter des Staatssicherheitsdienstes und viele andere Funktionsträger des SED-Regimes besitzen noch heute teilweise sehr umfassende Kenntnisse über personenbezogene Daten, auch aus sensiblen Lebensbereichen, von natürlichen Personen, besonders von Bewohnern der früheren DDR. Im November 1991 habe ich das Bundesministerium der Justiz darauf hingewiesen, daß in Bezug auf den Schutz von in der früheren DDR „amtlich" bekannt gewordenen Privatgeheimnissen eine datenschutzrechtlich bedauerliche Strafbarkeitslücke besteht: Eine nach dem 3. Oktober 1990 begangene Verletzung von solchen Privatgeheimnissen ist nach geltendem Recht nicht nach § 203 Abs. 2 StGB strafbar. Nach dieser Strafvorschrift wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis, offenbart, das ihm *als Amtsträger* anvertraut worden oder sonst bekanntgeworden ist. Funktionsträger der früheren DDR sind aber keine Amtsträger in diesem Sinne. Ich habe empfohlen, die sich daraus ergebende Strafbarkeitslücke unverzüglich zu schließen.

Ich begrüße sehr, daß nach Erörterung mit den Landesjustizverwaltungen das Bundesministerium der Justiz meine Initiative aufgegriffen und den Entwurf einer Vorschrift zur „Gewährleistung des Schutzes von Privatgeheimnissen" erarbeitet hat. Danach soll in den „Entwurf eines . . . Strafrechtsänderungsgesetzes — Innerdeutsche Rechtsangleichung —" ein Artikel eingestellt werden, der Funktionsträger der ehemaligen DDR, die in ihrer Funktion — unter Berücksichtigung des abweichenden Staats- und Verwaltungsaufbaus der ehemaligen DDR — Amtsträgern und für den öffentlichen Dienst besonders Verpflichteten nach bundesdeutschem Recht vergleichbar waren, den Amtsträgern im Sinne des § 203 Abs. 2 StGB gleichstellt. Diesem näher umschriebenen Personenkreis wird eine strafbewehrte Geheimhaltungspflicht für die ihnen während ihrer Tätigkeit in der ehemaligen DDR dienstlich bekanntgewordenen Privatgeheimnisse auferlegt.

Da durchweg andere Sanktionen kaum zur Verfügung stehen, müssen die Belange der Betroffenen vor unzulässiger Nutzung und Weitergabe ihrer personenbezogenen Daten durch das Strafrecht geschützt werden. Ich unterstreiche erneut die Dringlichkeit, den von der aufgezeigten Rechtslücke besonders betroffenen Bürgern der neuen Bundesländer einen dem Recht der alten Bundesländer gleichwertigen strafrechtlichen Schutz ihrer Privatgeheimnisse zu gewähren. Dabei bin ich mir bewußt, daß angesichts des Rückwirkungsverbots des Artikel 103 Abs. 2 GG, § 1 StGB nur eine nach Schaffung einer ergänzenden Strafrechtsnorm erfolgende Offenbarung unter Strafe gestellt werden kann. Um so zügiger muß die erkannte Strafbarkeitslücke geschlossen werden.

5.4 Das jugendgerichtliche Verfahren ist datenschutzrechtlich besonders sensibel

Im Jugendgerichtsgesetz gibt es unter Gesichtspunkten des dort besonders notwendigen Persönlichkeitsschutzes Regelungsdefizite, auf die ich schon früher hingewiesen habe (s. 11. TB S. 20f.) Die Bundesregierung hat dementsprechend schon bei der Vorbereitung des ersten Gesetzes zur Änderung des Jugendgerichtsgesetzes als weiteren Reformbedarf u. a. die Stellung und die Aufgabe der Jugendgerichtshilfe im Strafverfahren erkannt. Ich unterstreiche die Aussage, daß angesichts der im jugendgerichtlichen Verfahren vorgesehenen „Ermittlungstiefe" mit umfassenden Ermittlungen zur Persönlichkeit des Betroffenen (§§ 38 und 43 JGG), an die Befugnisnormen des Jugendgerichtsgesetzes „besonders hohe Anforderungen zu stellen" sind (vgl. Entwurf der Bundesregierung eines Ersten Gesetzes zur Änderung des Achten Buches Sozialgesetzbuch, BT-Drucksache 203/92 vom 3. April 1992 S. 53).

Mittlerweile ist in der Praxis die Unsicherheit darüber gewachsen, ob die Jugendgerichtshilfe personenbezogene Daten des Betroffenen ohne dessen Mitwirkung erheben darf. Vor diesem Hintergrund war die Bundesregierung im Rahmen eines Ersten Gesetzes zur Änderung des Achten Buches Sozialgesetzbuch bemüht, die Problematik bis zu einer Neuregelung in

einem zweiten Gesetz zur Änderung des Jugendgerichtsgesetzes durch eine Vorschrift mit „Übergangscharakter" zu überbrücken und dort eine „eng begrenzte Befugnis" zur Erhebung personenbezogener Daten ohne Mitwirkung des Betroffenen zu schaffen.

Dabei war davon auszugehen, daß die Aufgabe der Mitwirkung als Jugendgerichtshilfe im Verfahren nach dem Jugendgerichtsgesetz durch das Jugendamt wahrgenommen wird (§ 52 des Achten Buches Sozialgesetzbuch — SGB VIII). Das Achte Buch des SGB enthält in § 62 Abs. 3 Nr. 1 für die Datenerhebung zwar bislang schon eine Öffnungsregelung zugunsten anderweitiger, spezialgesetzlicher Regelungen. Im Jugendgerichtsgesetz jedoch gibt es solche speziellen Datenschutzvorschriften derzeit leider noch nicht. Diese Rechtslage wird den Aufgaben der Jugendgerichtshilfe nicht gerecht. Letztere kann sich nicht auf die Datenerhebung beim Betroffenen beschränken; sie muß sich vielmehr im Einzelfalle auch bei Dritten über den Jugendlichen — seine Persönlichkeit, seine Entwicklung, seine Umwelt — erkundigen dürfen.

Wichtig ist mir aber sicherzustellen, daß keineswegs die Wahrnehmung einer Aufgabe der Jugendgerichtshilfe für sich allein generell gestattet, Daten ohne Mitwirkung des Betroffenen zu erheben, sondern daß für jede Datenerhebung eine Einzelfallwürdigung erforderlich ist. Ich bin dafür eingetreten, eine Regelung zu schaffen, die das spezifische Vertrauensverhältnis zwischen Jugendgerichtshelfer und Jugendlichem angemessen berücksichtigt. Eine generelle Informationssammlung „hinter dem Rücken" des Jugendlichen ist damit grundsätzlich unvereinbar. Von wesentlicher Bedeutung ist, die Tranparenz der Erhebungsvorgänge für den Betroffenen zu gewährleisten. Schon deshalb ist ein vorheriger Hinweis an den Jugendlichen auf die beabsichtigte Datenerhebung bei Dritten besonders wichtig. Hinzu kommt, daß sowohl für die Entscheidung, ob überhaupt Daten ohne Mitwirkung des Betroffenen erhoben werden, wie auch für die Auswahl, bei welchem von mehreren möglichen Ansprechpartnern die Informationen erfragt werden, die schutzwürdigen Belange des Betroffenen zu berücksichtigen sind. Oft nämlich ist mit der Datenerhebung bei Dritten zugleich eine Übermittlung sehr sensibler Daten über den Jugendlichen an den Dritten verbunden; oft wird diesem durch die Anfrage der Jugendgerichtshilfe bekannt, daß gegen den Jugendlichen ein Strafverfahren betrieben wird. Dem Betroffenen sollte deshalb zuvor Gelegenheit eingeräumt werden, sich dazu zu äußern, denn erst er selbst wird erläutern können, weshalb eine Datenerhebung — und die damit u. U. verbundene Kundgabe des Strafverfahrens gegen ihn — bei einem bestimmten Dritten für ihn besonders belastend wäre.

Erfreulicherweise hatte dementsprechend der Gesetzentwurf der Bundesregierung meinen Vorschlag aufgegriffen, in § 62 Abs. 3 SGB VIII eine Bestimmung einzufügen, die die Datenerhebung ohne Mitwirkung des Betroffenen nur erlaubt, soweit dies zur Wahrnehmung der Aufgabe der Jugendgerichtshilfe „im Einzelfall erforderlich ist und keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden". Mit der Einfügung sollte außerdem vorgeschrieben werden, daß der Betroffene „vor der Erhebung zu hören und dabei über die Rechtsgrundlage der Erhebung und den Erhebungszweck aufzuklären" ist, „soweit dieser nicht offenkundig ist".

Zu meinem großen Bedauern hat dieser Teil des Gesetzentwurfes der Bundesregierung in den Ausschußberatungen des Deutschen Bundestages keine Billigung gefunden. Statt dessen ist in § 61 SGB VIII ein Absatz 3 eingefügt worden, der für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch das Jugendamt bei der Mitwirkung in Jugendstrafverfahren lediglich auf die Vorschriften des Jugendgerichtsgesetzes verweist. Die zugrunde liegenden Hinweise des Bundesrates, der die §§ 38 und 43 Jugendgerichtsgesetz nennt und als „ausreichende Rechtsgrundlage" für „die Ermittlungstätigkeit" bezeichnet, gehen jedoch ins Leere, da es sich dabei um Aufgabenbeschreibungen, nicht aber um Befugnisregelungen handelt, wie auch von der Bundesregierung in ihrer Gegenäußerung richtig erkannt worden war.

Die von Anfang an angestrebte umfassende Regelung im Jugendgerichtsgesetz ist damit um so dringlicher geworden. Ich hoffe, daß die Bundesregierung nunmehr bald den Entwurf eines zweiten Gesetzes zur Änderung des Jugendgerichtsgesetzes vorlegt und dabei auch den ursprünglichen Vorschlag zu § 62 Abs. 3 SGB VIII wieder aufgreift.

5.5 Schutz des Persönlichkeitsrechts auch bei Strafgefangenen — Zum Strafvollzugsgesetz —

Das geltende Strafvollzugsgesetz enthält kaum Regelungen zum Schutz des Persönlichkeitsrechts. Bereits seit Jahren bemüht sich das Bundesministerium der Justiz, dieses Gesetz zu novellieren (s. zuletzt 10. TB S. 22).

Im Jahr 1991 hat das Bundesministerium der Justiz einen überarbeiteten Referentenentwurf vorgelegt, der in einem besonderen Abschnitt Vorschriften über den Datenschutz enthält. Dieser ist aus meiner Sicht allerdings noch zu allgemein gehalten und trägt den besonderen rechtlichen und tatsächlichen Bedingungen des Strafvollzugs zu wenig Rechnung. Auch für einen Strafgefangenen muß der Grundsatz gelten, daß Persönlichkeit und Lebensverhältnisse nur insoweit erforscht werden, wie dies für die jeweilige staatliche Aufgabe, hier also für den Strafvollzug, erforderlich ist. Gerade wegen der besonderen Bedingungen in einer Strafvollzugsanstalt halte ich es für sehr wichtig, den Bereich normenklar zu beschreiben, der als innerer Kern des Persönlichkeitsrechts, also zum Schutz der unantastbaren Menschenwürde — auch eines Gefangenen —, dem Einblick Dritter entzogen bleiben muß. Hierbei denke ich z. B. an Regelungen über die Beobachtung des Gefangenen in seiner Zelle und bei Besuchskontakten.

Das Bundesministerium der Justiz hat im Sommer 1992 angekündigt, den Referentenentwurf zu überarbeiten.

5.6 Mitteilungen aus gerichtlichen und staatsanwaltschaftlichen Verfahren an andere Stellen — Justizmitteilungsgesetz —

Die Bundesregierung hat dem Deutschen Bundestag den Entwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen — Justizmitteilungsgesetz — vorgelegt (BT-Drucksache 12/3199). Für die Übermittlung personenbezogener Daten durch solche Mitteilungen bestehen bisher nur zum Teil bereichsspezifische gesetzliche Vorschriften; weitere sollen mit dem Entwurf (Artikel 2 bis 25) geschaffen werden. In das Einführungsgesetz zum Gerichtsverfassungsgesetz (EGGVG) sollen Regelungen über Zulässigkeitsvoraussetzungen für solche Mitteilungen und über das dabei allgemein zu beachtende Verfahren aufgenommen werden (Artikel 1). Damit soll die *gesetzliche Grundlage* für die bisher überwiegend in bundeseinheitlich vereinbarten Verwaltungsvorschriften des Bundes und der Länder geregelten Mitteilungspflichten der Gerichte und Staatsanwaltschaften an andere öffentliche Stellen geschaffen werden. Dieses Vorhaben entspricht einer von den Datenschutzbeauftragten des Bundes und der Länder bereits seit Jahren erhobenen Forderung (vgl. insbesondere 9. TB S. 19, 7. TB S. 14f. und zuletzt 13. TB S. 89, dort Nr. 2).

Das Bundesministerium der Justiz hat mich bei der Vorbereitung des Entwurfs beteiligt, aber nicht alle meine Empfehlungen berücksichtigt. Ich hatte z. B. gebeten, die Pflicht der ordentlichen Gerichte und der Staatsanwaltschaften zur Unterrichtung des Betroffenen über eine Mitteilung nicht durch zu viele Ausnahmen einzuschränken (§ 21 EGGVG des Entwurfs). Das BMJ hat dagegen auf Belange der Praxis hingewiesen. Ich stelle diese grundsätzlich nicht in Frage, muß aber unterstreichen, daß jede Mitteilung im Rahmen des Gesetzes einen Eingriff in das Persönlichkeitsrecht bedeutet; deshalb muß das Verfahren so gestaltet werden, daß die Eingriffe in das Persönlichkeitsrecht so gering wie möglich gehalten werden. Der vom Bundesverfassungsgericht betonte Grundsatz der Transparenz der Datenverarbeitung, daß jeder nämlich wissen können muß, wer was bei welcher Gelegenheit über ihn weiß, muß beachtet werden.

Der Entwurf sieht in den gesetzlichen Bestimmungen zur Ergänzung des EGGVG (Artikel 1) Mitteilungs*ermächtigungen*, nicht Mitteilungs*pflichten* vor. Betroffene können also aus dem Gesetz nicht erkennen, welche Datenübermittlungen über sie im Einzelfall an welche Empfänger tatsächlich erfolgen. Das ist deshalb nicht unproblematisch, weil vorgesehen ist, verwaltungsinterne Mitteilungspflichten auch künftig durch *Verwaltungsvorschriften* zu begründen. Die Verwaltung, nicht der Gesetzgeber soll die Fälle festlegen, in denen bei Ausübung pflichtgemäßen Ermessens unter Beachtung des Grundsatzes der Verhältnismäßigkeit in der Regel eine Mitteilung erfolgen soll. Im übrigen soll es aber bei der Ermessensausübung im Einzelfall bleiben. Dieses zweistufige Regelungssystem von Gesetz und Verwaltungsvorschriften kann hingenommen werden, wenn der Gesetzgeber gleichzeitig hinreichende Vorgaben für die Verwaltungsvorschriften festlegt und die Verwaltungsvorschriften ihnen entsprechen. Zu Recht ist daher im Entwurf vorgesehen, notwendige Maßstäbe für die Ausübung des Ermessens in das Gesetz aufzunehmen. Darüber hinaus kommt bei diesem Verfahren der Unterrichtung des Betroffenen von Übermittlungen seiner Daten besondere Bedeutung zu.

Grundsätzliche Voraussetzung für die Zulässigkeit einer Datenübermittlung nach dem Entwurf des Justizmitteilungsgesetzes ist, daß sie zur Erfüllung der in der Zuständigkeit des Empfängers liegenden *Aufgaben* erfolgt und hierfür auch *erforderlich* ist (vgl. § 13 Abs. 2 EGGVG des Entwurfs mit den dort genannten Vorschriften).

Nach dem Entwurf zu § 13 Abs. 2 EGGVG sind aber ebenso *schutzwürdige Interessen des Betroffenen* an dem Ausschluß der Übermittlung zu berücksichtigen, die gegenüber dem Erfordernis überwiegen können, daß der Empfänger von den personenbezogenen Daten Kenntnis erhält. Soweit solche schutzwürdigen Interessen für die übermittelnde Stelle erkennbar sind, ist eine Mitteilung unzulässig. In einem solchen Fall müssen auch in Verwaltungsvorschriften vorgesehene Regelmitteilungen unterbleiben. In Strafsachen ist die Übermittlung personenbezogener Daten des Beschuldigten vor Abschluß oder vor nicht nur vorläufiger Einstellung des Verfahrens entsprechend meiner Empfehlung *nur zulässig*, wenn aus der Sicht der übermittelnden Stelle unverzüglich Entscheidungen oder andere Maßnahmen des Empfängers geboten sind oder derzeit nicht getroffen werden sollten (§ 14 Abs. 4 EGGVG des Entwurfs). Hervorzuheben ist aber auch, daß z. B. in Strafverfahren wegen fahrlässig begangener Straftaten, in sonstigen Verfahren bei der Verurteilung zu einer anderen Maßnahme als einer Strafe oder bei Einstellung des Verfahrens in weitem Umfang eine Übermittlung personenbezogener Daten des Beschuldigten *unterbleibt*, wenn nicht besondere Umstände des Einzelfalles sie erfordern (§ 14 Abs. 3 EGGVG des Entwurfs). Dies bedeutet, worauf die Begründung des Entwurfs ausdrücklich hinweist (BT-Drucksache 12/3199 S. 19), daß eine Möglichkeit, Mitteilungspflichten durch Verwaltungsvorschriften zu begründen, in diesen Fällen nicht besteht; vielmehr ist jeweils im Einzelfall zu entscheiden.

Ich gehe davon aus, daß ich bei der Überarbeitung der derzeitigen Verwaltungsvorschriften auf der Grundlage des künftigen Justizmitteilungsgesetzes beteiligt werde. Hierbei werde ich gemeinsam mit den Landesbeauftragten für den Datenschutz darauf dringen, daß die gesetzlichen Vorgaben beachtet und insbesondere nur Regelmitteilungen vorgesehen werden, die den Anforderungen des Verhältnismäßigkeitsgrundsatzes entsprechen.

Der Bundesrat hat in seiner Stellungnahme zum Regierungsentwurf (BT-Drucksache 12/3199 Seite 38ff.) gebeten, die einzelnen Vorschriften bei der Beratung insbesondere „auch unter dem Aspekt der Vermeidung nicht unabdingbar erforderlicher Belastungen der Justiz zu prüfen und, soweit irgend möglich, solche Belastungen zu vermeiden" (ebenda Seite 38). Im Regierungsentwurf wurde, worauf ich eingangs hingewiesen habe, bereits eingehend auf die Belange der Praxis geachtet. Die entsprechenden

Regelungen sollten daher nicht zu Lasten des Persönlichkeitsrechts verändert werden.

In Hinblick auf die Bedeutung der Mitteilungen von Gerichten und Staatsanwaltschaften aus deren Verfahren für die Betroffenen wäre es wünschenswert, wenn der Gesetzentwurf möglichst bald verabschiedet würde.

5.7. Auch im Konkursverfahren geht es nicht ohne Datenschutz

Das Insolvenzrecht umfaßt die Rechtsnormen, die das Verfahren der anteiligen Befriedigung der Gläubiger eines zahlungsunfähigen Schuldners regeln; es ist derzeit vor allem in den Bestimmungen über das Konkurs- und Vergleichsverfahren enthalten. Als Ersatz für das — wie der Regierungsentwurf einer *Insolvenzordnung* im einzelnen erläutert (BT-Drucksache 12/2443, Begründung S. 72 ff.) — weitgehend funktionsunfähig gewordene Konkurs- und Vergleichsrecht ist ein modernes Insolvenzrecht vorgesehen; gleichzeitig soll die Gesamtvollstreckungsordnung entfallen, die bisher in den neuen Bundesländern und in Ost-Berlin als Übergangsregelung fortgilt. Zur Verwirklichung dieses Zieles hat die Bundesregierung den erwähnten Entwurf einer Insolvenzordnung sowie den Entwurf eines Einführungsgesetzes zur Insolvenzordnung (BT-Drucksache 12/3803) vorgelegt. Auch andere Bundesgesetze mit Berührung zum Insolvenzrecht sollen inhaltlich und redaktionell an die neue Insolvenzordnung angepaßt werden.

Die Insolvenzordnung enthält eine Reihe von Bestimmungen, die die Verarbeitung oder Nutzung von personenbezogenen Daten vor allem des Schuldners regeln. Fragen des Schutzes des Persönlichkeitsrechts des Schuldners stellen sich nicht nur bei Angaben zu dessen persönlichen Verhältnissen, sondern auch bei allen personenbezogenen Informationen zu seinem wirtschaftlichen Handeln. So folgt z. B. aus den Aufgaben des vorläufigen Insolvenzverwalters (§ 26 des Entwurfs) zwangsläufig ein vielfacher Umgang mit diesen Daten. Unter Aspekten des Persönlichkeitsrechts sind aber auch Geschäftspartner und Mitarbeiter eines Betriebes, für den ein Insolvenzverfahren eingeleitet wird, von dem Gesetzentwurf betroffen.

Da ich von dem Vorhaben erst nach Einleitung des förmlichen Gesetzgebungsverfahrens erfuhr, hatte ich keine Gelegenheit zu einer rechtzeitigen Stellungnahme; ich beabsichtige aber, dem federführenden Rechtsausschuß des Deutschen Bundestages in Kürze einige Empfehlungen zu übermitteln.

6 Finanzwesen

6.1 Die Abgabenordnung braucht Datenschutzregelungen

Das Bundesministerium der Finanzen hat den Entwurf eines Gesetzes zur Änderung der Abgabenordnung (AOÄG 1994) vorgelegt, mit dem die Voraussetzungen dafür geschaffen werden sollen, daß die Finanzverwaltung des Bundes und der Länder *einheitliches Datenschutzrecht* anwendet. Anders als der Vorentwurf, den das BMF nach erheblichen Einwendungen von meiner Seite nicht mehr weiterverfolgt, zielt der jetzige Entwurf nicht mehr darauf ab, Datenschutzvorschriften für den Bereich der Abgabenordnung abschließend festzulegen (s. 12. TB S. 29, 11. TB S. 88f.). Unter Beteiligung der Landesbeauftragten für den Datenschutz habe ich mit dem BMF weitgehende Übereinstimmung über die erforderliche Abgrenzung bei der Anwendung von Vorschriften der Abgabenordnung, des Bundesdatenschutzgesetzes und der Datenschutzgesetze der Länder erzielt (§ 31 b des Entwurfs). Andere Fragen sind noch offen.

6.1.1 Wann und in welchem Umfang dürfen Steuerdaten offenbart werden?

In den Entwurf wurde ausdrücklich der Grundsatz aufgenommen, daß die Offenbarung oder Verwendung der durch das Steuergeheimnis geschützten Daten nur für die *Zwecke steuerlicher Verfahren* zulässig ist (§ 30 Abs. 5 i. V. mit Abs. 2 Nrn. 1 und 2 des Entwurfs); es wurde verdeutlicht, daß eine Offenbarung oder Verwendung darüber hinaus eine *Zweckänderung* darstellt, die nur ausnahmsweise zulässig ist, wenn die im einzelnen aufgeführten Voraussetzungen gegeben sind, die weitgehend dem bisherigen § 30 Abs. 4 AO entsprechen. Nicht zuletzt ist vorgesehen, daß ein Empfänger die ihm offenbarten Steuerdaten grundsätzlich nur für den Zweck verwenden darf, zu dessen Erfüllung sie ihm offenbart wurden.

Die Offenbarung oder Verwendung von Steuerdaten soll unter anderem auch für die Verfolgung eines Vergehens der Geldwäsche (§ 261 Strafgesetzbuch) zugelassen werden. Ich habe empfohlen, entsprechend der Regelung in § 20 Abs. 1 Bundesverfassungsschutzgesetz Mitteilungen in diesen Fällen, soweit sie ohne Ersuchen des Empfängers erfolgen, nur zuzulassen, wenn *tatsächliche Anhaltspunkte* dafür gegeben sind, daß die Kenntnis der Daten zur Erfüllung der Aufgaben des Empfängers erforderlich ist.

6.1.2 Einheitliches Datenschutzrecht im Steuerverfahren

Die Regelung des Entwurfs über die Geltung der verschiedenen in Betracht kommenden Datenschutzvorschriften für die Finanzverwaltung des Bundes und der Länder (§ 31 b des Entwurfs) sieht vor, daß für den Umgang mit personenbezogenen Daten in Verfahren, in denen die Abgabenordnung von den Finanzbehörden (auch denen der Länder) anzuwenden ist, grundsätzlich das *Bundesdatenschutzgesetz* gilt, soweit die Abgabenordnung keine andere Regelung trifft. Einzelangaben über persönliche oder sachliche Verhältnisse einer juristischen Person, einer nichtrechtsfähigen Personenvereinigung oder einer Vermögensmasse sowie Betriebs- und Geschäftsgeheimnisse, die dem Steuergeheimnis unterliegen, stehen dabei den personenbezogenen Daten i. S. des Bundesdatenschutzgesetzes gleich. Die Vorschriften der Datenschutzgesetze der Länder über die Bestellung, die

Rechtsstellung und die Rechte und Pflichten der Landesbeauftragten für den Datenschutz, d. h. z. B. Kontroll- und Mitwirkungsrechte, Rechte und Pflichten zur Führung von Dateienregistern bleiben aber unberührt. In Verfahren, in denen die Abgabenordnung von den Gemeinden anzuwenden ist, sollen mit Ausnahme der Bestimmungen des Bundesdatenschutzgesetzes über das Zeugnisverweigerungsrecht und über Kontrollrechte der Landesbeauftragten für den Datenschutz insbesondere hinsichtlich der Daten, die dem Steuergeheimnis unterliegen, nach wie vor neben der Abgabenordnung die Landesdatenschutzgesetze Anwendung finden.

Der Entwurf sieht in § 31 b weiterhin vor, daß landesrechtliche Vorschriften, nach denen Behörden *Beauftragte für den Datenschutz* zu bestellen haben, unberührt bleiben. Demgegenüber habe ich dem BMF empfohlen, die Finanzbehörden generell zur Bestellung von Beauftragten für den Datenschutz zu verpflichten. Dies entspricht nicht nur einer bereits weitgehend geübten Praxis, sondern ist nach meiner Ansicht auch erforderlich, weil es im vorliegenden Zusammenhang um Daten geht, die dem erhöhten Schutz des *Steuergeheimnisses* unterliegen; für solche Daten sollte mit der Bestellung eines Beauftragten für den Datenschutz die gleiche *besondere Schutzmaßnahme* getroffen werden wie sie in § 79 Abs. 1, 2. Halbsatz SGB X für Daten, die dem Sozialgeheimnis unterliegen, vorgesehen ist. Diese Frage und weitere von mir zum Teil über den Entwurfstext hinaus zu anderen Vorschriften der Abgabenordnung übermittelte Vorschläge werden derzeit noch mit dem BMF diskutiert.

6.2 Datenschutz im Zinsabschlaggesetz

Das Bundesverfassungsgericht hat den Gesetzgeber verpflichtet, bis zum 1. Januar 1993 Vorkehrungen zu treffen, wonach Zinseinkünfte nicht nur rechtlich, sondern auch tatsächlich steuerlich gleich behandelt werden (Urteil vom 27. Juni 1991, BVerfGE 84 S. 239 ff.). Mit Artikel 1 des Gesetzes zur Neuregelung der Zinsbesteuerung (Zinsabschlaggesetz) vom 9. November 1992 (BGBl. I S. 1853 ff.) sind die entsprechenden Vorschriften des Einkommensteuergesetzes (EStG) über die Besteuerung der Einkünfte aus Kapitalvermögen geändert worden.

Ab 1993 wird ein dreißigprozentiger Zinsabschlag auf Kapitalforderungen erhoben, der auf die Einkommen- und Körperschaftsteuer anrechenbar ist (§ 43 a Abs. 1 Nr. 4 EStG). Die Beträge werden anonym an die Finanzämter abgeführt, so daß das Steuer- und Bankgeheimnis gewahrt bleiben.

Der Steuerabzug unterbleibt, soweit die anzurechnenden Kapitalerträge den Freibetrag von 6 000 DM für Alleinstehende und 12 000 DM für Verheiratete zuzüglich des Werbungskosten-Pauschbetrags nicht übersteigen und der Gläubiger der Kapitalerträge dem zum Steuerabzug Verpflichteten (z. B. Kreditinstitut, Bausparkasse) einen *Freistellungsauftrag* nach amtlich vorgeschriebenem Vordruck erteilt hat (§ 44 a Abs. 1 Nr. 1 und Abs. 2 Nr. 1 EStG). Wer zum Steuerabzug verpflichtet ist, hat dem *Bundesamt für Finanzen* auf Verlangen die Angaben aus dem Freistellungsauftrag zu Kontrollzwecken mitzuteilen (§ 45 d Abs. 1 EStG).

Das Bundesministerium der Finanzen hat mich bei der Erarbeitung des Gesetzentwurfs beteiligt. Entsprechend meiner Empfehlung wurde im einzelnen gesetzlich festgelegt, welche personenbezogenen Daten im Freistellungsauftrag enthalten sein und damit dem Bundesamt für Finanzen offenbart werden müssen (§ 45 d Abs. 1 EStG). Das Bundesamt für Finanzen darf diese Angaben nur verwenden, um die rechtmäßige Inanspruchnahme des Sparer-Freibetrags und des Pauschbetrags für Werbungskosten zu überprüfen (§ 45 d Abs. 2 EStG).

Während der Regierungsentwurf vorgesehen hatte, dem Bundesamt für Finanzen die Angaben „nur in ausgewählten Fällen" mitzuteilen, darf das Bundesamt für Finanzen nach dem beschlossenen Gesetz die *Daten aus allen Freistellungsaufträgen* abfordern. Ich werde die Verarbeitung der Daten beim Bundesamt für Finanzen aufmerksam verfolgen.

6.3 Antragsteller nach Vermögensgesetz kann Offenbarung seiner Daten widersprechen

Investitionen in den neuen Ländern werden erfahrungsgemäß durch unsichere Eigentumsverhältnisse erschwert. Der Gesetzgeber verfolgt das Ziel, diese Unsicherheit so schnell wie möglich zu beseitigen. Dazu soll beitragen, daß einem Investor vom Amt zur Regelung offener Vermögensfragen (Vermögensamt) nach glaubhafter Darlegung seines berechtigten Interesses Name und Anschrift eines Antragstellers i. S. des § 3 des Gesetzes zur Regelung offener Vermögensfragen (Vermögensgesetz) sowie der Vermögenswert, auf den sich die Anmeldung bezieht, mitgeteilt werden, wenn er mit dem Antragsteller eine direkte Einigung anstrebt (§ 32 Abs. 5 Vermögensgesetz). Der Antragsteller kann allerdings der Offenbarung dieser seiner Daten widersprechen. Ich habe dem Rechtsausschuß des Deutschen Bundestages vorgeschlagen, den Regierungsentwurf (BT-Drucksache 12/2480) dahin zu ergänzen, daß das Vermögensamt verpflichtet ist, jeden Antragsteller mit einer kurzen Widerspruchsfrist von zwei Wochen auf sein Widerspruchsrecht hinzuweisen, sobald ein Dritter erstmals eine Mitteilung im oben dargelegten Sinn beantragt. Der Gesetzgeber ist meiner Empfehlung gefolgt. Damit ist sichergestellt, daß jeder Antragsteller von seinem Widerspruchsrecht Gebrauch machen kann. Die kurze Widerspruchsfrist trägt dem Beschleunigungsgrundsatz Rechnung.

6.4 Zollverwaltungsgesetz datenschutzrechtlich noch mangelhaft — Zum Zollrechtsänderungsgesetz —

Im Zuge der Verwirklichung des europäischen Binnenmarkts ist ab 1. Januar 1993 ein Raum ohne Binnengrenzen für den freien Verkehr von Waren nach den Bestimmungen des EWG-Vertrages geschaffen worden. Für die Zollverwaltung ändern sich

insoweit die bisherigen Aufgaben. Im Zusammenhang mit dem innergemeinschaftlichen Warenverkehr ergeben sich neue Aufgaben. Die Bestimmungen des Zollgesetzes aus dem Jahre 1961 waren dementsprechend umzugestalten.

Gegenüber einem zunächst vom Bundesministerium der Finanzen vorgelegten Entwurf für das inzwischen verabschiedete Zollrechtsänderungsgesetz, mit dem das bisher geltende Zollgesetz zeitlich gestuft außer Kraft gesetzt und durch das Zollverwaltungsgesetz (ZollVG) ersetzt wird, hatte ich Bedenken erhoben, weil die Regelungen nicht ausreichend erkennen ließen, unter welchen Voraussetzungen und in welchem Umfang die Zollbehörden befugt sein sollten, personenbezogene Daten der Zollbeteiligten und sonstiger Personen zu erheben, zu verarbeiten und zu nutzen.

Wegen der Eilbedürftigkeit des Gesetzes, das zum Teil bereits am 1. Januar 1993 in Kraft treten mußte, hat sich die Bundesregierung außerstande gesehen, die auch von ihr als notwendig erkannten Regelungen noch in den Gesetzentwurf einzufügen. Immerhin erhielt das Zollverwaltungsgesetz eine Übergangsregelung, die das künftige „Inkrafttreten bereichsspezifischer gesetzlicher Regelungen" anspricht. Auch wird in der Begründung auf meine datenschutzrechtlichen Bedenken Bezug genommen (BT-Drucksache 12/3436 S. 19, zu § 28 Abs. 3). Ich bin daher zuversichtlich, daß die erforderlichen bereichsspezifischen Vorschriften über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Zollverwaltung möglichst bald geschaffen werden.

6.5 EG-weite Kontrolle über Warenlieferungen und -bewegungen

Für die Zeit nach dem Wegfall der Steuergrenzen für den Bereich der Umsatzsteuer zwischen den EG-Mitgliedstaaten am 1. Januar 1993 wurde das Besteuerungsverfahren neu geordnet. An die Stelle der bisherigen Grenzkontrollen tritt ein neues innerstaatliches und innergemeinschaftliches Kontrollverfahren (Richtlinie 91/680/EWG vom 16. Dezember 1991, umgesetzt durch das Gesetz zur Anpassung des Umsatzsteuergesetzes und anderer Rechtsvorschriften an den EG-Binnenmarkt — Umsatzsteuer-Binnenmarktgesetz — vom 25. August 1992, BGBl. I S. 1548ff.).

Die Unternehmer sind jetzt verpflichtet, über ihre innergemeinschaftlichen Warenlieferungen und -bewegungen gegenüber dem Bundesamt für Finanzen eine *Zusammenfassende Meldung* abzugeben. Der Gesetzgeber hat den unter meiner Beteiligung erarbeiteten Vorschlag der Bundesregierung akzeptiert, daß das Bundesamt für Finanzen von den Landesfinanzbehörden nur die zur Bestimmung der meldepflichtigen Unternehmer erforderlichen Angaben erhält und diese nur dazu verwenden darf, die Abgabe der Zusammenfassenden Meldungen sicherzustellen. Angaben aus den Zusammenfassenden Meldungen darf das Bundesamt für Finanzen den Landesfinanzbehörden mitteilen, soweit sie dort für steuerliche Kontrollen benötigt werden (§ 18a UStG).

Für die Nutzung der *Umsatzsteuer-Identifikationsnummer* der am innergemeinschaftlichen Handel beteiligten Unternehmen sowie den Datenaustausch zwischen dem Bundesamt für Finanzen und den Landesfinanzbehörden sowie den zuständigen Behörden der anderen EG-Mitgliedstaaten wurden auf meine Anregung entsprechende datenschutzrechtliche Regelungen getroffen (§ 27a UStG).

6.6 Erweiterte Amtshilfe unter den EG-Staaten im Bereich der Verbrauchsteuern

Die Vollendung des europäischen Binnenmarkts zum 1. Januar 1993 macht eine Erweiterung der Amtshilfe innerhalb der Mitgliedstaaten der EG erforderlich. In den Geltungsbereich der EG-Amtshilfe-Richtlinie vom 19. Dezember 1977 sind daher die Verbrauchsteuern auf Mineralöl, Alkohol, alkoholische Getränke und Tabakwaren einbezogen worden. Zur Umsetzung in das deutsche Recht hat die Bundesregierung das *EG-Amtshilfe-Gesetz* vom 19. Dezember 1985 (BGBl. I 1985, S. 2441f.) geändert (Artikel 10 des Gesetzes zur Anpassung von Verbrauchsteuer- und anderen Gesetzen an das Gemeinschaftsrecht sowie zur Änderung anderer Gesetze — Verbrauchsteuer-Binnenmarktgesetz —, BGBl. I 1992 S. 2204ff.). Darin sind meine Empfehlungen zum bereichsspezifischen Datenschutz, in die auch Hinweise aus dem Kreise der Landesbeauftragten für den Datenschutz eingeflossen sind, in folgenden wesentlichen Punkten berücksichtigt:

- Der Betroffene muß vor der Erteilung von personenbezogenen *Einzelauskünften* über ihn, sei es auf oder ohne Ersuchen, auch im Bereich der Verbrauchsteuern *regelmäßig angehört* werden.
- Solche *Auskünfte* dürfen *ohne Ersuchen* nur erteilt werden, wenn „tatsächliche Anhaltspunkte die Vermutung rechtfertigen", daß anderenfalls die Besteuerung gefährdet ist.
- In den Fällen, in denen nach deutschem Recht ein bereits übermitteltes personenbezogenes Datum zu *berichtigen*, zu *sperren* oder zu *löschen* wäre, sind alle Mitgliedstaaten, die die Auskunft erhalten haben, unverzüglich zu unterrichten und anzuhalten, die Berichtigung, Sperrung oder Löschung dieses Datums vorzunehmen.
- Eine *Weitergabe von Auskünften* an einen dritten Mitgliedstaat ist nur zulässig, soweit dies für die Erhebung der direkten und indirekten Steuern erforderlich ist und wenn der Staat, der die Auskunft gegeben hat, zugestimmt hat.

Mit der *Einrichtung einer automatisierten Datenbank* über die von den Finanzbehörden erteilten Bewilligungen für die Versendung und den Empfang verbrauchsteuerpflichtiger Waren unter Steueraussetzung soll sichergestellt werden, daß die Zollverwaltungen und die Wirtschaftsbeteiligten feststellen können, ob andere Wirtschaftsbeteiligte berechtigt sind, im EG-Binnenmarkt Waren unter Steueraussetzung zu beziehen. Die hierzu im Gesetz getroffenen Regelungen über die Verarbeitung personenbezogener

Daten entsprechen datenschutzrechtlichen Anforderungen.

Das Gesetz zeichnet sich im ganzen durch ein erfreuliches Datenschutzniveau aus.

6.7 Europäische Zollunterstützungsabkommen

6.7.1 EG-Zollinformationssystem muß Datenschutz berücksichtigen

Mit der Abschaffung der Zollkontrollen an den innergemeinschaftlichen Grenzen ist es erforderlich geworden, die gegenseitige Unterstützung der Mitgliedstaaten und deren Zusammenarbeit mit der EG-Kommission zu verstärken, um die *ordnungsgemäße Anwendung der von der EG erlassenen Zoll- und Agrarregelungen* zu gewährleisten. Die EG-Kommission beabsichtigt daher, zur Bekämpfung von Zuwiderhandlungen eine den Mitgliedstaaten zugängliche zentrale Datenbank (EG-Zollinformationssystem) einzurichten.

Zu diesem Zweck hat die Kommission einen Vorschlag für eine entsprechende Verordnung erarbeitet, die an die Stelle der bisher für die gegenseitige Unterstützung maßgeblichen Verordnung (EWG) des Rates Nr. 1468/81 treten soll. Das Bundesministerium der Finanzen bemüht sich mit meiner Beteiligung darum, daß für die *automatisierte Datenverarbeitung* im EG-Zollinformationssystem die datenschutzrechtlichen Regelungen in die neue Verordnung aufgenommen werden, die bereits für das — für die Anwendung *nationaler* Vorschriften eingerichtete — Zollinformationssystem der EG-Mitgliedstaaten (CIS) vorgesehen sind (s. 26.3) und weitgehend dem Datenschutzstandard des Schengener Durchführungsübereinkommens entsprechen. Darüber hinaus soll erreicht werden, auch den *konventionellen Datenaustausch* nach dem Vorbild des Schengener Durchführungsübereinkommens zu regeln. Die Kommission ist diesen Vorschlägen bislang nur teilweise gefolgt. Sie will sich grundsätzlich an dem Entwurf einer *EG-Datenschutz-Richtlinie* orientieren und weitergehende Vorstellungen einzelner Mitgliedstaaten nicht berücksichtigen.

Da derzeit nicht abzusehen ist, wann und mit welchem Inhalt die EG-Datenschutz-Richtlinie in Kraft treten wird, werde ich das Bundesministerium der Finanzen weiterhin dabei unterstützen, auf ausreichende *bereichsspezifische* Datenschutzvorkehrungen hinzuwirken.

6.7.2 Kooperationsabkommen der EG mit Drittländern

Die EG beabsichtigt, mit ihren wichtigsten Handelspartnern (osteuropäische, mittel- und zentralamerikanische Staaten, Staaten der GUS u. a.) Kooperationsabkommen zu schließen. Die konventionelle *Zusammenarbeit der Zollverwaltungen* soll dabei in „Protokollen über die Amtshilfe im Zollbereich" geregelt werden.

Mit den beteiligten Ressorts bin ich bemüht, die EG-Kommission davon zu überzeugen, daß die von ihr bisher vorgesehenen Datenschutzregelungen zur Wahrung des Rechts auf informationelle Selbstbestimmung nicht ausreichen.

6.7.3 Bilaterale Verträge mit datenschutzrechtlichen Mängeln

Die Amtshilfe zwischen der Bundesrepublik Deutschland und Drittländern (z. B. Polen, Ungarn, Russische Föderation) wird im Bereich nationaler Zuständigkeiten in Verträgen über die *gegenseitige Unterstützung der Zollverwaltungen* bilateral geregelt.

Soweit ich rechtzeitig beteiligt worden bin, habe ich zu den Vertragsentwürfen Stellung genommen und dabei insbesondere empfohlen,

- die Voraussetzungen für die Übermittlung personenbezogener Daten ohne Ersuchen zu präzisieren,
- die Zweckbindungsvorschriften enger zu fassen,
- die für die Erteilung von Auskünften an den Betroffenen zuständigen Behörden zu benennen, und
- vorzusehen, daß übermittelte personenbezogene Daten gelöscht werden, wenn ihre Speicherung zur Aufgabenerfüllung nicht mehr erforderlich ist.

Ich bedaure, daß meine Vorschläge nicht berücksichtigt worden sind.

6.8 EG-Kommission erhält automatisiert Daten über EG-Agrarausgaben

Die aus dem *Europäischen Ausrichtungs- und Garantiefonds für die Landwirtschaft* finanzierten Ausgaben der Europäischen Gemeinschaft (z. B. Erstattungen bei der Ausfuhr nach dritten Ländern, Interventionen zur Regulierung der Agrarmärkte) werden von den hierzu ermächtigten Stellen der Mitgliedstaaten geleistet (siehe auch 8.1). Die Angaben über die Zahlungsvorgänge müssen der EG-Kommission zur Prüfung des Rechnungsabschlusses übermittelt werden (Verordnung (EWG) Nr. 729/70 des Rates vom 21. April 1970 über die Finanzierung der gemeinsamen Agrarpolitik i. d. F. der VO (EWG) Nr. 2048/88).

Das für die Rechnungslegung zuständige Bundesministerium der Finanzen hat mir mitgeteilt, daß die über die Zahlungsvorgänge benötigten Daten der EG-Kommmission künftig auf automatisierten Datenträgern übermittelt werden sollen. Auf sein Betreiben werden die personenbezogenen Daten der Zahlungsempfänger zunächst in anonymisierter Form zur Verfügung gestellt; der volle Datenumfang wird für die Fälle nachgeliefert, die die Prüfer der EG-Kommission als Stichproben ausgewählt haben. Auf meine Anregung hat es weiterhin erwirkt, daß die EG-Kommission sich verpflichtet,

— die übermittelten Daten nur zur Prüfung des Rechnungsabschlusses zu verwenden, und

— die personenbezogenen Daten zu löschen, wenn sie zu diesem Zweck nicht mehr benötigt werden.

6.9 Abschriften von Urkunden an Finanzbehörden

Die Finanzbehörden sollen — so § 93 Abs. 1 Satz 3 AO — bei der Ermittlung des für die Besteuerung maßgeblichen Sachverhalts andere Personen als den jeweils betroffenen Steuerpflichtigen erst dann um Auskunft bitten, wenn die Sachverhaltsaufklärung bei diesem nicht zum Ziele führt oder keinen Erfolg verspricht. Als Ausnahme von diesem Grundsatz sehen das Erbschaftsteuer- und Schenkungsteuergesetz sowie das Grunderwerbsteuergesetz vor, daß Gerichte, Notare und Behörden den Finanzbehörden im Rahmen ihrer Anzeigepflicht vollständige beglaubigte Abschriften von Urkunden, z. B. von Verfügungen von Todes wegen, übersenden. Meine Bemühungen zu erreichen, daß die Finanzbehörden die Urkundsabschriften — mit zum Teil von ihnen nicht benötigten rein persönlichen Daten wie z. B. Motiven für eine letztwillige Verfügung — *nicht von Dritten* erhalten, blieben bisher ohne Erfolg (vgl. 13. TB S. 90, dort Nr. 9; 12. TB S. 30).

Dem Bundesministerium der Finanzen liegt gegenwärtig mein neuer Vorschlag vor, daß Gerichte, Notare und Behörden den Finanzbehörden in den im Erbschaftsteuer- und Schenkungsteuer- sowie im Grunderwerbsteuergesetz genannten Fällen lediglich die steuerlich maßgeblichen *Sachverhalte* (z. B. Grundstückskauf, Erbfall mit Vorliegen eines Testaments) *anzeigen* und die betroffenen *Personen benennen*. Auf diese Weise würden die Finanzbehörden die Angaben erhalten, die sie benötigen, um ihrerseits unter Mitwirkung des — ggf. auch zur Vorlage von Urkunden verpflichteten — Steuerpflichtigen den Sachverhalt im einzelnen aufklären zu können. Ein solches Verfahren entspricht auch § 97 Abs. 2 Satz 1 AO, wonach die Vorlage von Urkunden in der Regel erst dann verlangt werden soll, wenn der Vorlagepflichtige eine Auskunft nicht erteilt hat, wenn die Auskunft unzureichend ist oder Bedenken gegen ihre Richtigkeit bestehen.

Die Bundesnotarkammer hat meinem Vorschlag zugestimmt. Das BMF hat eine Stellungnahme angekündigt.

6.10 Kontrollmitteilungen an Finanzbehörden müssen neu geregelt werden

Die Bundesregierung kann zur Sicherung der Besteuerung mit Zustimmung des Bundesrates aufgrund des bereits durch das Steuerbereinigungsgesetz 1986 eingeführten § 93a Abgabenordnung (AO) Behörden durch Rechtsverordnung verpflichten, den Finanzbehörden bestimmte steuerlich relevante Sachverhalte wie z. B. Zahlungen von Honoraren an nebenamtlich in ihrem Auftrag tätige Lehrkräfte mitzuteilen. Solange diese Rechtsverordnung nicht vorliegt, fehlt es an einer Rechtsgrundlage für solche Mitteilungen. Das Bundesministerium der Finanzen hat dementsprechend auf meine Empfehlung hin die Verwaltungsanweisung aus dem Jahre 1967 aufgehoben, die solche Kontrollmitteilungen anordnete (s. 13. TB S. 90, dort Nr. 8).

In der jetzt schon länger andauernden Beratung des Entwurfs für die Rechtsverordnung nach § 93 a AO konnte ich zuletzt noch die textliche Klarstellung erreichen, daß eine Übermittlung solcher Mitteilungen nicht im automatisierten Abrufverfahren stattfindet. Nach dem gegenwärtigen Bearbeitungsstand dürfte die Rechtsverordnung nunmehr in absehbarer Zeit erlassen werden.

6.11 Keine Pflicht zu Meldungen für die Betriebskartei der Hauptzollämter

Die für Außenprüfungen zuständigen Hauptzollämter (s. §§ 193 ff. AO) führen eine Kartei mit Angaben über die für ihre Aufgabenerfüllung bedeutsamen Steuerpflichtigen ihres Bezirks (Betriebskartei). Durch eine Bürgereingabe ist mir bekannt geworden, daß die bisher manuell geführten Betriebskarteien auf automatisierte Verfahren umgestellt werden und die Hauptzollämter aus diesem Anlaß bei den Steuerpflichtigen allgemeine Datenerhebungen mit Fragebogen allein zu dem Zweck durchführen, den Datenbestand zu aktualisieren.

Ich habe gegenüber dem Bundesministerium der Finanzen darauf hingewiesen, daß die §§ 90 und 93 AO, die es zunächst als Rechtsgrundlage für die Fragebogenaktionen der Hauptzollämter genannt hatte, einen *konkreten Anlaß* zur Ermittlung steuerlich erheblicher Umstände voraussetzen und für Auskunftsersuchen in dieser *allgemeinen* Form keine Rechtsgrundlage bieten.

Das BMF hat sich im Ergebnis meiner Auffassung angeschlossen, daß nach den genannten Vorschriften eine Datenerhebung (Auskunftsersuchen) nur zur Feststellung eines für die Besteuerung erheblichen Sachverhalts erfolgen darf und die Umstellung der Betriebskarteien auf ein automatisiertes Verfahren keinen solchen Sachverhalt darstellt. Es hat daher die Hauptzollämter angewiesen, die Steuerpflichtigen bei allgemeinen Datenerhebungen zur Aktualisierung der Betriebskartei ausdrücklich darauf hinzuweisen, daß sie zur Beantwortung der Anfragen nicht verpflichtet sind.

7 Wirtschaft

7.1 Bundesausfuhramt und Änderung des Außenwirtschaftsgesetzes

In Ergänzung der in den letzten Jahren geschaffenen Regelungen zur Verbesserung der Außenwirtschaftskontrolle (12. TB S. 83, 13. TB S. 71 f., 94), wurde durch das Gesetz über die Errichtung eines Bundesausfuhramtes eine neue Bundesbehörde geschaffen. Das Bundesausfuhramt hat Verwaltungs- und Überwachungsaufgaben, die ihm durch das Außenwirt-

schaftsgesetz, das Kriegswaffenkontrollgesetz, das Atomgesetz und andere Bundesgesetze sowie aufgrund dieser Gesetze zugewiesen sind. Datenschutzrechtlich von besonderem Interesse ist es, daß dem Bundesausfuhramt aufgrund einer Ergänzung des Außenwirtschaftsgesetzes die gleichen Übermittlungsbefugnisse zustehen, wie dem Bundesamt für Wirtschaft.

Der Gesetzesentwurf enthielt eine Regelung, die das Zollkriminalamt ermächtigt hätte, im automatisierten Abrufverfahren auch Daten beim Bundesamt für Wirtschaft abzurufen. Diese Regelung war zumindest verfrüht, weil die fraglichen Daten nicht in der für einen automatisierten Abruf notwendigen Form geführt werden sollten. Sie war auch überflüssig, weil § 10 BDSG die Fragen des automatisierten Abrufs in einer Weise löst, die auch für diesen Fall angemessen ist, wenn die technischen Voraussetzungen gegeben sind. Auf meine Empfehlung hat der für den Gesetzentwurf federführende Wirtschaftsausschuß des Deutschen Bundestages die Ermächtigung für das Zollkriminalamt gestrichen.

7.2 Personenbezogene Daten eines Wirtschaftsprüfers trotz Widerspruchs veröffentlicht

Die Wirtschaftsprüferkammer veröffentlichte im Wirtschaftsprüferverzeichnis 1991 Namen und Anschriften aller Wirtschafts- und vereidigten Buchprüfer sowie Wirtschafts- und Buchprüfungsgesellschaften. Trotz des ausdrücklichen Widerspruchs eines Wirtschaftsprüfers gegen seine Nennung in diesem Verzeichnis waren auch seine Daten darin enthalten, weshalb er sich an mich gewandt hat.

Nach der Wirtschaftsprüferordnung führt die Kammer ein Berufsregister, das von jedermann ohne Begründung eingesehen werden darf. Zur Veröffentlichung in Form eines Druckwerks ist die Kammer nicht verpflichtet. Deshalb hätte das Selbstbestimmungsrecht des Betroffenen wenigstens in der Weise respektiert werden müssen, daß man seinen Widerspruch beachtete. Die Kammer berief sich jedoch auf ihre Aufgabe, die beruflichen Belange der Gesamtheit der Mitglieder zu wahren. Dazu müßten Namen und Anschriften aller Berufsangehörigen einem interessierten Publikum, aber auch Gerichten und Behörden, zur Verfügung gestellt werden. Ich erkenne diese Aufgabe an, kann aber nicht nachvollziehen, wieso es dazu erforderlich ist, durch eine Veröffentlichung die Daten des Betroffenen auch gegen seinen Widerspruch einem unbegrenzten Personenkreis zugänglich zu machen. Ich habe daher die Veröffentlichung trotz Widerspruchs als einen Verstoß gegen §§ 3, 11 BDSG alter Fassung förmlich beanstandet.

Gleichzeitig habe ich dem Bundesminister für Wirtschaft vorgeschlagen, die Wirtschaftsprüferordnung um eine Regelung zu ergänzen, die sowohl dem öffentlichen Interesse an dem Wirtschaftsprüfer-Verzeichnis als auch den schutzwürdigen Interessen der betroffenen Wirtschafts- und vereidigten Buchprüfer Rechnung trägt. Der Bundesminister hat mittlerweile einen entsprechenden Gesetzesentwurf zur Änderung der Wirtschaftsprüferordnung vorgelegt, nachdem der Widerspruch des Betroffenen gegen eine Veröffentlichung zu beachten ist und der darüber hinaus auch Regelungen über die sonstige Erhebung und Verarbeitung personenbezogener Daten von Wirtschafts- und vereidigten Buchprüfern enthält.

7.3 Datenschutzgerechte Änderung gewerberechtlicher Vorschriften vorgesehen

Das Bundesministerium für Wirtschaft hat den Entwurf eines Gesetzes zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften erarbeitet, dessen Ziel es vorrangig ist, datenschutzrechtlich relevante Vorschriften der Gewerbeordnung den Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts anzupassen. Bei der Erarbeitung des Entwurfes bin ich in einer erfreulich frühen Phase zugezogen worden. Der Entwurf enthält Regelungen über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, die der Gewerbeüberwachung dienen sollen.

Auch die Übermittlung von personenbezogenen Daten aus der Gewerbeanzeige wurde in dem Entwurf datenschutzrechtlich zufriedenstellend geregelt. Diese Daten dienen vielen recht unterschiedlichen Zwecken. So werden Angaben aus der Gewerbeanzeige z. B. an die Industrie- und Handelskammern, die Handwerkskammern, die für den Arbeitsschutz zuständige Landesbehörde, an das Eichamt, an die Bundesanstalt für Arbeit und an die Allgemeinen Ortskrankenkassen übermittelt. Auch die Gewerbeanzeigenstatistik wird aus Angaben aus den Gewerbeanzeigen gespeist.

Für den Umgang mit personenbezogenen Daten im Rahmen der Gewerbeüberwachung und für die Übermittlung von Daten aus der Gewerbeanzeige konnten ebenso datenschutzrechtlich zufriedenstellende Lösungen gefunden werden wie für eine Regelung zur Übermittlung von personenbezogenen Daten aus dem Gewerberegister an die wissenschaftliche Forschung.

7.4 Umgang mit personenbezogenen Daten von Handwerkern — Zur Handwerksordnung —

Auch die Handwerksordnung soll um Vorschriften ergänzt werden, die den Umgang mit personenbezogenen Daten regeln. Der Bundesminister für Wirtschaft hat mich und Vertreter der Datennutzer an der Beratung über einen entsprechenden Gesetzesentwurf beteiligt. Im Ergebnis wurden Regelungen entworfen, die sowohl den praktischen Erfordernissen als auch den datenschutzrechtlichen Anforderungen entsprechen.

7.5 Unzulässige Datenspeicherung beim Bundesaufsichtsamt für das Versicherungswesen geändert

Aufgrund einer Verfügung des Präsidenten des Bundesaufsichtsamts für das Versicherungswesen übermittelten die Versicherungsgesellschaften dem Bundesaufsichtsamt für das Versicherungswesen halbjährlich formularmäßig Angaben über Fälle von Veruntreuungen durch Außendienstmitarbeiter mit u. a. folgenden Daten:

— Personalien des beschuldigten Mitarbeiters

— Begehungsweise der Veruntreuung

— Höhe des Schadens

— Inhalt des Führungszeugnisses

— Inhalt des Auszugs aus dem Gewerbezentralregister.

Die Angaben wurden in eine Handkartei übertragen, die Formulare fünf Jahre lang aufbewahrt. Sie sollten der Überwachung der Unternehmen hinsichtlich der Sorgfalt bei der Auswahl, Führung und Kontrolle ihrer Mitarbeiter dienen. Dazu war die Speicherung der vollständigen Personalien der Mitarbeiter aber offenbar nicht erforderlich, denn etwaige Wiederholungsfälle hätte man auch mit Hilfe einer geeigneten Codierung der Personalien erkennen und mit den beteiligten Versicherungen klären können.

Ich hatte über dieses Verfahren schon in meinem 12. Tätigkeitsbericht (S. 82) berichtet, allerdings damals noch unter Bezugnahme auf die Handhabung aufgrund eines Rundschreibens aus dem Jahr 1973.

Eine neue Verfügung des Bundesaufsichtsamtes vom Februar 1990 hat dann zwar die Untergrenze für Übermittlungen von einer Schadenshöhe von DM 5 000 auf eine solche von DM 10 000 heraufgesetzt, die nicht erforderliche und deshalb rechtswidrige Speicherung der Personalien jedoch nicht beendet. Deshalb habe ich dieses Verfahren wegen Verstoßes gegen § 9 BDSG (alt) gegenüber dem Bundesministerium der Finanzen beanstandet. Das Bundesaufsichtsamt hat daraufhin im Rahmen der Automatisierung das Verfahren so geändert, daß die Angaben über den Beschuldigten nicht mehr im Klartext, sondern in einer codierten Form gespeichert werden. Diese Form läßt die Personen nicht mehr ohne weiteres erkennen und ermöglicht es trotzdem, Meldungen zusammenzuführen, die sich auf dieselbe Person beziehen, weil die Meldungen dann denselben Code führen. Die Speicherung beim Aufsichtsamt erfolgt in einer Form, die einer Anonymisierung im wesentlichen gleichwertig ist. Damit ist meinen Bedenken Rechnung getragen.

Ich muß allerdings darauf hinweisen, daß ein vergleichbares Verfahren für die Überwachung von Außendienstmitarbeitern von Bausparkassen inzwischen eingestellt wurde. Die Erfahrungen hatten dort gezeigt, daß solche Übermittlungen und Speicherungen personenbezogener Daten zur Kontrolle von Bausparkassen nicht erforderlich sind.

8 Landwirtschaft

8.1 Kommt der gläserne Landwirt? — Die neue Struktur der Agrarförderung —

Die EG hat eine grundlegende Änderung für die Struktur der Agrarförderung beschlossen. An die Stelle von Preisstützungen sollen betriebsbezogene Förderungsmaßnahmen treten, mit denen der Überproduktion entgegengewirkt werden soll. Die Maßnahmen sollen so durchgeführt werden, daß über jeden einzelnen geförderten Betrieb detaillierte Angaben über eigene und gepachtete Flächen und deren Nutzung sowie über den Viehbestand erhoben und verarbeitet werden. Weil unsere Landwirtschaft über viele Familienbetriebe verfügt, sind viele der Betriebsdaten auch personenbezogene Daten der Betriebsinhaber, und Angaben zur Betriebsstruktur werden oft Angaben über die Familien der Betriebsinhaber enthalten. Wirtschaftliche Zwänge werden dazu führen, daß praktisch alle landwirtschaftlichen Betriebe die Förderungsmaßnahmen in Anspruch nehmen. Als Folge werden in den zuständigen Agrarverwaltungen der Länder umfangreiche und tiefgegliederte Datenbanken über die in der Landwirtschaft tätigen Personen und ihre wirtschaftlichen Aktivitäten entstehen. Die Neuregelung stellt ein typisches Beispiel dafür dar, wie durch Änderung materiell-rechtlicher Regelungen ein tatsächlicher oder vermeintlicher Zwang zur Erhebung und Speicherung einer großen Anzahl personenbezogener Daten entsteht, die man bei einer anderen materiell-rechtlichen Regelung überhaupt nicht bräuchte.

Es ist sicher nicht übertrieben zu sagen, daß die neuen EG-Regelungen nahe daran sind, den gläsernen Landwirt zu schaffen. Diese Befürchtungen sind besonders deshalb begründet, weil die EG-Verordnung Nr. 3508/92 „zur Einführung eines integrierten Verwaltungs- und Kontrollsystems für bestimmte gemeinschaftliche Beihilferegelungen" (InVeKoS), verlangt, die zur Durchführung der Förderprogramme angelegten Datensammlungen auch intensiv zur Kontrolle zu nutzen. Deshalb sollen z. B. alle Parzellen mit ihren Grenzen exakt erfaßt werden. In den Förderungsanträgen ist anzugeben, welche Fläche wie genutzt wird. Kontrolliert werden soll damit, ob etwa Flächen doppelt angemeldet sind. Es sollen Luftbilder und Satellitenaufnahmen erstellt und mit den Meldungen im Rahmen der Agrarförderung verglichen werden, um zu erkennen, ob der optische Eindruck der gemeldeten Nutzung entspricht.

Ob das Betrugsrisiko bei der Agrarförderung nach gesicherten Erfahrungen wirklich so groß ist, daß die Einrichtung eines generellen und damit auch vorbeugend wirksamen Kontrollverfahrens im überwiegenden Allgemeininteresse liegt, — nur dann ist es zulässig — vermag ich nicht zu beurteilen. Ich muß hier von der Einschätzung der Fachverwaltung ausgehen. In diesem Zusammenhang entsteht auch die Frage, ob das vorgesehene sehr komplizierte Datenerhebungs- und Kontrollverfahren angesichts der unterschiedlichen Verwaltungsstrukturen und -traditionen überhaupt geeignet ist, europaweit ein gerech-

tes und den Zielen der EG entsprechendes Agrarförderungsverfahren zu sichern.

Sieht eine Regelung vor, daß personenbezogene Daten nicht nur zu den beantragten Förderungsmaßnahmen, sondern generell auch für eine intensive Kontrolle eigener und fremder Angaben verwendet werden, so muß der Betroffene bei der Erhebung darauf hingewiesen werden. Das könnte durch eine verständliche Erläuterung in den Antragsformularen geschehen. Weil die Daten der Agrarförderung durch die Verwaltungen der Bundesländer erhoben und verarbeitet werden, richtet sich der gesetzlich geforderte Umfang eines solchen Hinweises und seiner Erläuterungen nach dem jeweiligen Landesdatenschutzgesetz. Die Bund-Länder-Arbeitsgruppe, die auf Einladung des Bundesministeriums für Landwirtschaft und Forsten (BML) diese Fragen beraten hat, ist meiner Anregung, eine solche Erläuterung in die Formulare aufzunehmen, leider nicht gefolgt. Eine nähere Regelung hierüber bleibt nun den einzelnen Ländern überlassen.

8.2 Prüfungsteilnehmer muß Betriebsdaten seines Ausbilders nicht offenbaren

Die Verordnung über die Anforderungen in der Meisterprüfung für den Beruf Landwirt/Landwirtin ist mittlerweile in Kraft getreten. Meine Bedenken gegen die ursprünglich vorgesehene Regelung, nach der der Prüfungsteilnehmer gezwungen werden konnte, in der schriftlichen Meisterarbeit detaillierte Angaben über den Betrieb zu offenbaren, in dem er tätig ist (13. TB S. 79f.), sind vom Bundesministerium für Ernährung, Landwirtschaft und Forsten (BML) berücksichtigt worden. Die Prüfungsordnung sieht nun vor, daß Gegenstand der schriftlichen Meisterarbeit nur „in der Regel" der Betrieb sein soll, in dem der Prüfungsteilnehmer tätig ist. Dies läßt Ausnahmen für die Fälle zu, in denen der Betriebsleiter dem Meisteranwärter keinen so genauen Einblick in den Betrieb gewähren will oder nicht möchte, daß die Prüfungskommission einen Einblick in seinen Betrieb erhält. In diesen Fällen soll möglichst ein anderer Betrieb Gegenstand der Meisterprüfung sein. Nicht mehr zwingend ist auch, daß die Buchführungsabschlüsse, die Einnahmen und Ausgaben in den einzelnen Betriebszweigen und andere betriebliche Aufzeichnungen über die natürlichen und wirtschaftlichen Grundlagen des Betriebes enthalten, Grundlage für die schriftliche Meisterarbeit sind. Die Meisterprüfungsordnung schreibt dies zwar als Sollvorschrift vor, weil nur eine fundierte und praxisnahe Analyse die Fähigkeiten des Prüfungsteilnehmers nachweisen kann. Allerdings ist es denkbar, daß der Betriebsleiter nicht bereit ist, dem Meisteranwärter Aufzeichnungen in dem dazu erforderlichen Umfang zur Verfügung zu stellen. Die ursprünglich vorgesehene verpflichtende Regelung über die Verwendung von Betriebsdaten bei der schriftlichen Hausarbeit hätte die Betriebsleiter dem Druck ausgesetzt, entgegen ihren persönlichen Interessen betriebliche Unterlagen zur Verfügung zu stellen, wenn sie Meisteranwärtern nicht die Chance zum Ablegen der Prüfung nehmen wollten.

9 Personaldaten

9.1 Schutz von Arbeitnehmerdaten endlich gesetzlich regeln

Es ist allgemeine Überzeugung, daß für den Umgang mit personenbezogenen Daten eines Arbeitnehmers oder Bediensteten durch seinen Arbeitgeber oder Dienstherrn besondere Regeln vorhanden sein müssen, die der Tatsache Rechnung tragen, daß der Arbeitnehmer/Bedienstete seinem Arbeitgeber/Dienstherrn in aller Regel als der sozial Schwächere gegenüber steht. Gleichwohl gelten bis heute für den Schutz der personenbezogenen Daten von Arbeitnehmern, die bei privaten Arbeitgebern beschäftigt sind, grundsätzlich die Vorschriften des Dritten Abschnitts des Bundesdatenschutzgesetzes, die die Datenverarbeitung nicht-öffentlicher Stellen allgemein regeln und — abgesehen von § 28 Abs. 2 Nr. 1 Satz 2, letzter Anstrich — die Besonderheiten personenbezogener Daten im Arbeits- oder Dienstverhältnis nicht berücksichtigen. Die Vorschriften des Dritten Abschnitts des Bundesdatenschutzgesetzes gelten aufgrund des problematischen § 12 Abs. 4 BDSG (vgl. hierzu 9.2) auch für öffentlich-rechtliche und privatrechtliche Dienst- und Arbeitsverhältnisse bei öffentlichen Stellen des Bundes.

Einige Landesdatenschutzgesetze enthalten jeweils eine besondere Bestimmung über den Arbeitnehmerdatenschutz für die öffentlichen Bediensteten des jeweiligen Landes (z. B. § 22 BrDSG, § 28 HmbDSG, § 34 HDSG, § 29 DSGNW).

Die dargestellte Rechtslage wird seit langem als unbefriedigend empfunden. Sie ist nur deshalb einigermaßen erträglich, weil die Arbeitsgerichte inzwischen Grundsätze für den Umgang mit personenbezogenen Daten des Arbeitnehmers entwickelt haben und weil für Beamte, Soldaten und Zivildienstleistende das 9. Gesetz zur Änderung dienstrechtlicher Vorschriften angemessene Datenschutzregelungen gebracht hat.

Schon Mitte der 80iger Jahre haben sowohl die Datenschutzbeauftragten des Bundes und der Länder als auch der Deutsche Bundestag bereichsspezifische Regelungen für den Arbeitnehmerdatenschutz gefordert. Im Gegensatz zu anderen Bereichen, in denen der bereichsspezifische Datenschutz Fortschritte erzielen konnte, hat der Gesetzgeber im Bereich des Arbeitnehmerdatenschutzes bisher keinerlei Initiativen ergriffen. Auf dieses Defizit habe ich in meinen Tätigkeitsberichten (10. TB S. 28, 11. TB S. 26 und 13. TB S. 87) sowie vor dem Ausschuß für Arbeit und Sozialordnung des Deutschen Bundestages wiederholt hingewiesen.

Als der Ausschuß für Arbeit und Sozialordnung des Deutschen Bundestages am 20. März 1991 der Bundesregierung empfohlen hatte, in dieser Legislaturperiode einen Gesetzentwurf für ein Datenschutzgesetz so rechtzeitig vorzulegen, daß es auch noch abschließend beraten werden kann, habe ich mich in einem Schreiben an das Bundesministerium für Arbeit und Sozialordnung gewandt und gebeten zu veranlassen, daß ein Arbeitnehmerdatenschutzgesetz erarbeitet

sowie der Bundesregierung zur Beschlußfassung vorgelegt wird. Daraufhin hat mir das BMA mitgeteilt, er erkenne die Berechtigung meines Anliegens grundsätzlich an, die Belastung seines Hauses mit anderen bedeutsamen Gesetzgebungsvorhaben sei jedoch so groß, daß die Vorbereitung einer gesetzlichen Regelung des Arbeitnehmerdatenschutzgesetzes noch einige Zeit in Anspruch nehmen werde. Obwohl der Ausschuß für Arbeit und Sozialordnung seine Empfehlung am 13. November 1991 bestätigt hat, ist mir von einer Aktivität im Bundesministerium für Arbeit und Sozialordnung zur Erarbeitung eines Arbeitnehmerdatenschutzgesetzes in der Folgezeit nichts bekannt geworden.

Auf meine Veranlassung hin hat die Konferenz der Datenschutzbeauftragten von Bund und Ländern in ihrer Sitzung am 23./24. März 1992 ebenfalls ein Arbeitnehmerdatenschutzgesetz gefordert. Um die Arbeit an einem solchen Gesetz zu unterstützen, hat sie in dem Beschluß auch Grundsätze für den sachlichen Inhalt eines solchen Gesetzes aufgestellt, die der Anlage 4 entnommen werden können. Ich habe den Beschluß der Datenschutzkonferenz im April 1992 dem Bundesministerium für Arbeit und Sozialordnung mit der Bitte übersandt, nun die Arbeit an dem Gesetzentwurf konkret in Angriff zu nehmen. Eine Reaktion darauf steht bis heute aus.

In seiner Sitzung am 5. Februar 1992 hat der Deutsche Bundestag die Beschlußempfehlung des Innenausschusses zu meinem 10. bis 13. Tätigkeitsberichten (Drucksache 12/4094, s. Anlage 1) angenommen, worin die Bundesregierung erneut aufgefordert wird, bereichsspezifische Regelungen zum Arbeitnehmerdatenschutzgesetz so rechtzeitig vorzulegen, daß sie in dieser Legislaturperiode noch verabschiedet werden können.

Auch das Land Nordrhein-Westfalen hat die Bundesregierung in der Sitzung des Bundesratsausschusses für Arbeit und Sozialpolitik am 11. März 1993 aufgefordert, nunmehr schnellstmöglich einen Gesetzentwurf mit Regelungen über den Arbeitnehmerdatenschutz vorzulegen. Ein Vertreter des BMA legte daraufhin nochmals dar, daß auch die Bundesregierung in dieser Frage ein Regelungsbedürfnis sehe. Die Arbeiten gingen voran. Es werde seitens des BMA versucht, bis Ende des Jahres 1993 einen Referentenentwurf zu erarbeiten.

9.2 Verbesserung des Personalaktenrechts der Beamten, Soldaten und Zivildienstleistenden

Im Berichtszeitraum hat sich die Konferenz der Datenschutzbeauftragten mit ihrer Entschließung vom 26./27. September 1991 zur datenschutzgerechten Gestaltung des Rechts des öffentlichen Dienstes geäußert (vgl. Anlage 3). Ein Teil der dabei angesprochenen Fragen ist inzwischen durch das Neunte Gesetz zur Änderung dienstrechtlicher Vorschriften, über dessen Entstehung und Inhalt ich bereits berichtet habe (zuletzt 13. TB S. 43), geregelt worden. Bei den Beratungen des Gesetzes im Innenausschuß des Deutschen Bundestages konnten die in der vorigen Legislaturperiode mit dem Bundesministerium des Innern abgesprochenen datenschutzrechtlichen Verbesserungen des Regierungsentwurfs, die ich im 13. Tätigkeitsbericht bereits dargelegt habe, verwirklicht werden. Außerdem wurden auch die noch erforderlichen Regelungen für die Behandlung der Personalakten der Zivildienstleistenden in das Gesetz aufgenommen. Das Gesetz ist am 1. Januar 1993 in Kraft getreten. Damit ist nunmehr das Personalaktenrecht für Beamte weitgehend und — obwohl nicht alle meine Wünsche berücksichtigt worden sind — auf einem im ganzen erfreulichen datenschutzrechtlichen Niveau geregelt.

Ich bedauere allerdings, daß meine Forderung, die Regelung in § 12 Abs. 4 BDSG zu streichen, nicht berücksichtigt worden ist. Nach dieser Vorschrift gelten für die Datenverarbeitung im Zusammenhang mit Dienst- und Arbeitsverhältnissen die Vorschriften des Bundesdatenschutzgesetzes für den nichtöffentlichen Bereich. Es bleibt somit weiterhin bei einer datenschutzrechtlichen Schlechterstellung besonders der Angestellten und Arbeiter des Bundes gegenüber vielen entsprechenden Landesbediensteten, für die es keinen sachlichen Grund gibt. Ich hoffe, daß in dieser Frage noch nicht das letzte Wort gesprochen ist und werde mich auch künftig für eine Beseitigung des auch rechtssystematisch verfehlten § 12 Abs. 4 BDSG einsetzen.

9.3 Beihilfedaten sind besonders sensibel

In Beihilfeverfahren muß der Bundesbedienstete erfahrungsgemäß Daten über seinen Gesundheitszustand, die dem Patientengeheimnis unterliegen, offenbaren. Dem muß die Gestaltung des Beihilfeverfahrens entsprechen.

9.3.1 Abschottung der Beihilfestelle — immer wieder problematisch

Seit langem wird die Abschottung der Bearbeitung der Beihilfeangelegenheiten von der übrigen Personalverwaltung gefordert. Dieser Grundsatz ist in der seit dem 1. Januar 1993 geltenden Regelung des § 90a BBG nun gesetzlich festgeschrieben (s. o. 9.2). Im Berichtszeitraum konnte ich mehrfach zur Durchsetzung dieser Vorschrift beitragen.

Die Kaufmännische Krankenkasse Hannover (KKH) hat aufgrund meiner Empfehlungen zur Bearbeitung von Beihilfevorgängen (vgl. 12. TB S. 68) zwischenzeitlich die Bearbeitung von Beihilfeangelgenheiten ihrer Mitarbeiter und deren Angehörigen vollständig von der Personalverwaltung getrennt (s. 13. TB S. 93). Die Bearbeitung erfolgt in einer eigenen Stelle für die Leistungsangelegenheiten der bei der KKH versicherten Mitarbeiter. Über Widersprüche in Beihilfeangelegenheiten entscheidet nunmehr ein bei der Krankenkasse tätiger Jurist, der an Personalentscheidungen nicht beteiligt ist und auf seine Geheimhaltungspflicht auch gegenüber Vorgesetzten schriftlich hingewiesen wurde.

Einer anderen Krankenkasse habe ich empfohlen, ebenso vorzugehen. Das stieß leider auf Umsetzungs-

probleme, da die Krankenkasse über keinen Juristen zur Entscheidung über Widerspruchsfälle in Beihilfeangelegenheiten verfügt. Als Lösung habe ich vorgeschlagen, die Widersprüche in einer Organisationseinheit zu bearbeiten, in der keine Mitarbeiter mitwirken, die zugleich Vorgesetzte des Widersprechenden sind.

Eine Antwort der Krankenkasse steht noch aus.

9.3.2 Trennung von Beihilfestellen und Personalverwaltung trotz Einwilligung des Bediensteten erforderlich

Im Rahmen einer Eingabe wurden datenschutzrechtliche Bedenken im Hinblick auf das in den Verwaltungsstellen der Bundesknappschaft praktizierte Beihilfeverfahren an mich herangetragen. Der Petent monierte, daß die Beihilfeanträge und die dazugehörigen Unterlagen bei der Personalabteilung der Verwaltungsstelle zur Erstattung eingereicht werden und der anschließende Beihilfebescheid unter Vorlage der Arztrechnung durch den Verwaltungsstellenleiter unterzeichnet wird. Der Petent sah insoweit die Gefahr, daß sowohl die Personalabteilung als auch der Verwaltungsstellenleiter über die in den Belegen genannten Diagnosen Rückschlüsse auf den Grund einer Arbeitsunfähigkeit ziehen könnten. Daraus befürchtete er dienstliche Nachteile.

Nach Darlegung der Bundesknappschaft haben ihre Verwaltungsstellen das Beihilfeverfahren in eigener Zuständigkeit nach folgenden Grundsätzen geregelt:

1. Der Leiter der Verwaltungsstelle wird in die Bearbeitung der Anträge von aktiven Bediensteten nicht eingeschaltet; er unterzeichnet Beihilfebescheide nicht.

2. Mitarbeiter aus dem Bereich Personalwesen werden mit der Bearbeitung der Beihilfeanträge befaßt, wenn der Antragsteller zugestimmt hat. Anderenfalls wird der Antrag im Wege der Amtshilfe von einer anderen Verwaltungsstelle bearbeitet.

3. Die Beihilfe-Akten werden außerhalb der Personalstelle aufbewahrt.

Diese Bearbeitung von Beihilfeanträgen ist insoweit nicht mit datenschutzrechtlichen Vorschriften zu vereinbaren, als eine Befassung der Mitarbeiter der Personalverwaltung mit solchen Anträgen durch die Zustimmung des Antragstellers gerechtfertigt werden soll.

Die vom Gesetzgeber geforderte grundsätzliche Trennung der Beihilfebearbeitung von der Personalverwaltung unterliegt nicht der Disposition der Bediensteten.

Dabei verkenne ich nicht, daß § 90a Satz 3 BBG eine „Soll-Vorschrift" enthält, die kleineren personalverwaltenden Behörden einen gewissen Spielraum bei der Abschottung von Beihilfestellen und Personalverwaltung läßt. Dieser setzt aber voraus, daß die Dienststelle ihr Abweichen von der Regel der getrennten Bearbeitung im Einzelfall nachvollziehbar begründet. Tatsachen, um einen solchen Ausnahmefall hier annehmen zu können, hat mir die Bundesknappschaft nicht vorgetragen.

Ich habe der Bundesknappschaft empfohlen, die Bearbeitung von Beihilfeanträgen neu zu regeln und bei ihren Planungen folgende Lösungsmöglichkeiten zu prüfen:

— Übertragung von Aufgaben außerhalb der Personalverwaltung auf den nicht voll ausgelasteten Beihilfebearbeiter.

— Zusammenfassung der Beihilfebearbeitung bei einer Beihilfestelle für mehrere Verwaltungsbereiche.

Eine Stellungnahme der Bundesknappschaft hierzu steht noch aus.

9.3.3 Beihilfeverfahren im Widerspruchsfall jetzt datenschutzgerecht geregelt

Nicht alle Beihilfeverfahren sind mit Antragstellung und Bewilligungsbescheid erledigt. Kommt es zu Meinungsverschiedenheiten zwischen der Dienststelle und dem Bediensteten, kann der letztere Widerspruch einlegen. Auch im Widerspruchsverfahren muß die Abschottung der Beihilfestelle von der übrigen Personalverwaltung gewährleistet sein. Das war bei der von mir kontrollierten Physikalisch-Technischen Bundesanstalt nicht gewährleistet. Widersprüche waren dort an den „Herrn Präsidenten der PTB" zu richten. Soweit Widersprüchen durch die Beihilfestelle der PTB nicht abgeholfen wurde, wurden sie gemäß § 172 BBG dem Bundesministerium für Wirtschaft zur Entscheidung zugeleitet. Das Übersendungsschreiben wurde in der PTB mit einem begleitenden Aktenvermerk von der Beihilfestelle über den Personalreferatsleiter und den Leiter der Verwaltung an den Vizepräsidenten geleitet. Der Präsident der PTB zeichnete letztendlich das Übersendungsschreiben.

Alle Beteiligten, über die das Übersendungsschreiben lief, wirken an Personalentscheidungen der PTB mit. Deshalb verstieß das Verfahren gegen den Grundsatz der Abschottung der Beihilfebearbeitung von der Personalverwaltung.

Ich habe der PTB empfohlen vorzusehen, daß Widersprüche gegen Beihilfebescheide beim Justitiariat der PTB einzulegen sind, das an der Verwaltung von Personalangelegenheiten nicht beteiligt ist. Dieses kann unter direkter Einbeziehung der Beihilfestelle prüfen, ob dem Widerspruch abzuhelfen ist. Ist dies nicht der Fall, kann das Justitiariat dem Bundesministerium für Wirtschaft den Widerspruch zur Entscheidung vorlegen. Die PTB hat meine Empfehlungen aufgriffen und in einer entsprechenden Hausverfügung umgesetzt.

9.3.4 Hochsensible Diagnosedaten dürfen nicht in den normalen Geschäftsgang

Eine oberste Bundesbehörde bewahrt alle dort geführten Personalakten, nämlich Personalhaupt-, Besoldungs- und Beihilfeakten, gemeinsam in einem verschlossenen Stahlschrank in einem Raum auf. Diese Aufbewahrung ist mit § 90a BBG nicht zu vereinbaren, wonach Unterlagen über Beihilfen stets als Teilakten zu führen und von der übrigen Personalakte getrennt aufzubewahren sind.

Meine Kontrolle einiger — durch die Beihilfesachbearbeiter beliebig ausgewählter — Beihilfeakten hat einen Verstoß gegen datenschutzrechtliche Vorschriften ergeben, den ich wegen seiner Bedeutung ausführlicher darstellen möchte:

In einer Beihilfeakte befand sich unverschlossen ein Schreiben einer Kurklinik. Darin beantragte die Klinikleitung die Verlängerung einer Kurmaßnahme für einen Mitarbeiter der obersten Bundesbehörde. Das Schreiben enthielt hochsensible Diagnoseangaben.

Das Schreiben der Klinik war an den „Vertrauensärztlichen Dienst der Beihilfestelle" adressiert und enthielt folgenden roten Stempelaufdruck der Klinik: „Vertrauliche Arztsache! Dieser Bericht dient ausschließlich der Information des behandelnden Arztes über die in der Klinik erhobenen Befunde. Seine Weitergabe an den Untersuchten oder an nichtärztliche Stellen ist nicht statthaft." Trotzdem ist das Schreiben, wie anhand des Eingangsstempels festgestellt werden konnte, in den allgemeinen Geschäftsgang gelangt. Es muß daher davon ausgegangen werden, daß es in der Registratur geöffnet wurde und dann in einer Umlaufmappe über den Referenten der zuständigen Abteilung und deren Leiter, der gleichzeitig Personalchef ist, und von dort zurück an die Registratur gelangt ist, die die Post an die Arbeitsbereiche verteilt.

Aufgrund meines Prüfungsbericht hat mir die oberste Bundesbehörde inzwischen mitgeteilt, sie habe die notwendigen organisatorischen Maßnahmen getroffen um sicherzustellen, daß Personen außerhalb der Beihilfestelle keine Kenntnis vom Inhalt von Schreiben mit Krankheitsdaten erhalten. Ich habe sie auch aufgefordert, die anderen Personalakten auf ähnliche Fehler zu überprüfen und Maßnahmen zu treffen, um derartige Fehler künftig auszuschließen.

9.4 Zugriff der Personalvertretung auf Teile der Personaldatei der Dienststelle

Im Rahmen eines Kontrollbesuches bei der Physikalisch-Technischen Bundesanstalt in Braunschweig (PTB) habe ich festgestellt, daß aufgrund einer Dienstvereinbarung über die Einrichtung und den Betrieb einer Personaldatenverarbeitung dem Personalrat direkter Zugriff auf bestimmte, im System „Personaldatenverarbeitung" gespeicherte Personalaktendaten gestattet wird. Hierbei handelt es sich u. a. um Titel, Name, Geburtsname, Geschlecht, ob Trennungsgeldempfänger, Laufbahngruppe, Laufbahnwechsel, ob Zulagen gewährt werden, Fragen zur Funktion und Qualifikation, sowie die Teilnahme an Lehrgängen.

Über ein Bildschirmgerät in der Personalverwaltung oder „an sonstiger geeigneter Stelle" kann der Personalrat diese Daten lesen sowie sich sortieren und ausdrucken lassen. Er kann jederzeit unbeschränkt auf alle ihm zugänglichen Daten zugreifen.

Gegen dieses in der Dienstvereinbarung festgelegte Verfahren habe ich aus datenschutzrechtlicher Sicht Bedenken erhoben. Der Zugriff des Personalrats verstößt — jedenfalls in dem festgestellten Umfang — wegen fehlender Einwilligung der Beschäftigten grundsätzlich gegen § 68 Abs. 2 Satz 3 Bundespersonalvertretungsgesetz (BPersVG).

§ 90 Abs. 1 Satz 2 BBG legt fest, daß zur Personalakte alle Unterlagen gehören — einschließlich der in Dateien gespeicherten —, die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten). § 68 Abs. 2 Satz 3 BPersVG bestimmt, daß Personalakten von Mitgliedern der Personalvertretung nur mit Zustimmung des Beschäftigten eingesehen werden dürfen. Dies gilt nicht nur für die Personalakte als ganzes, sondern auch für ihre einzelnen Bestandteile.

Im Rahmen der vertrauensvollen Zusammenarbeit mit dem Personalrat nach § 2 Abs. 1 und § 68 Abs. 2 Satz 1 und 2 BPersVG ist die Dienststelle verpflichtet, der Personalvertretung auch ohne Zustimmung des betroffenen Beschäftigten Auskünfte aus Personalakten zu geben, und zwar in dem Umfang, wie die Personalvertretung ihrer zur Erledigung einer bestimmten und konkreten Aufgabe objektiv bedarf.

Zu der oben dargestellten Zugriffsregelung bei der PTB habe ich auch das Bundesministerium des Innern um eine Stellungnahme gebeten. Das Bundesministerium hält sie für unzulässig.

Ich habe inzwischen die Beteiligten auf die rechtliche Problematik hingewiesen. Nach der vorgesehenen Erörterung mit diesen werde ich zu dem Vorgang abschließend Stellung nehmen.

9.5 Telefondatenverarbeitung

Das Thema Telefondatenverarbeitung bei den öffentlichen Stellen des Bundes ist auch in den letzten beiden Jahren verstärkt an mich herangetragen worden. Im Bereich der automatisierten Verarbeitung von Personaldaten stellte es ein Schwerpunktproblem dar, dem in der Praxis eine immer bedeutsamere Rolle zukommt.

9.5.1 Dienstanschlußvorschriften endlich erlassen

Nachdem ich die volle Speicherung der Verbindungsdaten von Telefongesprächen, die über Dienstapparate geführt wurden, problematisiert hatte, erstellte die Bundesregierung den Entwurf von neuen „Allgemeinen Verwaltungsvorschriften über die Einrichtung und Nutzung dienstlicher Fernmeldeanlagen für

die Bundesverwaltung mit Ausnahme der Deutschen Bundespost (Dienstanschlußvorschriften — DAV —)", der meine Empfehlungen weitgehend berücksichtigte.

Allerdings traten diese Vorschriften aus Gründen, die nicht mit dem Datenschutz zusammenhingen, zunächst nicht in Kraft (vgl. 10. TB S. 30/31, 11. TB S. 26/27, 13. TB S. 44). An dieser Lage hatte sich bis zum Oktober 1992 nichts geändert.

Auf meine Initiative haben der Innenausschuß sowie der Ausschuß für Post- und Telekommunikation des Deutschen Bundestages schließlich das Thema „Dienstanschlußvorschriften" im Rahmen der Beratungen meines 10. bis 13. TB behandelt. Der Innenausschuß hat dem Deutschen Bundestag empfohlen, die Bundesregierung aufzufordern, die neuen DAV unverzüglich in Kraft zu setzen.

Daraufhin erließ das Bundesministerium der Finanzen die „Allgemeine Verwaltungsvorschrift über die Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Bundesverwaltung (Dienstanschlußvorschriften — DAV —)" vom 1. Dezember 1992, die am 1. Januar 1993 in Kraft getreten ist. Für das Ministerium für Post und Telekommunikation und dessen nachgeordnete Dienststellen treten die Vorschriften ein Jahr später in Kraft. Damit hat die Bundesregierung die Anforderungen des Datenschutzes bei der automatisierten Verarbeitung von Telefondaten endlich berücksichtigt.

Aus datenschutzrechtlicher Sicht sind folgende Regelungen dieser DAV wegen ihrer Allgemeingültigkeit von besonderem Interesse:

1. Jede abgehende Wählverbindung ist grundsätzlich nachzuweisen. Hierzu sind durch schriftliche Aufzeichnung oder durch Speicherung mittels einer Telekommunikationsdatenerfassungsanlage

   — das Datum,

   — die Nebenstellennummer und — sofern nicht anderweitig festgehalten —,

   — der Name des Anmelders,

   — die Tarifeinheiten oder Leistungsentgelte und

   — bei privaten Verbindungen eine besondere Kennzeichnung festzuhalten.

   Bei dienstlichen Verbindungen sind die Vorwahl und/oder die Rufnummer des Angerufenen, bei privaten Verbindungen die Vorwahl und/oder die um die letzten beiden Ziffern verkürzte Rufnummer des Angerufenen festzuhalten. Ist keine automatische Telekommunikationsdatenerfassungsanlage vorhanden, kann bei Orts- und/oder Nahgesprächen der Nachweis der Verbindungen unterbleiben.

   Als Fortschritt gegenüber den bisherigen Regelungen bewerte ich insbesondere, daß bei den privaten Telefongesprächen die Ziel-Nummer nur um die letzten beiden Ziffern verkürzt nachzuweisen ist.

2. Die Nachweise über dienstliche Verbindungen und die Notwendigkeit der Gespräche sind — zumindest stichprobenweise — durch den Dienstvorgesetzen oder den von ihm Beauftragten zu überprüfen. Eine Verknüpfung mit anderen Dateien ist nicht zulässig. Die Nachweise sind innerhalb von drei Monaten nach Abschluß der Prüfung zu vernichten oder zu löschen.

   Die für Stichprobenzwecke gefertigten Ausdrucke sollten nur dem jeweiligen (Fach-)Vorgesetzen zugehen dürfen, da allein dieser in der Lage ist, die dienstliche Notwendigkeit eines solchen Telefongesprächs zu beurteilen. Ich empfehle daher, einen geeigneten Fachvorgesetzten mit der Prüfung zu beauftragen.

3. Bei Verbindungen der Personalvertretung in Personalratsangelegenheiten und anderen Stellen, deren Telefonverkehr nicht der Aufsicht unterliegt, sind nur die Verbindungsentgelte festzuhalten, sofern nicht die genannten Stellen eine Aufzeichnung/Speicherung der übrigen Verbindungsdaten verlangen.

   Diese Regelung, die eine unzulässige Kontrolle dieser Stellen bei der Erfüllung ihrer originären gesetzlichen Aufgaben oder ihrer besonderen Vertrauensbeziehungen verhindert, entspricht meinen bereits seit dem 4. Tätigkeitsbericht erhobenen Forderungen.

4. Hinsichtlich der Privatgespräche sind die Bediensteten über das in der Dienststelle angewandte Erfassungsverfahren, die Behandlung der erfaßten Daten und den Zweck der Telekommunikationsdatenerfassung sowie darüber zu informieren, daß ihr Einverständnis zu der jeweiligen Form der Telekommunikationsdatenerfassung mit Anmeldung oder Durchführung der Verbindung als erteilt gilt.

5. Beim Einsatz von Telekommunikationsdatenerfasssungsanlagen unterbleibt bei Privatgesprächen ein Ausdruck der verkürzten Rufnummer des Angerufenen. Auf Verlangen des Bediensteten ist jedoch ein Auszug der Nachweisung einschließlich der verkürzten Rufnummer des Angerufenen zu erstellen. Dieser Auszug darf nur von besonders Beauftragten gefertigt und in verschlossener Form dem Bediensteten zugeleitet werden. Eine Kenntnisnahme durch Dritte, soweit sie nicht für den Auszug und die Versendung unumgänglich sind, ist unzulässig und auszuschließen.

   Die gespeicherten Daten der Privatgespräche sind nach Abrechnung der Nachweisung unverzüglich zu löschen, maschinelle Ausdrucke zu vernichten. Handschriftlich aufgezeichnete Daten sind nach Bezahlung der Leistungsentgelte zu vernichten oder, soweit möglich, dem Bediensteten auszuhändigen.

6. Die Entgelte für private Verbindungen im Telefondienst, Telex-, Teletex-, Telefax- und Bildschirmtextschreiben sowie für Telegramme dürfen nicht im Gehaltsabzugsverfahren einbehalten werden.

Von den Vorschriften der DAV kann nur aus zwingenden dienstlichen Gründen mit Zustimmung des Bundesministeriums der Finanzen abgewichen werden.

Mit den neuen Dienstanschlußvorschriften wurde ein großer Schritt hin zu einer datenschutzgerechten Verarbeitung der Telefondaten der Bundesbediensteten gemacht.

9.5.2 Physikalisch-Technische Bundesanstalt beseitigte Mängel

Vor dem Hintergrund der vorstehend aufgeführten Thematik habe ich im vergangenen Jahr im Rahmen einer Datenschutzkontrolle auch die Telefondatenverarbeitung bei der Physikalisch-Technischen-Bundesanstalt in Braunschweig (PTB) geprüft.

Ich mußte feststellen, daß das dortige Verfahren in wesentlichen Punkten gegen die zum Kontrollzeitpunkt noch geltenden Dienstanschlußvorschriften vom 1. Juni 1976 verstieß und auch vielfach nicht in Einklang mit den neuen DAV stand.

Ungeachtet der völlig unterschiedlichen Zweckbestimmung wurden für Dienst- und Privatgespräche von Dienstanschlüssen dieselben Gesprächsdaten (Nebenstellennummer, Datum, Zielnummer, Gesprächs-Kennziffer, Uhrzeit und Zahl der Gebühreneinheiten) gespeichert.

Die Speicherung und der Ausdruck der Uhrzeit sind nach den DAV nicht erforderlich und daher unzulässig. Ich habe dringend empfohlen, die Speicherung und Verarbeitung der Uhrzeit, sowohl bei den Dienst-, als auch bei den Privatgesprächen, durch geeignete Maßnahmen zu unterbinden.

Die Zielnummer wurde auch bei den Privatgesprächen unverkürzt gespeichert und ausgedruckt. Unter Hinweis auf die neuen DAV habe ich deutlich gemacht, daß ich aus datenschutzrechtlichen Gesichtspunkten die Speicherung und den Ausdruck der vollständigen Zielnummer bei Privatgesprächen zum damaligen Zeitpunkt für bedenklich, ab dem 1. Januar 1993 für unzulässig halte.

Alle Gesprächsdaten wurden in der PTB kontinuierlich in Listen ausgedruckt. Das sich daran anschließende Verfahren ist sowohl im Hinblick auf Dienst-, als auch auf Privatgespräche datenschutzrechtlich problematisch.

So mußte ich feststellen, daß die Dienstgesprächslisten regelmäßig allen Referats-, Labor-, Gruppen- und Abteilungsleitern zur Kontrolle zugeleitet und anschließend an die Fernsprechzentrale zurückgeschickt wurden. Eine derartig kontinuierliche, sämtliche Hierarchiestufen einschließende Mehrfachkontrolle ist weder mit dem Erforderlichkeits- noch mit dem Verhältnismäßigkeitsprinzip vereinbar. Vielmehr ist in der Regel eine Stichprobenkontrolle des dienstlichen Fernsprechverhaltens durch den Dienstvorgesetzten oder den von ihm Beauftragten zur Kontrolle ausreichend. Ich habe empfohlen, die für Stichprobenzwecke gefertigten Ausdrucke nur dem jeweiligen (Fach-)Vorgesetzten zuzuleiten.

Die Ausdrucke der Daten aus Privatgesprächen wurden den Nebenstellenberechtigten auch in den Fällen zugesandt, in denen die Nebenstellen von mehreren Mitarbeitern genutzt wurden. Damit erhielten die Nebenstellenberechtigten auch Kenntnis sämtlicher privater Gesprächsdaten ihrer Kollegen. Auch dieses Verfahren ist datenschutzrechtlich problematisch.

Zur Verarbeitung von Telefongesprächsdaten des Personalrats, für die in der PTB keine besondere Handhabung vorgesehen ist, habe ich eine den Regelungen der neuen DAV entsprechende Behandlung vorgeschlagen.

Daten dienstlicher Gespräche werden im System nach Ausdruck, Privatgesprächsdaten nach Abrechnung gelöscht. Ich mußte jedoch feststellen, daß seit 1982 sämtliche Datenausdrucke über dienstliche Telefongespräche in der PTB aufgewahrt wurden und Aufbewahrungs- oder Vernichtungsregelungen dafür nicht bestanden.

Die PTB hat die vorhandenen, nicht erforderlichen Listenausdrucke im Anschluß an meine Kontrolle vernichtet.

In der die Telefondatenverarbeitung regelnden Hausverfügung der PTB, die erst im Juni 1992 unter Beteiligung der Personalvertretung erlassen worden war, waren die Grundsätze einer datenschutzgerechten Gestaltung der Telefondatenverarbeitung bedauerlicherweise nicht berücksichtigt worden.

Unter Hinweis auf die zum Zeitpunkt der Kontrolle noch geltenden wie auf die neuen DAV habe ich der PTB dringend die Abstellung der datenschutzrechtlichen Defizite empfohlen.

Die PTB hat zwischenzeitlich alle meine datenschutzrechtlichen Empfehlungen und Forderungen anerkannt und datenschutzgerecht reagiert. So wurden datenschutzrechtliche Defizite umgehend abgestellt und notwendige technische Änderungen — soweit mit der vorhandenen Telefonanlage möglich — veranlaßt. Die PTB hat mir ferner zugesichert, bei der im Jahre 1993/94 vorgesehenen Installationen einer bereits beantragten neuen ISDN-TK-Anlage die Anforderungen des Datenschutzes voll zu berücksichtigen. Über das weitere Verfahren werde ich mich informieren lassen.

Aus vorgenannten Gründen habe ich gemäß § 25 Abs. 2 BDSG von einer Beanstandung abgesehen.

9.6 Der künftige Dienstherr/Arbeitgeber darf nicht alles und jedes fragen

Im Berichtszeitraum hatte ich mich immer wieder mit der Frage zu befassen, welche personenbezogenen Daten im Rahmen eines Bewerbungsverfahrens erhoben und im Falle einer Einstellung gespeichert werden dürfen. Ich wurde u. a. mit der Zulässigkeit bestimmter Fragen auf Bewerberfragebögen und mit dem Problem, was mit den Unterlagen abgewiesener Bewerber zu geschehen hat, konfrontiert.

Im Berichtszeitraum hat das Neunte Gesetz zur Änderung dienstrechtlicher Vorschriften, das seit 1. Januar 1993 in Kraft ist (vgl. 9.2), für Beamte in § 90 Abs. 4 BBG festgelegt, daß der Dienstherr personenbezogene Daten über Bewerber nur erheben darf, soweit dies zur Begründung und Durchführung des Dienst-

verhältnisses erforderlich ist. Fragebogen, mit denen solche personenbezogenen Daten erhoben werden, bedürfen vom 1. Januar 1994 an der Genehmigung durch die zuständige oberste Dienstbehörde (§ 90 Abs. 4 Satz 2 BBG). Der Grundsatz, daß von Bewerbern nur die zur Begründung und Durchführung des Dienstverhältnisses erforderlichen Daten erhoben werden dürfen, gilt übrigens nicht nur für Bewerber, die Beamte werden wollen, sondern — aufgrund der Rechtsprechung der Arbeitsgerichte — auch für Bewerber um eine Anstellung als Angestellte oder Arbeiter. § 90 Abs. 4 BBG und der aufgeführte arbeitsrechtliche Grundsatz machen deutlich, daß die datenschutzrechtlichen Grenzen für die Erhebung von Personaldaten durch den Dienstherrn/Arbeitgeber schon bei der Gestaltung von Bewerberfragebögen beachtet werden müssen.

Ich erwarte von der Regelung in § 90 Abs. 4 Satz 2 BBG, daß in Zukunft Bewerberfragebögen vereinheitlicht und auf die notwendigen Fragen beschränkt werden. Vor dem Hintergrund dieser Regelung sind z. B. folgende, mir bekannt gewordene Fragen, in Bewerberfragebögen grundsätzlich unzulässig:

— Wohnsitz seit dem 16. Lebensjahr

— Zweitwohnsitz

— Geburtsdatum, Geburtsort, Kreis, Bundesland/Staat und Staatsangehörigkeit des Ehegatten

— Vornamen, Geburtsdaten, Beruf/Tätigkeit, Familienstand und Sterbejahr der Eltern

— frühere und jetzige Zugehörigkeit zu Vereinen, Organisationen und Parteien

— Angehörige außerhalb der Bundesrepublik Deutschland

Zumindest problematisch sind folgende in der Praxis auftauchende Fragen:

— *Wehr-/Ersatzdienst*

Für Zwecke der Personalplanung ist es sicherlich wichtig zu wissen, ob ein Bewerber seinen Wehr- oder einen Ersatzdienst noch abzuleisten hat. Es ist jedoch unerheblich, wie er dieser Verpflichtung nachgekommen ist und vollkommen ausreichend, die Frage nach Wehr- oder Ersatzdienst mit ja oder nein zu beantworten. Wegen der sonst bestehenden Diskriminierungsgefahr ist stets gemeinsam nachzufragen.

— *Finanzelle Verpflichtungen*

Erste Voraussetzung für die Zulässigkeit einer entsprechenden Frage ist, daß die Tatsache einer Überschuldung für die konkret auszuübende Tätigkeit überhaupt eine Rolle spielt.

Erforderlich für die Beurteilung, ob eine Überschuldung vorliegt, können nicht alle finanziellen Verpflichtungen eines Bewerbers sein, sondern nur solche, die das Einkommen erheblich belasten und über das übliche Maß einer Kreditaufnahme (z. B. für den Bau eines Hauses) hinausgehen. Bei der Aufnahme dieser Frage in einen Personalfragebogen ist deshalb ein strenger und eindeutiger Maßstab (z. B. überschreiten die finanziellen Verpflichtungen einen wesentlichen Prozentsatz des Einkommens?) vorzugeben.

— *Gerichtliche Straf- und Ermittlungsverfahren*

Bei Ausschreibung eines konkreten Arbeitsplatzes ist die Frage nach Vorstrafen dann und nur soweit zulässig, als sie für diesen Arbeitsplatz von Bedeutung ist (BAG AP Nr. 25 zu § 123 BGB). Die Fragestellung muß daher entsprechend konkretisiert und eingegrenzt werden.

Auch die Frage nach schwebenden Ermittlungsverfahren kann bei Vorliegen bestimmter Voraussetzungen zulässig sein. Dem Arbeitgeber/Dienstherrn kann ein Fragerecht aber nur insoweit zugestanden werden, als er ein berechtigtes, billigenswertes und schützwürdiges Interesse an der Beantwortung seiner Frage für das Arbeitsverhältnis hat. Dieses Interesse muß objektiv so stark sein, daß dahinter das Interesse des Arbeitnehmers am Schutz seines Persönlichkeitsrechtes und der Unverletzlichkeit seiner Individualsphäre zurücktritt. Die uneingeschränkte Frage nach Ermittlungsverfahren ohne Bezug zu dem zu besetzenden Arbeitsplatz ist in der Regel unzulässig.

Ausdrücklich möchte ich hier darauf hinweisen, daß ein schwebendes Verfahren nicht ohne weiteres zur Nichteinstellung des Bewerbers führen darf. In solchen Fällen muß eine weitere Sachaufklärung, z. B. im Rahmen eines Gespräches mit dem Bewerber, vorgenommen werden. Der Bewerber muß also Gelegenheit haben, auf die Hintergründe näher einzugehen und Zweifel an seiner Eignung auszuräumen.

Meine Erfahrungen zeigen allerdings, daß ein Übermaß an Datenerhebung nicht allein dadurch verhindert werden kann, daß überhaupt nur das Gesamtmaß der für die Begründung und Durchführung des Dienst- oder Arbeitsverhältnisses erforderlichen Fragen gestellt wird. Von hoher Bedeutung ist auch, in welchem Stadium des Bewerbungs- und Einstellungsverfahrens Fragen an den Bewerber gerichtet werden. Insbesondere bei Einstellungen einer Gruppe von Bewerbern, aber auch bei Einstellungsverfahren nach Ausschreibungen lassen sich im allgemeinen eine erste Phase bis zur Vorauswahl der grundsätzlich geeigneten Bewerber und eine zweite Phase, in der die endgültige Auswahlentscheidung getroffen wird, unterscheiden.

Für die Entscheidung zur Vorauswahl (erste Phase) müssen nicht alle Daten bekannt sein, die der Dienstherr/Arbeitgeber bei der endgültigen Entscheidung benötigt. Deshalb empfehle ich ein zweistufiges Bewerbungsverfahren, in dem in einer ersten Phase nur Fragen gestellt werden, die die grundsätzliche Eignung des Bewerbers erkennen lassen. Bei Bewerbern, die diese Voraussetzungen nicht erfüllen, brauchen weitere Fragen nicht gestellt zu werden. Nur die grundsätzlich geeigneten Bewerber hätten erst dann eine weitere Gruppe von Fragen zu beantworten, in der alle für die endgültige Auswahlentscheidung erforderlichen Informationen enthalten sind. Dabei kann die Notwendigkeit bestimmter Fragen in der ersten Phase durchaus von einer Laufbahn oder Funktion zur anderen unterschiedlich sein.

Im allgemeinen darf ein Bewerber mit einem Fragebogen, der in der ersten Verfahrensphase verwendet wird, z. B. nach Staatsangehörigkeit, Alter, Ableistung von Wehr-/Zivildienst (allerdings nur mit ja oder nein), Ausbildung sowie Schwerbehinderung gefragt werden. Fragen nach dem Familienstand, nach Vornamen oder Geburtsdaten von Angehörigen sowie nach dem Beruf des Ehegatten sind in dieser Phase ohne Belang. Angaben zu den Eltern sind bei volljährigen Bewerbern ebenfalls nicht erforderlich. Auch nach krankheitsbedingten Ausfallzeiten, gesundheitlichen Dauerschäden, schweren Krankheiten, Vorstrafen/laufenden Verfahren, wirtschaftlichen Verhältnissen (auch derzeitiges Gehalt oder derzeitige Besoldungsgruppe) und nach der Verfassungstreue (auch nach Orden und Ehrenzeichen, soweit sie für die Prüfung der Verfassungstreue relevant sind) darf in dieser Verfahrensstufe in der Regel nicht gefragt werden; die Frage nach einer Schwerbehinderung ist zulässig, braucht in der ersten Phase des Einstellungsverfahrens aber nicht Grad, Dauer und Art dieser Behinderung zu umfassen. Ausnahmen für einzelne dieser Fragen sind bei bestimmten Laufbahnen und Funktionen möglich.

Nach der Vorauswahl findet in der Regel in einer zweiten Phase die Auswahlentscheidung statt. Dabei wird auch geklärt, ob Einstellungshindernisse vorliegen. Verfahrenstechnisch könnte in dieser Phase der Bewerberfragebogen um die zusätzlich erforderlichen Fragen ergänzt werden. Es kann aber auch ein ergänzender Fragebogen oder ein neuer Fragebogen ausgefüllt werden. In dieser Entscheidungsphase dürfen z. B. — soweit sie nicht bereits im früheren Stadium als zulässig angesehen werden — für die Begründung und Durchführung des Dienst-/Arbeitsverhältnisses erforderliche Fragen nach dem Familienstand (verheiratet/nicht verheiratet), Anzahl und Alter von Kindern etc. gestellt werden.

Bei Kontrollen habe ich festgestellt, daß sich Einstellungsbehörden von den Bewerbern bereits zu Beginn des Auswahlverfahrens den gesamten Personalbogen (Personalfragebogen), z. T. auch den Besoldungsbogen ausfüllen lassen. Nach den o. a. Grundsätzen begegnet dies Bedenken.

Vor dem dargestellten Hintergrund werde ich mich gegenüber dem für das öffentliche Dienstrecht zuständigen Bundesminister des Innern weiterhin dafür einsetzen, seinen Personalbogen, der von vielen Dienstherren gerade auch in den neuen Bundesländern als Vorbild für die Gestaltung eigener Fragebögen verwendet wird, den beschriebenen Vorgaben anzupassen (s. auch 13. TB S. 25/26).

In den an mich gerichteten Eingaben wurden auch die von vielen Behörden im Rahmen des Einstellungsverfahrens durchgeführten Bewerber-Gruppengespräche, in deren Verlauf Bewerber ihren Lebenslauf und ihr soziales Umfeld in Anwesenheit von Mitbewerbern einer Auswahlkommission darstellen müssen, kritisiert. Ich halte dieses Verfahren für unzulässig.

Eine Bundesbehörde hat versucht, das Verfahren damit zu rechtfertigen, daß Bewerbern in dieser Gesprächsphase Befangenheit und Nervosität genommen werden solle. Dies ist aber kein Grund, Bewerber zur Preisgabe ihrer personenbezogenen Daten an die jeweiligen Mitbewerber zu veranlassen. Selbstverständlich bestehen keine Bedenken gegen ein Gruppengespräch über ein neutrales Thema.

Nach Abschluß des Einstellungsverfahrens sind Bewerbungsunterlagen einschließlich Bewerberfragebogen an abgelehnte Bewerber zurückzugeben, weil die darin enthaltenen Informationen für den Dienstherrn/Arbeitgeber nicht mehr erforderlich sind. Die Rückgabe der Unterlagen setzt allerdings voraus, daß das Bewerbungsverfahren abgeschlossen ist, was u. a. bedeutet, daß die Personalvertretung im Rahmen ihrer Beteiligung bei Einstellungen auch über abgelehnte Bewerber unterrichtet wurde. In Zusammenhang mit einer Eingabe, in der ein abgelehnter Bewerber die Herausgabe des ausgefüllten Personalbogens verlangte, konnte ich auch das Auswärtige Amt von dieser Rechtsauffassung überzeugen.

9.7 Angefochtene Beurteilungen dürfen in Personalakten nur mit Vorbehalt gespeichert werden.

Ein Beamter des Bundeskriminalamtes hat sich dagegen gewandt, daß die letzte Beurteilungsnote in seiner Personalakte gespeichert wurde, obwohl er gegen die Beurteilung Widerspruch eingelegt hatte. Er befürchtete hierdurch Nachteile.

Zur Lösung des Anliegens kann nunmehr das Bundesbeamtengesetz in der Fassung des 9. Dienstsrechtsänderungsgesetzes (s. o. 9.2) herangezogen werden. Danach sind Unterlagen über Beschwerden, Behauptungen und Bewertungen, auf die die Tilgungsvorschriften des Disziplinarrechts keine Anwendungen finden, mit Zustimmung des Beamten unverzüglich aus der Personalakte zu entfernen und zu vernichten, falls sie sich als unbegründet oder falsch erwiesen haben (§ 90e Abs. 1 Nr. 1 BBG).

§ 90e Abs. 1 Nr. 1 BBG ist nach seinem klaren Wortlaut auch auf dienstliche Beurteilungen anzuwenden. Dies wird zwar bestritten, aber die unmittelbare Anbindung des Halbsatzes „dies gilt nicht für dienstliche Beurteilungen" an § 90e Abs. 1 *Nr. 2* BBG zeigt, daß sich diese Ausnahmeregelung nur auf die Nummer 2 bezieht. Auch eine am Zweck der Vorschrift orientierte Auslegung bringt kein anderes Ergebnis, da kein Grund dafür ersichtlich ist, daß Beurteilungsnoten in Personalakten verbleiben sollten, wenn sie sich als unbegründet oder falsch *erwiesen* haben.

In dem der Eingabe zugrunde liegenden Fall hat mir das Bundeskriminalamt zugesichert, die angefochtene Beurteilung bis zur endgültigen Entscheidung in der Personalakte als streitbefangen zu kennzeichnen und diese Tatsache bei Personalmaßnahmen gebührend zu berücksichtigen. Damit konnte ein Ergebnis erzielt werden, das in der Sache eine Sperrung der angefochtenen Beurteilung, nämlich deren Kennzeichnung mit dem Ziel, ihre Verwendung einzuschränken, darstellt (§ 12 Abs. 4 in Verbindung mit § 35 Abs. 4 und § 3 Abs. 5 Nr. 4 BDSG).

9.8 Personalnebenakten viel zu umfangreich

Bei der Kontrolle eines Hauptzollamtes hatte ich Gelegenheit, einen Teilbereich der Praxis bei der Führung von Personalakten, nämlich der sogenannten Personalnebenakten, in der Zollverwaltung kennenzulernen.

Das kontrollierte Hauptzollamt führte nämlich nur Personalnebenakten. Die eigentlichen Personalakten wurden bei der zuständigen Oberfinanzdirektion (OFD) geführt. Ein Vergleich einzelner Personalnebenakten mit der Personalhauptakte ergab, daß die Nebenakten mit nur geringen Einschränkungen Duplikate der Hauptakte waren. Dies ist unzulässig.

§ 90 Abs. 2 Satz 3 BBG i. d. F. des Neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften vom 11. Juni 1992 enthält Regelungen über die Führung von Nebenakten. Nach dieser Vorschrift dürfen Nebenakten, das sind Unterlagen, die sich auch in der Grundakte oder in Teilakten befinden, nur solche Informationen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerfüllung der betreffenden Behörde erforderlich ist.

Die Nebenakten bei dem kontrollierten Hauptzollamt hätten daher nur Unterlagen enthalten dürfen, die für dessen Aufgabenerfüllung erforderlich waren, wie z. B. Aufzeichnungen über Zuweisung und Dienstantritt, Fehlzeiten, Funktionsübertragungen, Beförderungen und ähnliches. Die vorgefundenen Unterlagen in den Nebenakten überschritten bei weitem dieses Maß. Nicht in die Personalnebenakten gehörende Unterlagen sind z. B. die Erklärung über die Treuepflicht, die Darstellung des dienstlichen Werdeganges des Beamten in der Finanzverwaltung, die Mitteilung über die vorläufig festgesetzte Vergütungsgruppe, das Beiheft „Beurteilungen" und die Berechnung zur Festsetzung des Besoldungsdienstalters.

Die festgestellte Dimensionierung der Personalnebenakten stellt nicht nur einen formalen Verstoß dar. Sie verletzt auch den Grundsatz, daß der Kreis der mit den Personalakten befaßten Beamten möglichst eng zu halten ist (BVerwG in NJW 1987 S. 1214; BAG in NZA 1988 S. 53 ff.).

Ich habe das Bundesministerium der Finanzen aufgefordert, darauf hinzuwirken, daß Personalnebenakten in seinem Geschäftsbereich so geführt werden, wie § 90 Abs. 2 Satz 3 BBG dies verlangt. Das Bundesministerium der Finanzen hat mir dies zwischenzeitlich zugesagt. Ich werde die Einhaltung dieser Zusage überwachen.

9.9 Anonyme Hinweise an den Dienstherrn

Eine Bundesbahndirektion erhielt mehrere anonyme Hinweise, daß ein Beamter einer Nebentätigkeit bei einer Gebäudereinigung nachgehe und dort auch in einer Zeit gearbeitet habe, während der er gegenüber der Deutschen Bundesbahn Dienstunfähigkeit angegeben hatte. Ohne zunächst den Beamten über das Vorbringen zu informieren und ihn dazu zu befragen, wandte sich die Deutsche Bundesbahn unmittelbar an das Reinigungsunternehmen. Eine telefonische Rückfrage dort ergab, daß der Beamte seit mehreren Jahren eine Nebentätigkeit ausübte, ohne daß ihm die dafür nach § 65 BBG erforderliche Genehmigung erteilt worden war. Daraufhin wurde das Reinigungsunternehmen von der DB um Mitteilung von Einzelheiten ersucht. Dabei wurde insbesondere — ohne Nennung des Grundes — auf die Zeiträume abgehoben, in denen sich der Beamte in der fraglichen Zeit bei der Deutschen Bundesbahn krank gemeldet hatte.

Nach dem in § 13 Abs. 2 Satz 1 BDSG normierten Ersterhebungsgrundsatz sind im Regelfall personenbezogene Daten beim Betroffenen selbst zu erheben.

Vorliegend halte ich jedoch eine Abweichung von dem Ersterhebungsgrundsatz aufgrund der Vorschriften des § 13 Abs. 2 Satz 2 Nr. 1 BDSG i. V. m. § 26 Abs. 1 und 2 der Bundesdisziplinarordnung (BDO) für gerechtfertigt.

§ 26 Abs. 2 BDO schreibt vor, daß dem Beamten im Rahmen eines Vorermittlungsverfahrens Gelegenheit zu geben ist, sich zu äußern, sobald es ohne Gefährdung des Ermittlungszweckes möglich ist. Dabei liegen Art und Umfang der Vorermittlungen im pflichtgemäßen Ermessen des Dienstvorgesetzten. Welche Ermittlungshandlungen im einzelnen und in welcher Reihenfolge durchgeführt werden, richtet sich nach der Lage des jeweiligen Einzelfalles.

Dabei ist zu berücksichtigen, daß das dem Beamten im Disziplinarverfahren zustehende Recht auf Gewährung rechtlichen Gehörs nicht nur Ausdruck von Rechtsstaatlichkeit, sondern auch der Fürsorgepflicht des Dienstherrn (§ 79 BBG) ist. Zur Fürsorgepflicht des Dienstherrn gehört es auch, darüber zu wachen, daß dem Beamten das rechtliche Gehör ordnungsgemäß, insbesondere rechtzeitig, gewährt wird. Gerade bei anonymen Anzeigen muß sich der Dienstvorgesetzte bei weiteren Ermittlungen zunächst Zurückhaltung auferlegen, um seiner Fürsorgepflicht zu genügen und den Beamten vor unberechtigten Angriffen zu schützen. Das darf allerdings die gebotene Sachaufklärung nicht verhindern. Der Ermittlungsführer muß deshalb abwägen, ob und wann der Beamte im Vorermittlungsverfahren zu beteiligen ist.

In dem der Eingabe zugrunde liegenden Fall habe ich mich der Auffassung der Deutschen Bundesbahn angeschlossen, eine vorherige Anhörung des Beamten hätte die Aufklärung des Sachverhaltes wahrscheinlich verhindert oder zumindest wesentlich erschwert. Dabei fiel besonders ins Gewicht, daß der Betroffene besonders enge Beziehungen zu Personen im Bereich des Reinigungsunternehmens unterhielt.

9.10 Vorsicht bei der Durchführung von Verfahren zur Personalauswahl und Personalförderung, besonders wenn Privatfirmen mitwirken

Der Personalrat beim Zentralamt für Mobilfunk — Telekom — hat mir vorgetragen, wegen der Neuorganisation des Mobilfunks sei geplant, bei der Durchführung von Assessment-Center-Verfahren zur Auswahl von künftigen Fach- und Führungskräften, Privatfirmen zu beteiligen. Zur Vorbereitung solcher Verfah-

ren sollten von den in die Verfahren einbezogenen Mitarbeitern Daten erhoben werden. In einem dazu bestimmten „Fragebogen zu persönlichen Daten/ Ausbildungsweg, beruflichem Werdegang" sollte u. a. nach dem Ausbildungsweg (auch Prüfungsergebnisse), dem beruflichen Werdegang (auch Motive für einen etwaigen Firmenwechsel), nach weiteren Tätigkeitsschwerpunkten im Bereich der Telekom, nach besonderen beruflichen Leistungen, außerberuflichen Aktivitäten und persönlichen Interessen gefragt werden.

Gegen die Durchführung solcher Assessment-Center-Verfahren habe ich aus datenschutzrechtlicher Sicht grundsätzlich keine Bedenken.

Zum Schutz des Persönlichkeitsrechts der an einem solchen Verfahren beteiligten Mitarbeiter sind jedoch die Grundsätze über den Schutz von Personaldaten zu beachten. So ist das im § 90 Abs. 4 Satz 1 BBG verankerte und in der Rechtsprechung der Arbeitsgerichte anerkannte Prinzip zu beachten, daß personenbezogene Daten über Beamte und andere Mitarbeiter nur erhoben werden dürfen, soweit dies zur Durchführung des Dienstverhältnisses erforderlich ist. Personenbezogene Daten der am Verfahren beteiligten Mitarbeiter dürfen deshalb nur insoweit erhoben werden, als sie für die Vorbereitung, Durchführung und Nachbereitung der Assessment-Verfahren wirklich erforderlich sind. Hierbei ist ein strenger Maßstab anzulegen. Dies gilt auch deswegen, weil zur Erzielung einer objektiven und vorurteilsfreien Bewertung der Teilnehmer an dem Assessment-Center-Verfahren möglichst wenig personenbezogene Daten aus der bisherigen Tätigkeit des Mitarbeiters in das Verfahren eingeführt werden sollten. Zu viele Daten aus dem Vorfeld des Verfahrens wären für das Ergebnis geradezu kontraproduktiv.

Mit dem mir zugeleiteten Fragebogen sollten, wie eingangs dargestellt, weit mehr Daten erhoben werden als für die Vorbereitung, Durchführung und Nachbereitung der Assessment-Center erforderlich sind.

Auch die Tatsache, daß mittels des Fragebogens die Daten beim Betroffenen selbst erhoben werden, vermag die Erhebung über das Maß des für die Durchführung des Dienst- oder Arbeitsverhältnisses Erforderlichen hinaus nicht zu rechtfertigen. Von einer wirksamen Einwilligung in die Datenerhebung kann nämlich nicht ausgegangen werden, denn für die Betroffenen besteht tatsächlich ein faktischer Zwang zur Offenbarung dieser Daten an den Arbeitgeber, da sie im Falle der Verweigerung nicht zum Assessment-Center-Verfahren zugelassen werden und damit Nachteile für ihr weiteres berufliches Fortkommen befürchten müssen.

Die Datenerhebung muß bei Assessment-Center-Verfahren auch deshalb auf das wirklich Erforderliche begrenzt werden, weil die Daten an die mit der Durchführung des Verfahrens beauftragte Privatfirma übermittelt werden sollen. Für Beamte gilt § 90d Abs. 2 Satz 1 BBG. Für die Übermittlung ist also die Einwilligung des Beamten erforderlich. Für Angestellte und Arbeiter gilt nichts anderes. Eine solche Einwilligung darf von Mitarbeitern nur im Rahmen des für das Assessment-Center-Verfahren wirklich Erforderlichen verlangt werden.

Soweit eine Datenübermittlung an die Privatfirma zulässig ist, muß durch vertragliche Vereinbarung sichergestellt sein, daß der Empfänger diese nach den Grundsätzen über den Umgang mit Personaldaten verarbeitet und nutzt. Insbesondere muß gewährleistet sein, daß die Privatfirma die Daten nur für den Zweck nutzt, zu dem sie ihr überlassen worden sind, und die Daten unverzüglich löscht, wenn das Assessment-Center-Verfahren — einschließlich Nachbereitung — abgeschlossen ist.

Ich habe meine vorstehend dargestellte Auffassung dem Hauptpersonalrat bei der Generaldirektion der Telekom mitgeteilt. Daraufhin wurde kurzfristig eine „Dienstvereinbarung zur Durchführung der Auswahl von Führungskräften im Bereich Mobilkommunikation" zwischen dem Vorstand der Telekom und dem Hauptpersonalrat, die den Datenschutz bei den betroffenen Mitarbeitern sicherstellen soll, abgeschlossen. Ich behalte mir vor, mich ggf. direkt an die Telekom zu wenden, um eine datenschutzgerechte Durchführung des geplanten Verfahrens sicherzustellen.

9.11 Was darf dem Konkurrenten um eine Stelle im öffentlichen Dienst im gerichtlichen Verfahren über andere Bedienstete mitgeteilt werden?

Aufgrund der Eingabe eines Personalrates hatte ich mich mit datenschutzrechtlichen Problemen der Konkurrentenklage im öffentlichen Dienst zu beschäftigen. Typischerweise wendet sich ein Beamter mit einer solchen Klage dagegen, daß nicht er, sondern ein anderer Mitarbeiter des Dienstherrn befördert wird oder eine bestimmte Stelle erhält.

Von datenschutzrechtlicher Relevanz sind hierbei die Fragen, welche Daten des zum Zuge gekommenen Konkurrenten der Dienstherr dem Verwaltungsgericht und welche Daten dieses gegenüber dem Kläger und etwaigen sonstigen Beteiligten offenbaren darf.

Nach § 99 Abs. 1 Satz 1 der Verwaltungsgerichtsordnung (VwGO) sind Behörden zu Auskünften gegenüber dem Gericht verpflichtet. Die oberste Aufsichtsbehörde kann allerdings eine Auskunft u. a. dann verweigern, wenn ein Vorgang nach einem Gesetz oder seinem Wesen nach geheimgehalten werden muß (§ 99 Abs. 1 S. 2 VwGO). Zwar unterliegen die in Personalunterlagen enthaltenen personenbezogenen Daten einer besonderen Geheimhaltung. Das macht aber Auskünfte über personenbezogene Daten, die aus Personalakten stammen, nicht unzulässig, soweit sie für eine sachgerechte Entscheidung, z. B. über eine Konkurrentenklage, erforderlich sind. Allerdings ist eine Durchbrechung des Personalaktengeheimnisses auch gegenüber einem Verwaltungsgericht nur nach entsprechender Abwägung in jedem Einzelfall unter Anlegung strenger Maßstäbe erlaubt. Die Behörde hat dabei die Interessen der Wahrheitsfin-

dung und das Interesse des Rechtssuchenden an der Auskunft, insbesondere auch die Schwere der in Frage stehenden Rechtsgutverletzung, gegen das Interesse an der Geheimhaltung abzuwägen.

Nach geltendem Recht kann ein Ausgleich dieser widerstrebenden Interessen wohl nur erreicht werden, wenn das Gericht unter Berücksichtigung datenschutzrechtlicher Gesichtspunkte prüft, welche Unterlagen es konkret aus der jeweiligen Personalakte benötigt, und nicht generell die gesamte Akte anfordert. Soweit erforderlich, sollte die beteiligte Behörde das Gericht auf diese Möglichkeit hinweisen. Besteht dieses aber auf der Übersendung der vollständigen Personalakte, wird die Behörde sich dem in aller Regel nicht entziehen können.

Eine Verwendung der notwendigen Daten aus Personalunterlagen durch ein Gericht im Rahmen einer Konkurrentenklage hält sich auch im Rahmen der Zweckbindung des § 90 Abs. 3 des Bundesbeamtengesetzes (BBG). Wenn es zulässig ist, der die Dienstaufsicht führenden Behörde Auskünfte aus Personalakten zu erteilen (§ 90d Abs. 1 BBG), können auch Auskünfte an ein über eine Konkurrentenklage entscheidendes Gericht grundsätzlich nicht unzulässig sein.

Sofern der Dienstherr dem Verwaltungsgericht personenbezogene Daten des berücksichtigten Bewerbers berechtigt offenbart hat, ist auch die Bekanntgabe dieser Daten durch das Gericht an die Beteiligten im erforderlichen Umfang zulässig. Nach § 100 VwGO können die Beteiligten die dem Gericht vorgelegten Unterlagen einsehen. Es ist aber nicht auszuschließen, daß solche Unterlagen personenbezogene Daten enthalten, deren Offenbarung nicht zwingend erforderlich oder aus datenschutzrechtlicher Sicht nicht vertretbar ist.

Nach § 99 Abs. 1 Satz 2 VwGO, der im Rahmen des § 100 VwGO analog angewendet wird, sind Vorgänge geheimzuhalten, deren Geheimhaltung durch besondere gesetzliche Bestimmungen vorgeschrieben ist oder die ihrem Wesen nach geheim sind. Es ist aber andererseits auch das Recht des Prozeßgegners aus Artikel 19 Abs. 4 GG zu beachten, wonach jedermann der Rechtsweg offensteht, wenn er durch die öffentliche Gewalt in seinen Rechten verletzt wird. Gegen diese Garantie eines lückenlosen und effektiven Rechtsschutzes würde es verstoßen, wenn eine — zulässige — Klage nicht begründet werden könnte, weil personenbezogene Daten von Konkurrenten nicht in den Prozeß eingebracht werden dürfen.

Zum Schutz des informationellen Selbstbestimmungsrechtes halte ich eine normenklare Regelung in der Verwaltungsgerichtsordnung — wie ich sie bereits in meinem 12. TB S. 28 forderte — für dringend nötig. Sie sollte näher festlegen, welche Unterlagen dem Verwaltungsgericht aus der Personalakte vorzulegen sind und damit den Prozeßbeteiligten zur Kenntnis gelangen. Dabei müßten das Erforderlichkeitsprinzip und gegebenenfalls entgegenstehende überwiegende schutzwürdige Interessen des zum Zuge gekommenen Konkurrenten berücksichtigt werden.

9.12 Disziplinarunterlagen Unbefugten zugänglich gemacht

Ein Bundesbeamter des Postdienstes beschwerte sich über fehlende Vertraulichkeit bei Vorermittlungen nach § 26 Bundesdisziplinarordnung (BDO). Tatsächlich hatte ein Stellenvorsteher des Postamts (hierbei handelte es sich um einen Fachvorgesetzen) das Ergebnis der disziplinarrechtlichen Vorermittlungen erfahren, weil es ihm in offener Form zur Aushändigung an den Betroffenen zugeleitet worden war. Zwei Fachabteilungsleiter des Postamtes erhielten ebenfalls Kenntnis vom Inhalt der Vorermittlungsakte. Außerdem war die gesamte Vorermittlungsakte anläßlich eines Gutachtenantrags dem betriebsärztlichen Dienst übersandt worden.

Personenbezogene Daten in Disziplinarakten unterliegen dem verstärkten Schutz des Personalaktengeheimnisses. Zugang zu ihnen dürfen nur der zuständige Dienstvorgesetzte und Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung des Disziplinarverfahrens beauftragt sind, und nur soweit dies für diesen Zweck erforderlich ist (§ 90 Abs. 3 Bundesbeamtengesetz).

Die Offenlegung des Ergebnisses der Vorermittlungsakten gegenüber dem Stellenvorsteher war nicht zulässig, da dieser nicht Dienstvorgesetzter im Sinne der beamtenrechtlichen Vorschriften und auch im übrigen für die Bearbeitung des Disziplinarverfahrens nicht zuständig war.

Von einer Beanstandung habe ich in diesem Falle abgesehen, da der Postdienst sichergestellt hat, daß die wesentlichen Ergebnisse von Vorermittlungen (§ 26 Abs. 4 BDO) nur noch im verschlossenen Umschlag übergeben werden und damit in solchen Fällen von dem aushändigenden Bediensteten nicht mehr zur Kenntnis genommen werden können.

Die Offenlegung des Inhalts der Vorermittlungsakte gegenüber den Fachabteilungsleitern des Postamtes wurde von der Generaldirektion der Deutschen Bundespost Postdienst nicht in Abrede gestellt. Sie wurde damit begründet, daß die erwähnten Abteilungsleiter in Vertretung des Amtsvorstehers als amtierende Dienstvorgesetzte mit dem Verfahren befaßt waren; im übrigen hätten beide Abteilungsleiter an der Entscheidung beteiligt werden müssen, den Beamten auf einen seiner Besoldungsgruppe entsprechenden Dienstposten einzusetzen. Hierzu seien mit den Abteilungsleitern auch die das Vorermittlungsverfahren auslösenden Vorfälle zu erörtern gewesen.

Die Durchsicht der Vorermittlungsakte ergab, daß lediglich in einem Falle ein Abteilungsleiter in Vertretung des Amtsvorstehers mit dem Vorgang befaßt war, als er den Gutachtenantrag an den postbetriebsärztlichen Dienst unterschrieben hat. Dies ist nicht zu beanstanden, obgleich sich hierbei die Frage stellt, ob nicht im Interesse der besonderen Vertraulichkeit dieses Vorganges eine Verschiebung der Entscheidung bis zur Rückkehr des Amtsvorstehers vertretbar gewesen wäre.

Die Kenntnisnahme des anderen Fachabteilungsleiters von den Disziplinarunterlagen war nicht gerechtfertigt. Personalrechtliche Entscheidungen im Disziplinarverfahren trifft der Dienstvorgesetzte. Ich habe deshalb die Offenlegung gemäß § 25 Abs. 1 BDSG als Verstoß gegen das Personalaktengeheimnis beanstandet.

Ich stehe z. Z. noch mit der DBP-Postdienst in Verbindung, da sie — entgegen meiner Auffassung — der Ansicht ist, auch die jeweils zuständigen Fachabteilungsleiter dürften von Disziplinarunterlagen Kenntnis nehmen.

Die Übermittlung der gesamten Vorermittlungsakte an den postbetriebsärztlichen Dienst war für den Untersuchungsauftrag, ob der Bedienstete „aus medizinischer Sicht für die ihm zur Last gelegten Verfehlungen voll verantwortlich gemacht werden kann" nicht erforderlich. Zwar läßt das Bundesbeamtengesetz die Vorlage der Personalakte an Ärzte, die im Auftrag der personalverwaltenden Behörde ein medizinisches Gutachten erstellen, ohne Einwilligung des Betroffenen *jetzt* ausdrücklich zu (§ 90d Abs. 1 Satz 3 BBG), aber auch dabei ist in jedem Einzelfall der Erforderlichkeitsgrundsatz (§ 90d Abs. 3 BBG) zu beachten.

Auf meine Beanstandung nach § 25 Abs. 1 BDSG wegen des Verstoßes gegen das Personalaktengeheimnis hin räumte die Generaldirektion — Postdienst — ein, daß es keine Notwendigkeit gibt, dem ärztlichen Dienst regelmäßig die Personalakten und alle Disziplinarunterlagen zu übersenden. Sollte es aus postbetriebsärztlicher Sicht für notwendig gehalten werden, weitere Unterlagen einzusehen, so könnten diese nachgefordert werden. Eine entsprechende Verfügung der Generaldirektion — Postdienst — ist zwischenzeitlich ergangen.

9.13 Defizite beim Sozialdienst einer obersten Bundesbehörde

Eine Petentin beschwerte sich darüber, daß vom Sozialdienst einer obersten Bundesbehörde nicht nur Daten über sie erhoben und gespeichert wurden, sondern daß ihr auch die Einsicht in diese Unterlagen verwehrt wurde. Sie empfand das Tätigwerden des Sozialdienstes nicht als Fürsorge, sondern als Einmischung in ihre Angelegenheiten. Der Sozialdienst hatte u. a. auch Informationen (z. B. über Fehlzeiten) bei Mitarbeitern und Vorgesetzten über sie erhoben.

Ich konnte zunächst erreichen, daß die zuständige Behörde der Petentin die begehrte Einsicht in die sie betreffenden Unterlagen gewährte. Auf ihren Wunsch war dabei einer meiner Mitarbeiter anwesend.

Ich habe den Fall zum Anlaß genommen, die Stellung des Sozialdienstes innerhalb dieser obersten Bundesbehörde und deren Umgang mit personenbezogenen Daten zu überprüfen. Als zentrale Frage ergab sich: Darf der Sozialdienst Daten ohne die Zustimmung eines Betroffenen erheben und speichern und in welchem Umfange darf er diese Daten offenbaren? Problematisch ist dies insbesondere, weil der Sozialdienst nach der für ihn geltenden Dienstanweisung sowohl (gegenüber den Betroffenen) beratende als auch (gegenüber der Dienststelle) begutachtende Funktion hat. Mitarbeiter des Sozialdienstes können Ärzte, Psychologen und Sozialarbeiter sein, die das Berufsgeheimnis nach § 203 Abs. 1 Nr. 1, 2 und 5 StGB zu wahren haben.

Soweit der Sozialdienst beratend tätig wird, ist seine Inanspruchnahme durch die Bediensteten völlig freiwillig. Diese müssen uneingeschränkt davon ausgehen können, daß das Besprochene zwischen ihnen und ihrem Gegenüber „Privatsache" bleibt. Hiervon kann nur dann abgewichen werden, wenn ein Bediensteter die Ärzte, Psychologen und Sozialarbeiter ausdrücklich von ihrer Schweigepflicht entbunden hat. Die Entbindung oder auch Nicht-Entbindung von der Schweigepflicht sollte schriftlich dokumentiert werden.

Der Grundsatz der Freiwilligkeit für die Inanspruchnahme der beratenden Tätigkeit hat auch zur Folge, daß Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten des Betroffenen nur für den Zweck der Beratung erfolgen dürfen. Deshalb ist es nicht zulässig, daß der Sozialdienst im Rahmen einer beratenden Tätigkeit Nachfragen über den Betroffenen bei anderen Mitarbeitern der Behörde oder sonstigen Dritten ohne dessen Einwilligung vornimmt. Eine Speicherung so erhobener Daten in den Akten des Sozialdienstes ist nach § 12 Abs. 4 i. V. mit § 28 Abs. 1 Nr. 1 BDSG nicht zulässig. Die Rechtsfolge einer solchen unzulässigen Speicherung personenbezogener Daten in Akten ist nach § 35 Abs. 3 BDSG deren Sperrung.

Die Mitarbeiter des Sozialdienstes werden auch begutachtend tätig, wenn die personalführenden Referate an die Beratungs- und Betreuungsstelle mit der Bitte herantreten, eine psychosoziale Beurteilung eines Bediensteten vorzunehmen. In diesen Fällen werden deren Mitarbeiter im „offiziellen Auftrag" tätig.

Soweit eine begutachtende Tätigkeit des Sozialdienstes in Betracht kommt, ist von wesentlicher Bedeutung, daß der Betroffene schon auf Grund der Offenheit und des Vertrauens, die für das öffentliche Dienstverhältnis gelten, unterrichtet werden muß, wenn ein solches Gutachten über ihn angefordert wird. Die Fragen an die Gutachter müssen konkret auf das (z. B. für die Personalwirtschaft) wesentliche Ziel formuliert sein. Das Gutachten muß sich auf die Beantwortung der gestellten Fragen beschränken, darf insbesondere keine Angaben über die Art einer Erkrankung enthalten.

Die Trennung in beratende und begutachtende Tätigkeit kann in den Fällen problematisch sein, in denen der Betroffene, über den eine Begutachtung erbeten wurde, sich bereits zu einem früheren Zeitpunkt oder parallel mit der Bitte um Beratung an den Sozialdienst gewandt hat. Hier muß Prinzip sein, daß die Informationen aus Beratungen des Betroffenen für eine begutachtende Tätigkeit nur verwendet werden, wenn der Betroffene einer Entbindung von der Schweigepflicht für diesen Zweck zugestimmt hat. Wird diese nicht

gewährt, muß die Beurteilung durch einen Dritten erfolgen.

In dem meiner Kontrolle zugrunde liegenden Fall entsprachen Dienstanweisungen und Praxis nicht den nach den obigen Grundsätzen zu stellenden datenschutzrechtlichen Anforderungen. Ich stehe mit der betroffenen obersten Bundesbehörde in Kontakt, um eine Abstellung der Defizite zu erreichen.

9.14 Umgang mit ärztlichen Unterlagen

Bundesbedienstete und Bewerber für den öffentlichen Dienst des Bundes werden häufig ärztlich untersucht. Die dabei anfallenden Daten sind besonders sensibel und unterliegen dem Patientengeheimnis. Immer wieder besteht Anlaß, den Umgang mit solchen Daten zu überprüfen.

9.14.1 Im wesentlichen korrekte Handhabung bei der Physikalisch-Technischen Bundesanstalt

Bei der Physikalisch-Technischen Bundesanstalt in Braunschweig (PTB) habe ich auch deren Betriebsärztlichen Dienst kontrolliert. In der PTB wurden im Jahre 1978 die nach dem Arbeitssicherungsgesetz vertraglich wahrzunehmenden Aufgaben dem Berufsgenossenschaftlichen Arbeitsmedizinischen Dienst e. V. (BAD) übertragen. Ein Arzt des BAD führt in den Räumen des Betriebsärztlichen Dienstes der PTB regelmäßig arbeitsmedizinische Vorsorgeuntersuchungen durch.

Im Jahre 1991 hat sich der BAD gegenüber der PTB auch zur Durchführung von Einstellungsuntersuchungen verpflichtet.

Die Durchführung der Untersuchungen und das sich anschließende Verfahren sind datenschutzrechtlich unbedenklich. Die Verbindung der arbeitsmedizinischen Vorsorgeuntersuchung mit der Einstellungsuntersuchung durch denselben Arzt hat sogar den Vorteil, wiederholte Datenerhebungen in einem besonders sensiblen Bereich zu vermeiden.

Über das Ergebnis der medizinischen Untersuchung wird jeder Proband schriftlich mittels Formblatt informiert. Dieses sieht zehn Untersuchungsbefunde vor sowie Leerzeilen für die Angabe von Befunden, die „außerhalb des Normbereichs" liegen. Diese Befunde werden dem Betroffenen in einem verschlossenen Fensterumschlag per Hauspost zugestellt.

Um besser gewährleisten zu können, daß diese Mitteilungen nur dem Betroffenen zugestellt werden, habe ich der PTB empfohlen, bei der Versendung der Befundmitteilung per Hauspost künftig den Umschlag mit dem Stempel des Betriebsärztlichen Dienstes zu versehen und deutlich sichtbar mit dem Vermerk „persönlich" zu kennzeichnen. Die PTB ist meiner Empfehlung gefolgt.

9.14.2 Ärztliche Begutachtung ohne Wissen des Bediensteten

Ein früherer Verwaltungsangestellter eines Arbeitsamtes beklagte sich, er sei anhand von Beschwerdebriefen, die er seinem ehemaligen Arbeitgeber geschrieben habe, ohne sein Wissen ärztlich begutachtet worden.

a) Eine unangekündigte Datenschutzkontrolle im Arbeitsamt bestätigte den Sachverhalt. Ablichtungen von Beschwerdebriefen des Petenten an dessen seinerzeitigen Vorgesetzten im Arbeitsamt waren über die Verwaltungsabteilung des Arbeitsamtes an den Ärztlichen Dienst gelangt. Allein auf der Grundlage dieser Briefe erstellten der Ärztliche Dienst und ein Außengutachter der Bundesanstalt für Arbeit (BA) Gutachten. Diese wurden auf Dauer zu den zum Betroffenen geführten Unterlagen des Ärztlichen Dienstes genommen. Der Betroffene erfuhr von alledem nichts, insbesondere auch nicht das Ergebnis der Gutachten. Ich habe diese Verfahrensweise als Verstoß gegen den Grundsatz offener Datenerhebung und -verarbeitung im öffentlichen Dienstverhältnis und gegen den Manteltarifvertrag für die Angestellten der BA beanstandet (s. auch 11.5.1).

b) Die Kontrolle ergab weiterhin, daß die vorgenannten Arztgutachten anschließend ohne Wissen des Petenten in dessen Personalhauptakte aufgenommen worden waren, obwohl sie Behauptungen enthielten, die für ihn ungünstig waren. Dies habe ich als Verstoß gegen den Mantelfarifvertrag für die Angestellten der BA förmlich beanstandet.

c) Nachdem das Arbeitsverhältnis zwischen der BA und dem Petenten beendet worden war, hatte der Betroffene Leistungen nach dem Arbeitsförderungsgesetz bezogen. Damit unterfielen die im Rahmen dieses Verfahrens angefallenden Daten dem Sozialgeheimnis. Gleichwohl hat das Arbeitsamt in einer Presseveröffentlichung u. a. Zitate aus einem über den Petenten erstellten ärztlichen Gutachten bekannt gegeben. Ziel der Presseinformation soll gewesen sein, unwahre Tatsachenbehauptungen in vorangegangenen Presseartikeln richtigzustellen.

   Die BA hat eingeräumt, daß die für eine Offenbarung von Sozialdaten zu diesem Zweck erforderliche Genehmigung durch das Bundesministerium für Arbeit und Sozialordnung nicht vorgelegen hat (§ 69 Abs. 1 Nr. 3 SGB X). Für das entsprechende Genehmigungsverfahren hätte nach den Weisungen der BA der Gesamtvorgang der Hauptstelle Nürnberg zur Einholung der Genehmigung des Bundesministeriums für Arbeit und Sozialordnung vorgelegt werden müssen. Die öffentliche Weitergabe von Teilen der über den Petenten erstellten ärztlichen Gutachten verstieß damit gegen das Sozialgeheimnis gemäß § 35 Abs. 1 SGB I i.V.m. §§ 67, 69 Abs. 1 SGB X. Auch dies habe ich förmlich beanstandet.

Die BA hat meine unter a) bis c) aufgeführten Beanstandungen anerkannt und Abhilfe zugesagt. Sie wird in ihren Personalakten-Richtlinien festlegen, daß ärzt-

liche Gutachten, auch solche „nach Aktenlage", nur mit Wissen des Betroffenen erstellt werden dürfen. Begutachtungsaufträge müssen in Zukunft den Zweck so genau beschreiben, daß der Arzt nur das entsprechende Ergebnis mitteilen muß, nicht aber einzelne Befunde. Der Zweck muß sich unmittelbar auf die Entscheidung oder Maßnahme beziehen, die nach den gesetzlichen oder tariflichen Vorschriften zu treffen ist (z. B. Feststellung der Dienstfähigkeit/Arbeitsfähigkeit). Begutachtungsauftrag und Unterrichtung des Betroffenen sind aktenkundig zu machen.

Unterlagen, die im Zusammenhang mit der Einschaltung des Ärztlichen Dienstes bei Dienstverhältnissen anfallen, werden in Zukunft als Personalakten im materiell-rechtlichen Sinne behandelt; damit sind für die Rechte des Betroffenen auf Einsichtnahme, Anhörung usw. auch der MTA und die Personalakten-Richtlinien anzuwenden.

Ein Arbeitsamtsarzt, der von der BA als Arbeitgeber/Dienstherr mit der Erhebung und Übermittlung personenbezogener Daten beauftragt wird, darf diese Daten nur übermitteln, wenn ein Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Die Verantwortung hierfür liegt beim Arbeitsamtsarzt. Die Personalverwaltung weist den Betroffenen auf dienst- oder arbeitsrechtliche Folgen einer Verweigerung der Einwilligung hin.

9.14.3 Anforderung ärztlicher Unterlagen über einen Beamten nur mit dessen Kenntnis

Bei einem Vollzugsbeamten des Bundesgrenzschutzes war unklar, ob er nach einem Unfall noch dienstfähig war. Dies veranlaßte den Dienstherrn

— von einem Krankenhaus und einer Rehabilitationsklinik Befundunterlagen anzufordern, ohne den Betroffenen vorher davon zu informieren und

— von dem Beamten zu fordern, sich von einem Bundesgrenzschutzarzt auf seine Dienstfähigkeit untersuchen zu lassen.

Das Beamtenverhältnis fordert Offenheit und gegenseitiges Vertrauen zwischen dem Beamten und seinem Dienstherrn. Dieser Grundsatz hat auch Auswirkungen auf die Erhebung von Daten, insbesondere von sensiblen Daten, durch den Dienstherrn. Er verbietet es, Daten, die dem Patientengeheimnis unterliegen, hinter dem Rücken des Beamten anzufordern. Dies gilt besonders dann, wenn — wie in dem Fall der Eingabe — dem Dienstherrn bekannt sein muß, daß das Krankenhaus und die Reha-Klinik die erbetenen Unterlagen ohne Einwilligung des Beamten nicht offenbaren dürfen. Deshalb hätte der Dienstherr den Beamten davon unterrichten müssen, daß er zur Prüfung seiner Dienstfähigkeit die genannten Unterlagen anfordern wolle und gleichzeitig den Beamten auffordern müssen, die betroffenen Ärzte von ihrer Schweigepflicht zu entbinden.

An dieser Beurteilung ändert sich auch nichts dadurch, daß der Beamte verpflichtet ist, an der Feststellung seiner Dienstfähigkeit mitzuwirken. Eine solche Mitwirkungspflicht war hier nach § 42 Abs. 1 BBG im Hinblick auf die Dienstunfähigkeit und nach § 55 BBG im Hinblick auf eine notwendige Prüfung künftiger Verwendungsmöglichkeiten anzunehmen.

Die Mitwirkung ist eine Obliegenheit des Beamten. Ob er ihr im Einzelfall nachkommt, hängt von seiner Entscheidung ab. Kommt er ihr nicht nach, so kann dies zu Nachteilen führen, z. B. weil der Dienstherr dann vom Vorliegen einer eingeschränkten Verwendungsfähigkeit ausgehen kann. Derartige Schlüsse können jedoch nicht gezogen werden, wenn der Beamte berechtigte Gründe für seine Weigerung hat oder versäumt wurde, ihn auf die Folgen einer Weigerung hinzuweisen.

Die Forderung des Dienstherrn an den Beamten, sich von einem Arzt des BGS untersuchen zu lassen, war unter datenschutzrechtlichen Gesichtspunkten nicht zu beanstanden. Die Erforderlichkeit der damit verbundenen Datenerhebung nach § 13 Abs. 1 BDSG wurde für mich nachvollziehbar dargelegt. Das Vorgehen entsprach auch dem Grundsatz des § 13 Abs. 2 Satz 1 BDSG, wonach personenbezogene Daten grundsätzlich beim Betroffenen zu erheben sind.

Ob vorhandene Vorgutachten ausreichten oder ob eine neue Untersuchung notwendig war, ist eine medizinische Fachfrage, die ich nicht überprüfe.

Aufgrund der Diskussion, die ich anläßlich dieses Falles mit dem BMI geführt habe, hat dieser inzwischen die Bestimmungen über das Verfahren zur Feststellung der Polizeidienstunfähigkeit im BGS dahingehend geändert, daß der einzelne Beamte vor einer grenzschutzärztlichen Überprüfung zu unterrichten ist; ihm ist Gelegenheit zu geben, sich zu der beabsichtigten Maßnahme zu äußern. Im Zusammenhang der Feststellung der weiteren Verwendungsfähigkeit einzuholende oder vorhandene Berichte ärztlichen Inhaltes dürfen ausschließlich vom Arzt im BGS mit Kenntnis des Betroffenen eingeholt und ausgewertet werden.

9.14.4 Deutsche Bundesbank zur besseren Wahrung des Patientengeheimnisses veranlaßt

Die Deutsche Bundesbank (einschließlich Landeszentralbanken) verwendet einen Vordruck für die Erstellung vertrauensärztlicher Gutachten bei Einstellungsuntersuchungen und andere amts- oder vertrauensärztliche Untersuchungen. Dieser ist vom untersuchenden Arzt auszufüllen und enthält die Forderung nach detaillierten Anamnese- und Diagnosedaten. Die ausgefüllten Vordrucke werden außerhalb der Personalakte in besonderen Ordnern unter Verschluß gehalten.

Die im Gutachten vermerkten Daten unterliegen der ärztlichen Schweigepflicht. Sie dürfen daher grundsätzlich nur mit Zustimmung des Betroffenen an die Personalverwaltung übermittelt werden. Auch mit Zustimmung darf der Arzt lediglich das Ergebnis der ärztlichen Untersuchung übermitteln; d. h. die Feststellung, ob ein Bewerber für die Übernahme in das Dienst- oder Arbeitsverhältnis, für eine bestimmte Tätigkeit geeignet, nicht geeignet oder nur einge-

schränkt (und gegebenenfalls mit welchen Einschränkungen) geeignet ist. Darüber hinausgehende Daten sind für die Aufgabenerfüllung der Personalverwaltung nicht erforderlich.

Ärztliche Unterlagen, die in einem unmittelbaren Zusammenhang mit dem Dienst- oder Arbeitsverhältnis stehen, gehören zur Personalakte (vgl. § 90 Abs. 1 Satz 2 BBG). Sie sind in der Personalakte in einem verschlossenen Umschlag aufzubewahren. Der Umschlag ist zu versiegeln. Bei jedem Öffnen sind das Datum und das Handzeichen des Öffnenden zu vermerken. Eine Trennung solcher ärztlicher Unterlagen von der Personalakte würde auch das Recht des Betroffenen auf umfassende Einsicht in seine Personalakte gefährden.

Ich habe meine datenschutzrechtliche Bewertung der Deutschen Bundesbank mitgeteilt und sie gebeten, künftig entsprechend zu verfahren. Die Bundesbank hat sich meiner Auffassung zwischenzeitlich in vollem Umfange angeschlossen. Sie hat Regelungen getroffen, nach denen ihre Personalverwaltung bei ärztlichen Untersuchungen nur noch das Ergebnis der Untersuchung anfordern und ärztliche Unterlagen in einem verschlossenen Umschlag in der Personalakte aufbewahren wird.

10 Sozialwesen — Allgemeines

10.1 Der Datenschutz im Sozialgesetzbuch wird neu geregelt

Eine grundlegende Überarbeitung der Regelungen über das Sozialgeheimniss (§ 35 SGB I) und den Schutz der Sozialdaten (2. Kapitel SGB X) war schon aufgrund des Volkszählungsurteils des Bundesverfassungsgerichts erforderlich; sie wurde nach der Neufassung des Bundesdatenschutzgesetzes noch dringender. Infolge der teilweise neuen Paragraphenfolge des BDSG stimmen die Verweisungen im Sozialgesetzbuch auf das BDSG nicht mehr. Außerdem setzen die §§ 79ff. SGB X, die auf das BDSG Bezug nehmen, voraus, daß dieses nur für Daten in Dateien gilt, was jedoch nicht mehr zutrifft.

Das Bundesministerium für Arbeit und Sozialordnung hat mir in einem frühen Stadium den Referentenentwurf einer Novellierung des Sozialgesetzbuches vorgelegt, mit dem diese Mängel beseitigt werden sollen. Der Entwurf sieht eine weitgehend abschließende bereichsspezifische Regelung des Umganges mit Sozialdaten vor. Bei seiner Ausgestaltung wurde, abgesehen von den Bestimmungen über die Landesbeauftragten für den Datenschutz und die Schadensersatzregelung, darauf verzichtet, auf die Vorschriften des BDSG zu verweisen. Dessen Regelungen wurden in den Text des Sozialgesetzbuches so weit wie möglich übernommen, sofern nicht wegen der Besonderheiten der zu regelnden Materie Abweichungen erforderlich waren. Dem Rechtsanwender soll damit ein in sich geschlossener Gesetzestext in die Hand gegeben werden, der ein zusätzliches Nachschlagen in anderen Gesetzen weitgehend erspart.

Der Gesetzentwurf bringt in vielen Punkten — wenn auch nicht alle meine Forderungen umgesetzt wurden — wesentliche datenschutzrechtliche Fortschritte. Er enthält in der nach langen Gesprächen vorgesehenen Fassung natürlich auch Kompromisse zwischen datenschutzrechtlichen Wünschen und den Bedürfnissen der Praxis.

Wesentliche Punkte des Gesetzentwurfes sind:

- Das Sozialgeheimnis schützt künftig die Erhebung, die Verarbeitung und die Nutzung von Sozialdaten (§ 35 Abs. 1 Satz 1 SGB I). Bislang bietet es grundsätzlich nur Schutz gegen eine unbefugte Offenbarung von Sozialdaten.
- Die Wahrung des Sozialgeheimnisses soll die Verpflichtung einschließen, auch innerhalb des Leistungsträgers sicherzustellen, daß die Sozialdaten nur Befugten zugänglich sind und nur an diese weitergegeben werden (§ 35 Abs. 1 Satz 2 SGB I). Diese Ergänzung war notwendig, da der zentrale Begriff des „Offenbarens" durch den Begriff des „Übermittelns" ersetzt wurde. Maßgebend hierfür waren die Anlehnung an die Terminologie des BDSG (§ 3 Abs. 5 Nr. 3) sowie die Verwendung einheitlicher Begriffe im Sozialgesetzbuch, das im Fünften Buch — gesetzliche Krankenversicherung — bereits den Begriff des „Übermittelns" kennt.
- Der Sozialdatenschutz Verstorbener soll erstmals gesetzlich geregelt werden (§ 35 Abs. 5 SGB I).
- Der Begriff der „Sozialdaten" wird erstmals im Gesetz definiert (§ 67 Abs. 1 SGB X). Sozialdaten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden.
- „Übermitteln" i. S. des Sozialgesetzbuches ist über den Wortlaut des § 3 Abs. 5 Nr. 3 BDSG hinaus auch das Bekanntgeben nicht gespeicherter Sozialdaten. Damit werden zurecht auch Daten geschützt, die ausschließlich im Gedächtnis festgehalten sind.
- Es wird ausdrücklich festgestellt, daß auch die Weitergabe innerhalb der speichernden Stelle eine „Nutzung" darstellt (§ 67 Abs. 7 SGB X).
- Einen wichtigen Punkt stellt die Regelung der Datenerhebung ohne die Mitwirkung des Betroffenen bei anderen Sozialleistungsträgern dar (§ 67 a Abs. 2 Satz 2 Nr. 1 SGB X). Das BMA hat nachvollziehbar vorgetragen, daß im Interesse eines zügigen Verwaltungsverfahrens, das auch im Interesse des Betroffenen liegt, auf eine unmittelbare Datenerhebung bei anderen Leistungsträgern letztlich nicht verzichtet werden kann. In dieser Frage konnte nach langen Erörterungen ein Kompromiß gefunden werden, der eine Ersterhebung von Sozialdaten bei anderen Sozialleistungsträgern zuläßt, wenn — kumulativ —

  a) diese zur Übermittlung der Daten an die erhebende Stelle befugt sind,

b) diese Daten für die erhebende Stelle zur Anwendung der Rechtsvorschriften nach diesem Gesetzbuch erforderlich sind,

c) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und

d) keine Anhaltspunkte dafür bestehen, daß die Erhebung bei einem anderen Sozialleistungsträger überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt.

— Sofern Ausnahmen vom Ersterhebungsgrundsatz zulässig sind, ist der Betroffene von der erhebenden Stelle in geeigneter Form schriftlich auf diese Erhebungsmöglichkeiten hinzuweisen (§ 67a Abs. 2 Satz 3 SGB X).

— Das Speichern, Verändern oder Nutzen von Sozialdaten ist grundsätzlich nur zulässig, wenn es zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden gesetzlichen Aufgaben nach dem Sozialgesetzbuch erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind (§ 67c Abs. 1 Satz 1 SGB X). In den Verhandlungen wurde heftig um die Frage gerungen, ob und unter welchen Voraussetzungen Sozialdaten auch für andere Zwecke genutzt werden dürfen als die, für die sie erhoben wurden. Der Entwurf läßt eine Ausnahme von dieser Zweckbindung zu, wenn die nach oben genannten Kriterien rechtmäßig gespeicherten Daten für die Erfüllung von Aufgaben nach anderen Rechtsvorschriften des Sozialgesetzbuches als diejenigen, für die sie erhoben wurden, erforderlich sind. In derartigen Fällen dürfen diese Daten von derselben Stelle auch für andere — im Sozialgesetzbuch festgelegte — Zwecke gespeichert, verändert oder genutzt werden. Eine weitere Ausnahme kommt dann in Betracht, wenn der Betroffene im Einzelfall in die Zweckänderung eingewilligt hat (§ 67c Abs. 2 SGB X). Selbstverständlich bleiben spezielle Zweckbindungsregelungen, wie z. B. in § 64 Abs. 1 SGB VIII erhalten.

— Die Verantwortung für die Zulässigkeit einer Übermittlung von Sozialdaten trägt die übermittelnde Stelle. Erfolgt die Übermittlung jedoch auf Ersuchen des Empfängers, trägt dieser die Verantwortung für die Richtigkeit der Angaben in seinem Ersuchen (§ 67d Abs. 2 SGB X).

— Die bislang bestehende generelle Zulässigkeit der Datenübermittlung im Rahmen der Amtshilfe (§ 68 SGB X) wird eingeschränkt auf die Übermittlung für Aufgaben der Polizeibehörden und zur Durchsetzung öffentlich-rechtlicher Ansprüche.

— Die Regelung über die Übermittlung von Sozialdaten im Rahmen der Aufgabenerfüllung des Sozialleistungsträgers (§ 69 Abs. 1 Nr. 1 SGB X) wird im Interesse der Normenklarheit neu formuliert. Es soll einmal klargestellt werden, daß eine Übermittlung auch erfolgen darf, wenn sie im Rahmen einer zulässigen Zweckänderung erfolgt. Zum anderen wird deutlich gemacht, daß eine Übermittlung für die Aufgabenerfüllung der abgebenden wie der empfangenden Stelle zulässig ist.

— Die Befugnis der Krankenkassen zur Datenübermittlung im Zusammenhang mit einer Arbeitsunfähigkeit eines Arbeitnehmers wird konkret geregelt. Die Kassen sollen befugt sein, einem Arbeitgeber mitzuteilen, ob die Fortdauer einer Arbeitsunfähigkeit oder eine erneute Arbeitsunfähigkeit eines Arbeitnehmers auf derselben Krankheit beruht; die Übermittlung von Diagnosedaten an den Arbeitgeber ist nicht zulässig (§ 69 Abs. 4 SGB X).

— Die Übermittlung von Sozialdaten für die Forschung und Planung ist nur zulässig, soweit sie für die Durchführung eines bestimmten Vorhabens erforderlich ist (§ 75 Abs. 1 SGB X). Dabei ist die Übermittlung an eine nicht-öffentliche Stelle nur rechtmäßig, wenn diese sich der Kontrolle des für die übermittelnde Stelle zuständigen Datenschutzbeauftragten unterwirft (§ 75 Abs. 3 SGB X).

— Der Betroffene ist künftig von der speichernden Stelle zu Beginn eines Verwaltungsverfahrens in allgemeiner Form schriftlich darauf hinzuweisen, daß er der Übermittlung von Daten widersprechen kann, die dem Patientengeheimnis unterliegen (§ 76 Abs. 2 Nr. 1 2. Halbsatz SGB X).

— Ins Ausland oder an über- und zwischenstaatliche Stellen ist auch bei Vorliegen eines Übermittlungstatbestandes eine Übermittlung nur zulässig, wenn dadurch schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden. Der Empfänger ist von der übermittelnden Stelle auf die Bindung an den Übermittlungszweck hinzuweisen (§ 77 SGB X).

— Personen oder Stellen, die nicht in § 35 SGB I genannt sind und denen Sozialdaten übermittelt worden sind, dürfen diese grundsätzlich nur zu dem Zweck verarbeiten oder nutzen, zu dem sie ihnen befugt übermittelt worden sind (§ 78 Abs. 1 Satz 1 SGB X).

— Über die Regelung in § 10 BDSG hinaus wird als Voraussetzung für die Zulässigkeit automatisierter Abrufverfahren eine „Vielzahl von Übermittlungen" oder deren „besondere Eilbedürftigkeit" verlangt. Die Voraussetzungen für die Einrichtung automatisierter Verfahren mit entsprechenden Leistungsträgern im Ausland werden geregelt.

— Eine Verarbeitung oder Nutzung von Sozialdaten im Auftrag durch nicht-öffentliche Stellen, die nicht in § 35 SGB I genannt sind, ist nur zulässig, wenn sich diese Stellen der Kontrolle des für den Auftraggeber zuständigen Datenschutzbeauftragten unterwerfen und die weiteren Voraussetzungen des § 80 Abs. 5 SGB X vorliegen.

— Bei der Regelung über die Datenschutzbeauftragten wird auf die Widerspruchsregelung des § 24 Abs. 3 Sätze 4 und 5 BDSG nicht Bezug genommen, da diese sich nicht bewährt hat und der Schutz der Sozialdaten eine uneingeschränkte Kontrolle durch die Datenschutzbeauftragten erfordert (§ 81 Abs. 2 Satz 1 SGB X).

— Die in § 35 SGB I genannten Stellen haben einen Datenschutzbeauftragten zu benennen (Verwei-

sung durch § 81 Abs. 4 SGB X auf die §§ 36, 37 BDSG). Zusätzlich wird sichergestellt, daß diese in räumlich getrennten Organisationseinheiten bei der Erfüllung ihrer Aufgaben zu unterstützen sind.

— Wird einem Betroffenen von einem Sozialleistungsträger des Bundes durch eine unzulässige oder unrichtige automatisierte Verarbeitung seiner Sozialdaten ein Schaden zugefügt, so haftet der Schädiger unabhängig von seinem Verschulden (§ 82 SGB X i.V.m. § 7 BDSG).

— Dem Betroffenen ist auf Antrag grundsätzlich sowohl über die zu seiner Person gespeicherten Sozialdaten, auch soweit sie sich auf die Herkunft oder den Empfänger dieser Daten beziehen, als auch über den Zweck der Speicherung Auskunft zu erteilen (§ 83 Abs. 1 SGB X). Wird das Auskunftsbegehren abgelehnt, so hat die ablehnende Stelle den Betroffenen darauf hinzuweisen, daß er sich an die im konkreten Fall zuständige Datenschutzkontrollinstanz wenden kann (§ 83 Abs. 5 SGB X). Diese kann dann prüfen, ob die Ablehnung der Auskunftserteilung rechtmäßig war (§ 83 Abs. 6 SGB X).

— Sozialdaten sind u. a. zu löschen, wenn ihre Speicherung — und zwar unabhäng ob in Dateien oder Akten — unzulässig ist. Im Unterschied zur Regelung des BDSG für die übrige Verwaltung sind Sozialdaten auch in Akten zu löschen, da das SGB X insoweit schon von jeher von der Gleichstellung der Daten in Akten und Dateien ausgegangen ist. Sie sind ebenfalls zu löschen, wenn sie für die Aufgabenerfüllung des Sozialleistungsträgers nicht mehr erforderlich sind und kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Interessen des Betroffenen beeinträchtigt werden (§ 84 Abs. 2 SGB X).

— In § 84 a SGB X wird ausdrücklich festgeschrieben, daß Rechte des Betroffenen nach dem Zweiten Kapitel des SGB X nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden können.

— Ein Arzt oder ein Angehöriger eines anderen Heilberufes darf grundsätzlich personenbezogene Daten für die Durchführung eines bestimmten Forschungsvorhabens an einen Träger oder Spitzenverband der gesetzlichen Unfallversicherung übermitteln (§ 100 a SGB X). Das Forschungsvorhaben darf nur durchgeführt werden, wenn sichergestellt ist, daß keinem Beschäftigten, der an Entscheidungen über Sozialleistungen oder um deren Vorbereitung beteiligt ist, die für das Forschungsvorhaben zur Verfügung gestellten Daten zugänglich sind. Die Durchführung des Forschungsvorhabens ist im übrigen organisatorisch und räumlich von den anderen Aufgaben des Verbandes oder Trägers zu trennen.

Zusammenfassend kann ich feststellen, daß die Abstimmung des Gesetzentwurfes mit dem BMA weit vorangeschritten ist. Eine Klärung einiger noch offener Detailfragen erscheint in nächster Zeit möglich. Es ist zu wünschen, daß der Gesetzentwurf noch in dieser Legislaturperiode beraten und verabschiedet wird. Ich gehe davon aus, daß die eine oder andere bei der Vorbereitung des Entwurfs besonders umstrittene Frage in den gesetzgebenden Körperschaften noch einmal vertieft beraten werden kann.

10.2 Grundsatz der Ersterhebung beim Betroffenen verletzt

Der Ersterhebungsgrundsatz des § 13 Abs. 2 Satz 1 BDSG, mit dessen Anwendung bei der Erhebung von Sozialdaten ich mich schon im 13. Tätigkeitsbericht, S. 62 befaßt habe, wird auch von Sozialversicherungsträgern nicht immer beachtet.

Ein Unternehmen hatte eine Steuerberatungsgesellschaft damit beauftragt, die für sie zuständige Berufsgenossenschaft über die Aufnahme ihres Geschäftsbetriebes zu informieren. Dies hatte sie mit der Bitte verbunden, ihr im Zusammenhang mit der Geschäftsaufnahme von ihr auszufüllende Vordrucke zu übersenden. Daraufhin hat die Berufsgenossenschaft je ein Exemplar eines entsprechenden Vordruckes an die das Unternehmen vertretende Steuerberatungsgesellschaft und gleichzeitig an die für das Unternehmen zuständige, kommunale Gewerbebehörde übersandt. Diese *gleichzeitige* Anfrage beim Betroffenen und einem Dritten verstößt gegen den Ersterhebungsgrundsatz des § 13 Abs. 2 Satz 1 BDSG, wonach personenbezogene Daten grundsätzlich (zuerst) beim Betroffenen zu erheben sind. Den oben beschriebenen Verstoß gegen den Ersterhebungsgrundsatz habe ich gegenüber der Berufsgenossenschaft beanstandet, nachdem diese sich geweigert hatte, das beschriebene Verfahren zu ändern.

In einem weiteren Fall hatte ein Bürger Leistungen nach dem Arbeitsförderungsgesetz beantragt und glaubte, er müsse deshalb seine Mitgliedschaft bei der Krankenkasse beenden. Tatsächlich besteht aber beim Bezug von Leistungen nach dem Arbeitsförderungsgesetz Versicherungspflicht; die bisherige Krankenkasse bleibt zuständig.

Da eine vom Petenten mitgeteilte neue Anschrift als Adresszusatz den Namen seines Vermieters enthielt, aber auch dessen unter gleichem Namen geführte Firma im Telefonbuch stand, fragte die Krankenkasse dort telefonisch direkt an, ob der Petent dort beschäftigt sei.

Diese Art der Nachforschung verstieß gegen den Ersterhebungsgrundsatz. Die von der Krankenkasse begehrte Information hätte zunächst beim Petenten erhoben werden müssen. Eine Erhebung ohne Mitwirkung des Betroffenen war nicht zulässig, weil die Voraussetzungen des § 13 Abs. 2 Satz 2 BDSG nicht vorlagen.

Die Krankenkasse hat mir mitgeteilt, daß sie unabhängig von meiner Einschaltung dem Petenten ihr Bedauern über das Verhalten ihrer Mitarbeiterin ausgesprochen hat. Sie hat auf meine Bitte hin zugesagt, alle Mitarbeiter aufzufordern, in vergleichbaren Fällen den Ersterhebungsgrundsatz zu beachten.

10.3 Rechte Betroffener auf Einsicht in ärztliche Unterlagen durchgesetzt

Probleme im Zusammenhang mit der Einsicht von Bürgern in ihre Akten (§ 25 SGB X) treten bei fast allen Trägern der sozialen Sicherung auf. Ich greife zwei Fälle heraus, mit denen ich mich aufgrund von Bürgereingaben während des Berichtszeitraums beschäftigt habe.

10.3.1 Bundesversicherungsanstalt für Angestellte (BfA) wollte nur über Hausarzt Einsicht gewähren

Eine Versicherte der BfA wollte nach Abschluß einer Kur in ihre Krankengeschichte, konkret in den Entlassungsbericht der Kurklinik, Einsicht nehmen. Die BfA bat daraufhin um Namen und Anschrift ihres Hausarztes, um diesem den Entlassungsbericht der Kurklinik übersenden zu können. Eine unmittelbare Einsichtnahme der Petentin lehnte sie zunächst ab, gestand sie dann aber zu, nachdem ich mich eingeschaltet hatte.

Die ursprüngliche Haltung der BfA, den Entlassungsbericht nur an den Hausarzt zu übersenden, ist mit geltendem Recht nicht zu vereinbaren. Die BfA hat § 25 Abs.2 Satz 4 SGB X nicht beachtet. Dort wird ausdrücklich darauf hingewiesen, daß der Rechtsanspruch des Betroffenen auf Akteneinsicht (§ 25 Abs.1 SGB X) nicht beschränkt wird. Im Einzelfall kann es zwar durchaus sinnvoll sein und im Interesse eines Antragstellers liegen, den Inhalt von Akten über gesundheitliche Verhältnisse durch einen Arzt vermitteln zu lassen, weil dieses Verfahren eine gleichzeitige fachkundige Beratung und Betreuung des Betroffenen ermöglicht. Besteht der Versicherte jedoch auch nach einem entsprechenden Hinweis durch den Sozialversicherungsträger auf einer unmittelbaren Einsicht, so darf ihm diese nicht vorenthalten werden.

10.3.2 Ersatzkasse gewährt nach Diskussion Akteneinsicht

Ein Versicherter hatte eine Ersatzkasse um Akteneinsicht gebeten. Diese wurde ihm mit der Begründung verweigert, daß Akteneinsicht ausschließlich in laufenden Verwaltungsverfahren gewährt werde; ein solches liege aber nicht vor. Darüber hinaus enthalte die Akte Informationen über Dritte, deren Zustimmung erforderlich sei. Die Akte enthalte schließlich auch ein psychologisches Gutachten, von dessen Inhalt nur ein Arzt des Vertrauens des Petenten Kenntnis nehmen könne.

Die Weigerung der Ersatzkasse entspricht nicht dem geltenden Recht. § 25 Abs.1 Satz 1 SGB X räumt den Beteiligten einen Rechtsanspruch auf Einsicht in die das Verfahren betreffenden Akten ein, und zwar unabhängig davon, ob ein Verwaltungsverfahren bereits abgeschlossen ist oder nicht. Der Rechtsanspruch setzt vielmehr nur voraus, daß es einmal ein Verfahren gegeben hat, daß die Unterlagen, in die Einsicht begehrt wird, dieses Verfahren betreffen und daß die Kenntnis der Akten zur Geltendmachung oder Verteidigung der rechtlichen Interessen eines am Verfahren Beteiligten erforderlich ist. Ein solches Interesse ist z. B. gegeben, wenn die Einsichtnahme bezweckt, eine tatsächliche Unsicherheit über ein Rechtsverhältnis zu klären, eine Rechtsbeziehung aufgrund des Ergebnisses der Einsichtnahme zu regeln oder eine gesicherte Grundlage für die Verfolgung eines Anspruchs zu erhalten. Solche rechtlichen Interessen können auch noch nach Abschluß des Verwaltungsverfahrens bestehen oder entstehen, insbesondere wenn es um einen neuen Gesichtspunkt geht, wie etwa den Anspruch auf Berichtigung, Löschung oder Sperrung von Daten nach § 20 BDSG.

Daß § 25 Abs. 1 Satz 1 SGB X auch nach Abschluß eines Verwaltungsverfahrens einen Anspruch auf Einsicht in die das Verfahren betreffenden Akten gibt, folgt übrigens eindeutig aus dessen Satz 2. Wenn dort als eine Satz 1 einschränkende Regelung gesagt wird, bis zum Abschluß eines Verwaltungsverfahrens bestehe kein Anspruch auf Einsichtnahme in Entwürfe zu Entscheidungen und die Arbeiten zu ihrer unmittelbaren Vorbereitung, so kann das doch nur bedeuten, daß ein solches Recht nach Abschluß des Verwaltungsverfahrens besteht. Wenn der Beteiligte nach Abschluß des Verfahrens aber sogar in solche vorbereitenden Unterlagen Einsicht nehmen darf, besteht kein Grund, ihm andere Teile vorzuenthalten.

Eine engere Interpretation hätte zur Folge, daß der Betroffene im Sozialleistungsbereich schlechter gestellt wäre als es das BDSG generell vorsieht, das seit der Novellierung ein Auskunftsrecht auch über in Akten gespeicherte personenbezogene Daten enthält und keine verfahrensmäßigen Einschränkungen vorsieht.

Die Ersatzkasse hat sich meiner Rechtsauffassung zwar nicht angeschlossen, aber mittlerweile — ohne Anerkennung einer Rechtspflicht — dem Petenten Akteneinsicht über einen Arzt seines Vertrauens angeboten. Mit diesem Verfahren hat der Petent sich einverstanden erklärt.

Dabei hat die Krankenkasse mir versichert, daß, soweit die Akte Angaben über Dritte enthielt, die entsprechenden Passagen vor Gewährung der Akteneinsicht unkenntlich gemacht wurden.

10.4 Datenoffenbarung im Sozialgerichtsverfahren

Die Frage, in welchem Umfang Sozialdaten im sozialgerichtlichen Verfahren offenbart werden dürfen (13. TB S. 62) hat mich auch im Berichtszeitraum beschäftigt.

10.4.1 Unaufgeforderte Weitergabe eines Bescheides einer Landesversicherungsanstalt

Ein Bürger und eine Berufsgenossenschaft führten einen Rechtsstreit vor einem Sozialgericht über die Anerkennung einer Berufskrankheit.

Im Laufe dieses Rechtsstreits hat die Berufsgenossenschaft — ohne hierzu vom Gericht aufgefordert wor-

den zu sein — einen ihr vorliegenden Bescheid einer Landesversicherungsanstalt über den Betroffenen an das Sozialgericht übersandt. Dies hat sie damit begründet, ihr sei aus jahrelanger Erfahrung bekannt, daß Gerichte insbesondere bei der Klärung schwieriger medizinischer Fragen und Zusammenhänge auch Akten der Rentenversicherungsträger beiziehen, wenn dies für erforderlich gehalten wird. Im vorliegenden Fall hat die Berufsgenossenschaft die unaufgeforderte Übersendung des Bescheides der Landesversicherungsanstalt über den Betroffenen für sachgerecht erachtet, weil sich aus der Begründung des Bescheides ergab, daß fachärztliche Untersuchungen nicht durchgeführt worden waren. Hierdurch habe man dem Sozialgericht eine möglicherweise vorgesehene Beiziehung der Akte des Rentenversicherungsträgers ersparen wollen.

Diese nicht vom Gericht veranlaßte und somit auf die Eigeninitiative der Berufsgenossenschaft hin erfolgte Übersendung des Bescheides der Landesversicherungsanstalt war unzulässig (§ 69 Abs. 1 Nr. 1, 2. Alternative SGB X), da sie nicht für die Durchführung eines mit der Erfüllung einer der gesetzlichen Aufgaben der Berufsgenossenschaft zusammenhängenden gerichtlichen Verfahrens erforderlich war. Dies wird bereits daran deutlich, daß das Sozialgericht üblicherweise auf eigene Initiative vom Rentenversicherungsträger Akten anfordert, diese aber nicht unaufgefordert übersandt werden.

Da die Berufsgenossenschaft mir zunächst mitgeteilt hat, daß sie die in diesem Fall erfolgte Übermittlung von Sozialdaten an das Sozialgericht für zulässig hält, habe ich den oben beschriebenen Verstoß gegen § 35 SGB I i. V. m. § 69 Abs. 1, Nr. 1, 2. Alternative SGB X gemäß § 25 Abs. 1 BDSG beanstandet.

Außerdem habe ich die Berufsgenossenschaft gebeten, in Zukunft auf die von ihr ebenfalls eingeräumte Praxis zu verzichten, sich nicht erforderliche Unterlagen der Rentenversicherungsträger vom Sozialgericht zur Auswertung zusenden zu lassen. Insoweit hat die Berufsgenossenschaft mittlerweile signalisiert, daß sie sicherstellen wird, daß diese von ihr bisher praktizierte Vorgehensweise in Zukunft nicht mehr vorkommen wird.

10.4.2 Darf stets die gesamte Versicherungsakte dem Sozialgericht zugeleitet werden?

Eine Bürgerin hat sich dagegen gewandt, daß die BfA ihre gesamte Versichertenakte im Rahmen eines Verfahrens an ein Sozialgericht trotz ihres vorsorglichen Widerspruchs übersandt hat. Die BfA hatte zwar zunächst der Aufforderung des Sozialgerichts zur Aktenübersendung nicht entsprochen. Nachfolgend aber hatte sie dem Ersuchen des Sozialgerichts Rechnung getragen und die gesamte Akte übersandt, obwohl das Gericht deutlich gemacht hatte, auf welche Informationen es ihm ankam, nämlich auf „die Kenntnis der Angaben der Klägerin, die sie ggf. im Zusammenhang mit der in Streit stehenden Zeit der Arbeitslosigkeit ab Januar 1985 gemacht hat, sowie die Kenntnis der Belegung dieses Zeitraumes mit versicherungsrechtlich relevanten Tatbeständen".

Die Verfahrensweise der BfA bewerte ich aus datenschutzrechtlicher Sicht wie folgt:

Nach § 119 Abs. 1 SGG sind alle Behörden grundsätzlich zur Vorlage von Urkunden und Akten und zur Auskunftserteilung gegenüber dem Sozialgericht verpflichtet. Diese Verpflichtung kann im Hinblick auf das Sozialgeheimnis aber nur insoweit bestehen, wie Vorlage und Auskunft nach eigener Einschätzung des Gerichts erforderlich sind.

Im vorliegenden Fall war es nicht erforderlich, dem Sozialgericht die gesamte Versichertenakte zu überlassen. Dieses hatte nämlich die konkreten Sachverhalte genau bezeichnet, zu deren Aufklärung es die angeforderten Unterlagen benötigte. In einem derartigen Fall obliegt es dem Sozialversicherungsträger, die Vorlage gegenüber dem Sozialgericht auf die Unterlagen zu begrenzen, die für die Beantwortung der konkret bezeichneten Fragen maßgebend sind. Ich habe daher der BfA eine entsprechende Verfahrensweise empfohlen.

Die BfA sieht sich bisher außerstande, dieser Empfehlung zu folgen. Sie beruft sich dabei auf die §§ 103, 106 SGG, wonach die Verfahrensbeteiligten im sozialgerichtlichen Verfahren umfassend zu Sachverhaltsermittlungen beizutragen haben. Aus dieser prozessual geregelten Mitwirkungspflicht folgert die BfA, daß die Kenntnis der für das Gerichtsverfahren einschlägigen Unterlagen für das Gericht unverzichtbar ist, die Daten dementsprechend also nicht vorenthalten werden dürfen. Nur das Gericht allein, nicht die Behörde oder der jeweils beteiligte Leistungsträger, könne beurteilen, wie die Entscheidungsreife des Rechtstreits herbeizuführen ist. In dieser Grundfrage besteht kein Streit. Entscheidend ist, daß nach dem eigenen zutreffenden Vortrag der BfA nur die für das jeweilige Verfahren einschlägigen Unterlagen vorzulegen sind. Lassen sich diese von den übrigen bei dem um Aktenübersendung ersuchten Leistungsträger angefallenen Unterlagen trennen, so hat der Leistungsträger das Gericht darauf hinzuweisen und auf eine entsprechende Einschränkung des Ersuchens hinzuwirken.

Ich werde mich zu dieser Frage nochmals mit der BfA in Verbindung setzen, um eine Lösung zu erreichen, die einerseits datenschutzrechtliche Gesichtpunkte berücksichtigt und andererseits eine vollständige und ausreichende Sachverhaltsermittlung durch das Sozialgericht ermöglicht.

10.4.3 Dürfen Gesundheitsdaten im Sozialgerichtsverfahren in öffentlicher Sitzung bekanntgegeben werden?

Ein Versicherter wandte sich dagegen, daß seine Gesundheitsdaten bei dem Rentenversicherungsträger zwar vertraulich behandelt werden, der Inhalt ärztlicher Gutachten im öffentlichen Sozialgerichtsverfahren jedoch jedermann bekannt werde.

Die Sitzungen des Sozialgerichtes sind grundsätzlich öffentlich (§ 169 GVG i. V. m. § 61 SGG). Das Gericht kann die Öffentlichkeit aber ausschließen, wenn ein privates Geheimnis erörtert wird, dessen unbefugte Offenbarung durch den Zeugen oder Sachverständi-

gen mit Strafe bedroht ist (§ 172 Nr. 3 GVG). Der Inhalt ärztlicher Gutachten stellt in aller Regel ein derartiges Geheimnis dar (s. § 203 StGB). Über die Frage des Ausschlusses der Öffentlichkeit wird entschieden, wenn ein Beteiligter es beantragt oder das Gericht es für angemessen erachtet (§ 174 Abs. 1 GVG).

10.5 Datenoffenbarung nach § 69 SGB X

10.5.1 Weitergabe von Sozialdaten an die Staatsanwaltschaft

In einem Ermittlungsverfahren wegen nicht gezahlter Beiträge wurde eine Krankenkasse von der Staatsanwaltschaft zur Offenbarung personenbezogener Daten aufgefordert. Dabei ging es um die Mitteilung der Namen von Arbeitnehmern, deren Arbeitnehmeranteile zur Sozialversicherung ein Arbeitgeber vorenthalten haben sollte. Weiter sollten die jeweiligen Beitragsmonate und die jeweiligen Arbeitnehmeranteile in diesen Beitragsmonaten bezeichnet werden.

Die Krankenkasse hat eine Offenbarung unter Hinweis darauf verweigert, daß sie zur Offenbarung personenbezogener Daten nur verpflichtet sei, wenn damit auch die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch verbunden ist (§ 69 Abs. 1 Nr. 1, 2. Alt. SGB X). Daran fehle es im vorliegenden Fall, da der Beitragsschuldner zwischenzeitlich die Beiträge beglichen habe.

Die aus datenschutzrechtlicher Sicht zentrale Frage ist in diesem Zusammenhang, ob der Sozialversicherungsträger im Rahmen eines Ermittlungsverfahrens personenbezogene Daten zulässigerweise an die Staatsanwaltschaft übermitteln darf und wenn ja, ob er hierzu ausnahmslos verpflichtet ist oder ob ihm die Entscheidungsbefugnis über die Offenbarung obliegt. Hierzu vertrete ich folgende Meinung:

Nach der Strafprozeßordnung kann die Staatsanwaltschaft im Rahmen eines Ermittlungsverfahrens Auskunft von allen öffentlichen Behörden verlangen (§ 161 StPO). Die sich daraus ergebende grundsätzliche Auskunftsverpflichtung der Behörde wird jedoch durch bereichsspezifische Regelungen, wie z. B. durch das Sozialgesetzbuch, konkretisiert und begrenzt.

Zu den gesetzlichen Aufgaben der Träger der gesetzlichen Krankenversicherung im Rahmen des Beitragseinzuges gehört es, eine Strafanzeige oder eine Anzeige an die Gewerbeaufsichtsbehörde zu erstatten, wenn eine solche Maßnahme zur Wahrung der Zahlungsdisziplin und zur Verhütung weiterer Schäden für die Versichertengemeinschaft erforderlich ist. Diese Befugnis muß den Krankenkassen im Hinblick auf eine ordnungsgemäße Aufgabenerfüllung zugestanden werden. Ohne sie würde ein dafür notwendiges Strafverfahren in aller Regel nicht in Gang kommen.

Anders als im Rahmen des § 73 SGB X, wo eine Interessenabwägung zwischen Strafverfolgung einerseits und Sozialgeheimnis andererseits durch eine neutrale Stelle, nämlich den Richter, geboten ist, ist der Sachverhalt im Rahmen des § 69 Abs.1 Nr.1 SGB X zu beurteilen. Hier geht es um Strafverfahren mit sozialrechtlichem Bezug. Der Gesetzgeber hat hier entschieden, daß eine Offenbarung von dem Sozialgeheimnis unterliegenden Daten nach dieser Vorschrift — nur — in Betracht kommt, wenn dies der Erfüllung sozialrechtlicher Aufgaben dient.

Dies bedeutet jedoch nicht, daß personenbezogene Daten bei entsprechenden Auskunftsersuchen von Staatsanwaltschaften generell offenbart werden müßten. Maßgebend bleibt vielmehr, daß sie für die Durchführung eines Verfahrens erforderlich sind, welches mit der Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch zusammenhängt. Ein derartiger Zusammenhang ist bei einem Strafverfahren wegen Vorenthaltung von Beitragsleistungen nicht immer und ausnahmslos zu bejahen. Die Krankenkasse ist ja auch nicht in jedem derartigen Fall verpflichtet, Strafanzeige zu erstatten. Die Entscheidung, ob die Offenbarung der personenbezogenen Daten zur Wahrung der Zahlungsdisziplin oder zur Verhütung weiterer Schäden für die Versichertengemeinschaft erforderlich ist, obliegt der Krankenkasse. Mangels Kenntnis der Besonderheiten des Einzelfalls kann diese Entscheidung nicht von der Staatsanwaltschaft anstelle der Krankenkasse getroffen werden.

Führt die Prüfung der Krankenkasse zu der Entscheidung, daß eine Offenbarung der Daten an die Staatsanwaltschaft nicht für ihre Aufgabenerfüllung oder ein damit zusammenhängendes gerichtliches Verfahren erforderlich ist, ist sie auch zur Auskunft nicht verpflichtet. § 35 Abs.3 SGB I bestimmt, daß, soweit eine Offenbarung nicht zulässig ist, auch keine Auskunftspflicht, keine Zeugnispflicht und keine Pflicht zur Vorlegung oder Auslieferung von Schriftstücken, Akten, Dateien und sonstigen Datenträgern besteht. Aus dieser Vorschrift ergibt sich ein auch im Strafverfahren geltendes Zeugnisverweigerungsrecht und Beschlagnahmeverbot zugunsten des Leistungsträgers.

10.5.2 Weitergabe von Sozialdaten an Versicherte

Mit Datenübermittlungen im Zusammenhang mit der Nichtzahlung von Sozialversicherungsbeiträgen, habe ich mich aufgrund einer Eingabe auch noch in anderer Hinsicht befaßt. Ein Arbeitgeber hatte einen Teil der Versicherungsbeiträge nicht an die Krankenkasse entrichtet. In einem Schreiben bat die Krankenkasse einen seiner Arbeitnehmer um Übermittlung von Unterlagen und Informationen, die dazu dienen sollten, die Eintreibung der rückständigen Sozialversicherungsbeiträge bei dem Arbeitgeber zu ermöglichen. Sie erbat von diesem darüber hinaus Informationen darüber, ob der Inhaber einer weiteren Firma (die unter der gleichen Adresse wie die Firma des Arbeitgebers des Petenten betrieben wurde) dem Petenten gegenüber tätig geworden sei. Die Krankenkasse war berechtigt, diese Daten zu erheben, weil sie für die Erfüllung ihrer Aufgaben erforderlich waren. Eine Verpflichtung der angeschriebenen Person zur Beantwortung dieser Frage — darin stimmt die Krankenkasse in ihrer Stellungnahme zu diesem Fall mit mir überein — bestand allerdings nicht.

Um ihr Auskunftsersuchen zu begründen, informierte die Krankenkasse den Petenten darüber, daß der weitere Firmeninhaber bereits früher unter der betreffenden Anschrift nicht eingetragene Firmen geleitet und Sozialversicherungsbeiträge nicht abgeführt hatte. Insoweit war die Offenbarung der personenbezogenen Daten über den Firmeninhaber durch die Krankenkasse an den Petenten zur Erfüllung ihrer gesetzlichen Aufgaben (hier: Ermittlungen zur Ermöglichung der Einziehung rückständiger Sozialversicherungsbeiträge) nicht erforderlich; sie erfolgte somit ohne Rechtsgrundlage.

In ihrer Stellungnahme zu diesem Fall hat die Krankenkasse mir mitgeteilt, daß sie meine Rechtsauffassung teilt. Sie hat — auf meine Aufforderung — zugesagt, in ihrer Dienstanweisung „Datenschutz" diesen Fall abstrakt zu behandeln und unsere gemeinsame Rechtsauffassung bekannt zu geben. Dabei wird sie die Mitarbeiter der Einzugsstelle unter Bezug auf die einschlägigen Dienstanweisungen auf die Vorschrift des § 69 Abs. 1 SGB X ausdrücklich hinweisen und diese näher erläutern.

10.6 Muß ein Leistungsträger den Informanten über einen angeblichen Leistungsmißbrauch benennen?

Mancher Sozialleistungsempfänger hat schon erlebt, daß ein Nachbar, Kollege oder sonstiger Bekannter dem Leistungserbringer Hinweise gab, daß die Sozialleistung ungerechtfertigt bezogen werde. So erhalten Arbeitsämter beispielsweise Mitteilungen, bestimmte Arbeitslose gingen einer Schwarzarbeit nach oder Rentenversicherungsträger werden informiert, daß Bezieher von Erwerbsunfähigkeitsrenten schwere körperliche Arbeiten verrichten. Solche Hinweise Dritter — oft als Denunziation empfunden — sind häufig, aber keineswegs immer, anonym.

Zu einem Hinweis, der unter voller Namensnennung erfolgt war, hatte die Bundesanstalt für Arbeit aufgrund einer Prüfung festgestellt, daß kein Leistungsmißbrauch vorlag. Der Leistungsbezieher verlangte daraufhin von der BA, ihm den Informanten zu nennen, um sich vor weiteren derartigen Hinweisen, die er als Denunziationen bewertete, schützen zu können. Die BA lehnte dies ganz allgemein aus Datenschutzgründen ab.

Dem kann ich mich so nicht anschließen. Bei der Beurteilung ist einerseits zu berücksichtigen, daß die Bundesanstalt für Arbeit auf Hinweise angewiesen ist, um von Leistungsmißbräuchen zu erfahren und um diesen nachgehen zu können; die Aufdeckung solcher Mißbräuche liegt im Interesse der Versichertengemeinschaft. Andererseits muß jedoch verhindert werden, daß bösartige und willkürliche Denunziationen von Sozialleistungsbeziehern übliche Praxis werden.

Die Anwendung des § 19 BDSG führt zu einer angemessenen Lösung des Problems. Nach dieser Vorschrift unterbleibt die Auskunft u. a. insoweit, als dadurch die ordnungsgemäße Erfüllung der in der Zuständigkeit des Sozialversicherungsträgers liegenden Aufgaben gefährdet würde (§ 19 Abs. 4 Nr. 1 BDSG) oder die Daten wegen überwiegender berechtigter Interessen eines Dritten geheimgehalten werden müssen (§ 19 Abs. 4 Nr. 3 BDSG) und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muß.

Im Hinblick auf das Informationsinteresse der BA kann die gebotene Abwägung oft zu einer Auskunftsverweigerung führen. Auch können dem Träger im Einzelfall konkrete Anhaltspunkte vorliegen, die — beispielsweise wegen einer sich abzeichnenden Gefährdung des Informanten — eine Geheimhaltung seiner Daten gebieten. Ich bin jedoch der Meinung, daß das Interesse des Betroffenen an der Auskunft dann nicht zurücktreten muß, wenn ausreichende Anhaltspunkte dafür vorliegen, daß der Informant die Behörde wider besseres Wissen oder leichtfertig falsch informiert hat. Hierbei lehne ich mich an die Rechtsprechung des Bundesverwaltungsgerichtes (BVerwGE 89, 14) zu der Frage der Benennung eines Informanten für den Bundesgrenzschutz an.

In meinem 12. Tätigkeitsbericht (S. 63) habe ich dargestellt, wie mit anonym eingegangenen Anzeigen verfahren werden sollte. Der Bundesminister für Arbeit und Sozialordnung hat mir hierzu mittlerweile das von der Bundesanstalt für Arbeit jetzt angewandte Verfahren mitgeteilt, aus dem ich insbesondere die folgenden beiden Punkte hervorheben möchte:

a) Für den Fall erwiesener Unrichtigkeit einer anonymen Anzeige wird mit Zustimmung des Leistungsbeziehers die Anzeige aus dem Vorgang entfernt.

b) Anonyme Anzeigen werden auch dann entfernt, wenn sich ihre Richtigkeit mit aktuell verfügbaren Mitteln nicht abschließend klären läßt.

Dies entspricht meinen Vorschlägen.

10.7 Zweckbindung übermittelter Sozialdaten nicht beachtet

Eine arbeitslose Bürgerin hat sich darüber beschwert, daß eine Industrie- und Handelskammer (IHK) ihre Sozialdaten für eigene Zwecke (Löschung eines Berufsausbildungsvertrages im Ausbildungsberuf Datenverarbeitungskauffrau) verwendet hat. Diese Daten hatte die IHK aus der Anfrage eines Arbeitsamtes erfahren, mit der dieses klären wollte, ob es Arbeitslosenhilfe zu zahlen hatte.

Die zweckfremde Verwendung der Daten verstößt gegen § 78 SGB X. Über diese Bewertung bin ich mir mit dem Landesbeauftragten für den Datenschutz NordrheinWestfalen, an den ich die Eingabe zuständigkeitshalber abgegeben hatte, einig.

Ich habe den Einzelfall zum Anlaß genommen, das BMA zu bitten, den Leistungsträgern und ihren Verbänden zu empfehlen, bei Übermittlung von Sozialdaten den Empfänger besonders auf die Zweckbindung nach § 78 SGB X hinzuweisen.

Das BMA will dem mit folgenden Einschränkungen nachkommen:

— Eine Belehrung von Behörden, Rechtsanwälten oder Berufsverbänden ist im Regelfall nicht erforderlich, da diese genügend eigene Rechtskenntnisse haben.

— Keine Belehrungspflicht besteht, wenn der Leistungsträger einen Arzt beauftragt, da dieser nach § 203 Abs. 1 Nr. 1 StGB ohnehin schweigepflichtig ist und damit § 78 SGB X für sein Verhalten keine Rolle spielt.

— Keine Belehrung ist ferner zu erteilen, wenn der Betroffene in die Nutzung seiner Daten beim Empfänger eingewilligt hat, weil der Leistungsträger nicht beurteilen kann, auf welche Nutzung der Daten sich die Einwilligung erstreckt.

Einig bin ich mit dem BMA, daß

— ein Hinweis auf § 78 SGB X dann notwendig ist, wenn der Leistungsträger im Einzelfall Daten an nicht institutionell gebundene Privatpersonen offenbart, z. B. bei der Unterrichtung über Unterhaltsansprüche, Pfändungsgläubiger etc. und

— der Hinweis auf § 78 SGB X an einen Datenempfänger unabhängig von den obigen Ausführungen stets dann zu erfolgen hat, wenn konkrete Anhaltspunkte dafür bestehen, daß der Empfänger seine Pflichten nicht kennt oder vernachlässigt.

Ich sehe in der Haltung des BMA einen Fortschritt und werde die Auswirkungen in der Praxis kontrollieren. Zu einzelnen Punkten besteht allerdings noch Erörterungsbedarf.

10.8 Erfüllt der Sozialversicherungsausweis seinen Zweck?

Aus verschiedenen Presseartikeln in jüngster Zeit habe ich entnommen, daß Zweifel aufgetreten sind, ob der Zweck des Sozialversicherungsausweises, illegale Beschäftigungsverhältnisse aufzudecken und Leistungsmißbrauch zu verhindern, erreicht werden kann (s. auch 13. TB S. 93 Nr. 35). In erster Linie wird vorgebracht, beim Verlust eines Ausweises werde nach § 96 Abs. 2 SGB IV ohne weiteres ein neuer ausgestellt. Dies führe dazu, daß viele Versicherte über mehrere Sozialversicherungsausweise verfügten, womit sich Mißbrauchsmöglichkeiten ergäben. Auf Antrag wird nämlich ein neuer Sozialversicherungsausweis ausgestellt, wenn der alte zerstört, abhanden gekommen oder unbrauchbar geworden ist.

Ich bin daraufhin an den Bundesminister für Arbeit und Sozialordnung mit der Bitte um eine Stellungnahme herangetreten, welche Meinung er zu diesem Vorbringen vertritt und gegebenenfalls welche Maßnahmen er zu ergreifen denkt. Er hat mir mitgeteilt, daß er zwar die Presseberichterstattung für teilweise übertrieben und unqualifiziert hält, in der Mehrfachausstellung von Sozialversicherungsausweisen aber durchaus ein Problem sieht. Insbesondere bei den geringfügig Beschäftigten ist es offenbar zu mißbräuchlichen Ausstellungen mehrerer Sozialversicherungsausweise gekommen. Verschiedene so Beschäftigte haben mehreren Arbeitgebern durch Vorlage jeweils eines Sozialversicherungsausweises suggeriert, das Beschäftigungsverhältnis sei das einzige und damit sozialversicherungsfrei. Die Arbeitgeber werden später aber zur Beitragszahlung herangezogen, wenn sich durch die Zusammenrechnung der Beschäftigungen die Versicherungs- und Beitragspflicht ergibt.

Als eine Möglichkeit der Mißbrauchsbekämpfung wird vom BMA die fortlaufende Numerierung der Sozialversicherungsausweise beim jeweiligen Inhaber angeführt. Sie würde die Arbeitgeber zu einer sorgfältigeren Prüfung veranlassen. Die Frage ist allerdings, ob damit nicht ein personenbezogenes Datum aufgenommen und damit der Grundsatz verletzt wird, daß die auf dem Sozialversicherungsausweis ausgewiesene fortlaufende Vordrucknummer keine Angaben über den Ausweisinhaber enthalten darf.

Ergänzend habe ich dem BMA eine Regelung in Anlehnung an das Paßgesetz vorgeschlagen. Um kontrollieren zu können, was aus einem ausgegebenen Paß geworden ist, hat der Gesetzgeber den Inhaber nicht nur (wie in § 96 Abs. 2 SGB IV) verpflichtet, einen unbrauchbar gewordenen Paß zurückzugeben, sondern auch bestimmt, den Verlust eines Passes und sein Wiederauffinden anzuzeigen. Verstöße gegen diese Pflicht sind als Ordnungswidrigkeit eingestuft.

Mein Vorschlag ist inzwischen in den Entwurf eines Gesetzes zur Umsetzung des Föderalen Konsolidierungsprogramms aufgenommen worden.

10.9 Drei Sozialversicherungsträger wollen eine gemeinsame Datei — Zum Agrarsozialreformgesetz 1994 —

Die Organisation der landwirtschaftlichen Sozialversicherung weist insofern eine Besonderheit auf, als sie die landwirtschaftliche Alterskasse, die landwirtschaftliche Krankenkasse und die landwirtschaftliche Berufsgenossenschaft in einer Verwaltungsgemeinschaft zusammenfaßt. Daraus ergeben sich besondere datenschutzrechtliche Probleme (s. auch 12. TB S. 61). Seit kurzem liegt ein Entwurf eines Gesetzes zur Reform der agrarsozialen Sicherung (Agrarsozialreformgesetz 1994 — ASRG 1994 —) vor, der sich auch dieser Fragen zumindest teilweise annimmt.

In die Beratung dieses Gesetzentwurfes wurde ich frühzeitig einbezogen und konnte so auf die nachfolgend dargestellten datenschutzrechtlichen Bestimmungen Einfluß nehmen:

— In das Gesetz über die Alterssicherung der Landwirte (ALG) soll eine Regelung aufgenommen werden, wonach die drei Träger der landwirtschaftlichen Sozialversicherung personenbezogene Daten in einer *gemeinsamen* Datei verarbeiten dürfen, soweit die Daten jeweils zu ihrer

Aufgabenerfüllung erforderlich sind. Durch technische und organisatorische Maßnahmen ist sicherzustellen, daß die in dieser Datei enthaltenen personenbezogenen Daten der Versicherten den Beschäftigten der einzelnen Sozialversicherungsträger nur im jeweils erforderlichen Umfang zugänglich sind.

Aus datenschutzrechtlicher Sicht besonders erfreulich ist der Hinweis auf § 76 SGB X, wonach Daten, die der ärztlichen Schweigepflicht unterliegen, nur unter eingeschränkten Bedingungen an andere Träger der Sozialversicherung weitergegeben werden dürfen.

— Die landwirtschaftlichen Alterskassen dürfen für ihre Mitglieder eine Mitgliedsnummer vergeben. Es konnte Einigkeit erreicht werden, daß die personenbezogenen Merkmale, welche diese Mitgliedsnummer enthalten darf, abschließend in den Gesetzentwurf aufgenommen werden. Welche Merkmale dies im einzelnen sein werden, ist noch umstritten. Wegen der spezifischen Situation der landwirtschaftlichen Sozialversicherung als Verwaltungsgemeinschaft habe ich mich — anders als in der übrigen Sozialversicherung — damit einverstanden erklärt, daß die drei Träger der landwirtschaftlichen Sozialversicherung für jeden Versicherten die gleiche Nummer vergeben dürfen. Nicht zulässig ist es jedoch, die Renten- oder Krankenversicherungsnummer als einheitliche Nummer zu verwenden. Damit wird der Gleichklang mit der Sozialversicherung im übrigen gewahrt.

Eine weitere Vorschrift des Entwurfes normiert den Grundsatz, daß die Verarbeitung oder Nutzung personenbezogener Daten in Dateien nur zulässig ist, soweit dies zur Erfüllung einer der landwirtschaftlichen Alterskasse gesetzlich zugewiesenen Aufgabe erforderlich ist.

Dem BMA soll eine Verordnungsbefugnis eingeräumt werden, auf Grund derer er die Datenverarbeitung bei den landwirtschaftlichen Alterskassen, insbesondere den Umgang mit der Mitgliedsnummer, näher regeln kann. Diese Verordnungsbefugnis entspricht der Regelung in § 152 SGB VI, der u. a. bestimmt, an welche Personen die Mitgliedsnummer zu vergeben ist, wie diese Nummer zusammengesetzt ist, wie das Versicherungskonto zu führen ist, welche Daten es enthalten darf und wann Daten und Versicherungsunterlagen gelöscht werden dürfen.

— Die datenschutzrechtlichen Bestimmungen lehnen sich im übrigen weitgehend an den Zweiten Abschnitt des SGB VI an, der Vorschriften über den Datenschutz in der gesetzlichen Rentenversicherung enthält (§§ 147 ff. SGB VI) oder erklären diese mittels ausdrücklicher Verweisung für entsprechend anwendbar.

Ich erwarte, daß der Entwurf bald verabschiedet wird. Das Gesetz ist für die Gewährleistung des Datenschutzes bei der landwirtschaftlichen Sozialversicherung dringend erforderlich.

11 Arbeitsverwaltung

11.1 Schärfere Kontrolle von Leistungsbeziehern der Bundesanstalt für Arbeit

Zur Bekämpfung von Schwarzarbeit und Leistungsmißbrauch führt die Bundesanstalt für Arbeit (BA) bei Betrieben Außenprüfungen auf der Grundlage des § 132 a AFG durch. In welchem Umfang dabei personenbezogene Daten erhoben und verarbeitet werden dürfen, wirft datenschutzrechtliche Probleme auf (vgl. 12. TB S. 64 f.). Das BMA macht geltend, Außenprüfungen der BA seien nur effizient, wenn sie umfassend prüfen könne; dazu gehöre auch das automatisierte Abgleichen von Dateien der Beschäftigten eines überprüften Betriebes mit Dateien der Bundesanstalt für Arbeit (s. 13. TB S. 93).

Das BMA hat plausibel vorgetragen, daß es notwendig ist, Meldungen der Arbeitgeber an die BA über Beginn, Unterbrechungen und Ende von Beschäftigungen mit den der Arbeitsverwaltung bekannten Daten über Leistungsbezugszeiten computergestützt abzugleichen. Allerdings sind hierfür gesetzliche Bestimmungen, insbesondere über Art und Umfang der bei Außenprüfungen zu erhebenden Daten, erforderlich. Die der Bundesanstalt zustehenden Befugnisse sowie die Rechte der betroffenen Personen müssen gesetzlich festgelegt sein. Im Rahmen einer Novellierung des § 132 a AFG wurden meine Anregungen berücksichtigt.

Wichtig für mich war, den durch den Datenabgleich verursachten Eingriff in die Rechtsposition von ggf. Millionen völlig unverdächtigen Versicherten so gering wie möglich zu gestalten.

Folgende datenschutzrechtliche Regelungen wurden im Interesse der Versicherten in das Gesetz aufgenommen:

— Im Rahmen von Außenprüfungen nach § 132 a AFG dürfen von der Bundesanstalt grundsätzlich nur solche Daten erhoben werden, die zur Feststellung erforderlich sind, ob in dem Betrieb jemand gearbeitet und gleichzeitig Arbeitslosengeld beantragt oder bezogen hat und ob die Angaben in der Arbeitsbescheinigung nach § 133 AFG zutreffend bescheinigt sind.

— Die für diesen Zweck erforderlichen Daten wurden abschließend festgelegt: Familien- und Vornamen, Geburtsdatum, Versicherungsnummer und Anschrift des Arbeitnehmers oder Selbständigen sowie Beginn, Ende, Entgelt und Arbeitszeit der Beschäftigung oder Tätigkeit.

— Die so erhobenen Daten unterliegen einer strikten Zweckbindung. Sie dürfen nur verarbeitet und genutzt werden, um Leistungsmißbrauch aufzudecken und zu verfolgen und um Beitragsansprüche, die bei der Außenprüfung bekannt werden, geltend zu machen und einzuziehen.

— Hat der Arbeitgeber die erforderlichen Daten in automatisierten Dateien gespeichert, so hat er sie in der Regel auf Verlangen und auf Kosten der BA aus den Datenbeständen auszusondern und der BA

zur Verfügung zu stellen. Nur wenn diese Aussonderung mit einem unverhältnismäßigen Aufwand verbunden wäre, darf er maschinenlesbare Datenträger oder Listen, die neben den erforderlichen Daten auch andere Daten enthalten — also ungesondert — zur Verfügung stellen, soweit nicht im Einzelfall überwiegende schutzwürdige Belange der Betroffenen entgegenstehen. Dabei obliegt es nicht der Entscheidung der BA, sondern der des Arbeitgebers, ob die Aussonderung der Daten für ihn einen unverhältnismäßigen Aufwand darstellt.

— Werden die Daten ungesondert zur Verfügung gestellt, dürfen die überschüssigen Daten weder verarbeitet noch genutzt werden.

— Nach Erreichen des mit der Maßnahme verfolgten Zwecks sind die Daten oder Datenträger unverzüglich zu vernichten oder dem Arbeitgeber auf sein Verlangen zurückzugeben.

— Außenprüfungen dürfen nur durch einen besonders ermächtigten Mitarbeiter der Arbeitsverwaltung angeordnet werden.

Künftig kann die Bundesanstalt für Arbeit in Betrieben mit ausländischen Arbeitnehmern auch prüfen, ob diese im Rahmen ihrer Arbeitserlaubnis und auch nicht zu ungünstigeren Arbeitsbedingungen als deutsche Arbeitnehmer beschäftigt werden (§ 19 a AFG). Die vorstehenden datenschutzrechtlichen Regelungen gelten entsprechend (§ 19 a i.V.m. § 132 a AFG).

Nach Angaben des BMA erhalten derzeit rd. 55 000 Personen Versorgungsleistungen aus Sonderversorgungssystemen der ehemaligen DDR. Um etwaige unbegründete Doppelleistungen durch die Bundesanstalt für Arbeit zu erkennen, wurde ein Datenaustausch zwischen der letzteren und den zuständigen Trägern der Sonderversorgungssysteme oder der Bundesversicherungsanstalt für Angestellte nach der neu gefaßten Verordnung über das Ruhen von Lohnersatzleistungen nach dem Arbeitsförderungsgesetz bei Zusammentreffen mit Versorgungsleistungen der Versorgungssysteme (§ 2 der Verordnung) festgelegt. Dieser Datenaustausch ist in den neuen Ländern notwendig, weil die Arbeitsverwaltung dort die erforderlichen Daten in der Übergangsphase nicht — wie sonst üblich — bei der Arbeitslosmeldung erhoben hat. Der Austausch darf nur einmal erfolgen und zwar innerhalb von sechs Monaten nach Inkrafttreten der Verordnung.

11.2 Computerviren in automatisierten Dateien der Arbeitsverwaltung im Beitrittsgebiet

Mich interessierte, wie im Bereich der Sozialversicherung datenschutzrechtliche Probleme und Fragen in den fünf neuen Bundesländern behandelt, gelöst und beantwortet werden. Ich habe daher Informations- und Kontrollbesuche in den Arbeitsämtern Stralsund und Berlin VI (Ost) durchgeführt.

Im Arbeitsamt Stralsund haben sich bei der Kontrolle der Bereiche Arbeitsvermittlung und Arbeitsberatung, der Leistungsabteilung und der Poststelle keine gravierenden datenschutzrechtlichen Defizite ergeben, die sich aus der konkreten Situation eines Arbeitsamtes in den neuen Ländern herleiten ließen. Problematisch waren auch dort Fragen, die den gesamten Bereich der Bundesanstalt für Arbeit betreffen. Beispiele hierfür sind, daß jeder Stellenbewerber allgemein nach schwebenden Straf- und Ermittlungsverfahren (allerdings auch nach herausgehobenen Funktionen im System der ehemaligen DDR) befragt wird. Der Umfang der Unterlagen in den Leistungsakten ist auch dort zu groß und damit für die Aufgabenerfüllung der Arbeitsverwaltung nicht erforderlich. Ich werde weiter versuchen, mit der Bundesanstalt für Arbeit einvernehmliche Lösungen über diese Fragen zu finden.

Ein Problem, das mir bei der Kontrolle auffiel, möchte ich hier jedoch näher darstellen:

Die Prüfung einer von den Vermittlungsabteilungen der Bundesanstalt für Arbeit bundesweit verwandten Stellenangebotskarte — ein allgemeines Formular, auf dem freie Stellen eingetragen werden — ergab, daß dort erfragt wird, ob ein Arbeitgeber „nicht, auch oder nur" an einer Vermittlung von ausländischen Arbeitskräften interessiert ist. Diese generelle Fragestellung bringt — übrigens nicht nur für Ausländer, sondern auch für Deutsche — die Gefahr einer Diskriminierung mit sich.

Die in der Stellenangebotskarten aufgelisteten Fragen beantwortete der Arbeitgeber dem Vermittler meist telefonisch oder mündlich; die Antworten waren grundsätzlich freiwillig. Durch ein routinemäßig bedingtes, schematisches Abfragen seitens der Vermittler konnte jedoch bei den Arbeitgebern der Eindruck erweckt werden, sie müßten die Fragen ausnahmslos beantworten. Aus Gesprächen mit Vermittlern des Arbeitsamtes Stralsund war zu schließen, daß diese Einschätzung der Verpflichtung zur Antwort dort ausgeprägt war. Die — häufig erst kurzzeitig im Bereich der Arbeitsverwaltung tätigen — Vermittler orientierten sich in der Regel sehr genau an dem vorgegebenen Fragenkatalog der Stellenangebotskarte, der auch an keiner Stelle auf die Freiwilligkeit der Antworten hinwies. Den Arbeitgebern wurde so der Eindruck vermittelt, die Bearbeitung ihres Stellenangebots hinge von einer lückenlosen Beantwortung der Fragen der Stellenangebotskarte ab.

Das sich aus dem geschilderten Verfahren ergebende Problem konnte inzwischen erfreulicherweise im Einvernehmen mit der Bundesanstalt für Arbeit wie folgt gelöst werden. Bei der Entgegennahme von Stellenangeboten durch die Vermittlungsfachkräfte der BA wird nicht mehr *initiativ* gefragt, ob ausländische Arbeitnehmer/-innen nicht, auch oder nur eingestellt werden. Nimmt ein Betrieb von sich aus Einschränkungen vor, ist seitens der Vermittlungskräfte möglichst auf eine Rücknahme solcher Einschränkungen hinzuwirken und zu empfehlen, freie Arbeitsstellen ausschließlich unter dem Gesichtspunkt der Eignung für die auszuführende Tätigkeit zu beschreiben. Erst

wenn der Betrieb ausdrücklich nicht bereit ist, eine solche Einschränkung zurückzunehmen, sind die entsprechenden Daten in der Stellenangebotskarte zu erfassen. Für die schriftliche Mitteilung eines Stellenangebotes durch den Arbeitgeber ist ein neuer Vordruck „Vermittlungsauftrag" vorgesehen, der Angaben zur Nationalität nicht mehr vorsieht.

Im Jahre 1991 hatte ich die Information erhalten, daß beim Aufbau der Arbeitsämter in den neuen Bundesländern die vorübergehend — bis November 1991 — eingerichtete „Zentrale Arbeitsverwaltung" virenverseuchte APC aus der DDR-Produktion (Robotron-Werke) einsetze.

Die Bundesanstalt für Arbeit teilte mit, eine Überprüfung sämtlicher APC in den Arbeitsämtern der neuen Bundesländer und in der Dienststelle der „Zentralen Arbeitsverwaltung" hätte diesen Verdacht bestätigt. Dort seien Computerviren entdeckt worden, die vermutlich durch das unerlaubte Benutzen von Programmen einschleust worden waren. Befallen waren ausschließlich Programme. Datenverluste oder -verfälschungen konnten nicht nachgewiesen werden. Die BA hat mir mitgeteilt, alle befallenen Programme seien mit einem Virenbeseitigungsprogramm behandelt worden, sie seien weiter verwendbar.

Die „Zentrale Arbeitsverwaltung" hat die Verwendung von APC durch eine Rundverfügung geregelt. Gleichzeitig hat das zuständige Fachreferat der Hauptstelle der BA den Fachabteilungen ein Sicherheitskonzept für den Einsatz ihrer Verfahren auf APC in den neuen Bundesländern zur Verfügung gestellt hat.

Aufgrund der in diesem Sicherheitskonzept vorgesehenen Maßnahmen, insbesondere des Einsatzes einer Sicherheitssoftware, halte ich aus datenschutzrechtlicher Sicht — zumindest vorübergehend — den Einsatz der vorgenannten APC für die Aufgabenerfüllung der Arbeitsämter in den neuen Bundesländern weiterhin für vertretbar. Hierbei habe ich insbesondere auch berücksichtigt, daß nach Auskunft der BA die von der „Zentralen Arbeitsverwaltung" beschafften APC aus der Produktion der Robotron-Werke zwar noch in nahezu allen Arbeitsämtern der neuen Bundesländer im Einsatz sind, dabei aber in aller Regel nur der Textverarbeitung und der Unterstützung von statistischen Erhebungen und Auswertungen dienen. Außerdem handelt es sich um eine Übergangslösung. Die Verwendung dieser APC wird in den Arbeitsämtern — so die BA — mit dem bereits begonnenen Einsatz von zentral vorgegebenen Anwendungen in den nächsten zwei Jahren überwiegend entbehrlich werden.

Im Rahmen einer Datenschutzkontrolle im Arbeitsamt Berlin VI konnte ich festgestellen, daß die Hauptvermittler der Abteilung „Arbeitsvermittlung" dort ihre Beratungs- und Vermittlungstätigkeit unter optimalen Datenschutzbedingungen in Einzelzimmern wahrnehmen können. Auch das in dieser Abteilung installierte manuelle Nummern- Aufrufsystem gewährleistet die Anonymität der Arbeitsuchenden (s. auch 11. TB S. 53, 12. TB S. 63f.).

11.3 Verdeckte Kennzeichnung als Alkoholiker beseitigt — Computerunterstützte Arbeitsvermittlung („coArb") —

Das von der Bundesanstalt für Arbeit (BA) genutzte Verfahren der computerunterstützten Arbeitsvermittlung „coArb" hat mich weiterhin beschäftigt (s. 13. TB S. 63f.), vor allem wegen der Speicherung von Beratungsvermerken mit negativen Aussagen und der technisch bedingten Unmöglichkeit, solche Daten zu löschen, worüber sich Arbeitssuchende bei mir beschwerten.

Ich habe das Verfahren erneut kontrolliert und dazu, zusammen mit Vertretern der BA, auch drei Arbeitsämter besucht.

Die Erhebung und Speicherung personenbezogener Daten für die Arbeitsvermittlung und -beratung sind — soweit es um das angesprochene Problem geht — in einem bundesweit geltenden Runderlaß der BA mit folgendem Wortlaut grundsätzlich datenschutzgerecht geregelt:

> „Auf das Verbot einer negativen Kennzeichnung von Arbeit- und Ratsuchenden wird hingewiesen. Ebenso sind unbewiesene oder nicht beweisbare Tatsachen nicht zu erheben und zu speichern. Insbesondere sind auch bloße subjektive Eindrücke und Bewertungen nicht . . . festzuhalten."

Das Problem liegt in der Umsetzung dieses Runderlasses in der Praxis.

Für eine erfolgreiche Vermittlung benötigt die BA einerseits ein Mindestmaß an Daten. Andererseits muß sich der Umfang dieser Daten jedoch auf das für die Aufgabenerfüllung notwendige Maß beschränken.

Die Kontrolle von etwa 450 Beratungsvermerken ergab, daß sich die Praxis im Vergleich zu früher zwar erheblich verbessert hat, aber doch noch gewisse Mängel aufweist, wie folgende Beispiele zeigen:

— In einem Fall fiel im Bemerkungsfeld einer Erfassungsmaske die Kennzeichnung „YYY" auf. Die Vertreter der Arbeitsverwaltung erklärten, damit würden intern in der Kurzfassung des Bewerberangebotes Alkoholismusfälle gekennzeichnet. Hierbei stünden die „YYY" symbolisch für Sektkelche; sie wiesen auf Alkoholismus hin. Diese Kennzeichnung wurde jedoch nicht von allen Vermittlern verwendet.

  Die BA hat mir bestätigt, daß die Verwendung verdeckter Kennzeichen als „Hinweis auf Alkoholismus" keinesfalls zulässig ist und zugesichert, daß das verantwortliche Arbeitsamt künftig die hierzu gegebene interne Weisungslage beachten wird. Das durch „YYY" gekennzeichnete Bewerberangebot wurde entsprechend korrigiert, „YYY" wurde gelöscht.

— Über eine Arbeitssuchende war vermerkt:

  „Anruf des Ehemannes. Frau X wurde heute früh in das Krankenhaus eingeliefert. Hat das Kind

verloren, Schwangerschaft ist nicht mehr gegeben . . ."

Hier hätte nur die Beendigung der Schwangerschaft vermerkt werden dürfen.

— Der Vermerk

„Hat Arbeitsverhältnis bei der Firma X beendet, da sie sich aufgrund einer Totaloperation im Februar 1991 gesundheitlich überfordert fühlte. Nunmehr an baldiger Arbeitsaufnahme interessiert"

hätte ohne das sensible Datum „Totaloperation" erfolgen können und müssen.

Dieser Vermerk hat im übrigen nicht dazu geführt, ein ärztliches Gutachten zur Vermittlungsmöglichkeit der Kundin zu veranlassen. Nach Aussagen des zuständigen Vermittlers waren die mündlichen Angaben der Betroffenen glaubwürdig. Er habe ohne Einschaltung des Ärztlichen Dienstes ihre Einsatzmöglichkeiten beurteilen können.

— Problematisch erschien mir auch folgender Beratungsvermerk über eine ausländische Arbeitssuchende:

„Frau Y (ehemalige Arbeitgeberin) hat sich sehr positiv über Frau X (Arbeitssuchende) geäußert; würde sie auch gerne einstellen, da Frau X schon einmal bei ihr gearbeitet hat, wird jedoch als Ausländerin von der Kundschaft abgelehnt, kann sich das als Arbeitgeberin nicht leisten."

Hierzu legte die Vermittlerin dar, die Wiedergabe der Erklärungen der ehemaligen Arbeitgeberin sei erforderlich gewesen, um klarzustellen, daß die Entlassung der Arbeitssuchenden nicht aus fachlichen Gründen erfolgt ist.

Ich habe mit der BA vereinbart, demnächst über derartige Fälle zu sprechen und Lösungsmöglichkeiten zu suchen, die dem Persönlichkeitsrecht jedes einzelnen gerecht werden. Soweit die BA dann nicht darlegen kann, aus welchen Gründen diese und vergleichbare Eintragungen für ihre Vermittlungstätigkeit erforderlich sind, werde ich deren Löschung fordern (§ 84 SGB X).

Das System „coArb" ist so programmiert, daß Inhalte einzelner Beratungsvermerke nicht gelöscht werden können, sondern es ist nur vorgesehen, gegebenenfalls Korrekturvermerke zu speichern oder — in Ausnahmefällen — das gesamte Bewerberangebot zu löschen und anschließend verändert neu einzugeben. Diese Regelung halte ich seit langem für problematisch. § 84 SGB X gebietet nämlich — anders als das Bundesdatenschutzgesetz — Daten zu löschen, wenn die speichernde Stelle die Daten nicht mehr für ihre Aufgabenerfüllung benötigt und schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Ein Beispiel soll das Anliegen bestärken. Bei einem seit mindestens dreizehn Jahren arbeitslosen Bewerber war noch aus dem Jahre 1983 vermerkt

„Herr X ist äußerst unschlüssig. Für ihn wäre eine Bildungsmaßnahme nicht nur bezüglich des Lerninhaltes notwendig, sondern auch, um sich zu stabilisieren",

obwohl der Inhalt dieses Vermerkes auch für die zuständige Hauptvermittlerin keinerlei aktuelle Entscheidungsrelevanz mehr besaß.

Ich habe der BA empfohlen, die Speicherung von Eintragungen in den Beratungsvermerken auf die zur Aufgabenerfüllung relevanten und damit zulässigen Informationen zu beschränken und wie — in anderen Erfassungsmasken auch — so zu gestalten, daß Eintragungen jederzeit von den Vermittlern/Vermittlerinnen verändert und gelöscht werden können.

Ich gehe davon aus, daß ich auch hierzu gemeinsam mit der Bundesanstalt für Arbeit eine datenschutzgerechte Regelung erreichen werde.

11.4 Pflicht zur Offenbarung von Einkommensdaten Unterhaltsverpflichteter deutlich eingeschränkt

Unterhaltsverpflichtete haben sich häufig dagegen gewandt, daß ihr Einkommen im Rahmen eines Arbeitslosenhilfeverfahrens einem Unterhaltsberechtigten detailliert offenbart wurde (vgl. 13. TB S. 93). Die Bundesanstalt für Arbeit verzichtet jetzt auf die genaue Ermittlung des Einkommens eines unterhaltsverpflichteten Angehörigen, wenn dieser durch einen Steuerbescheid oder eine Bescheinigung seines Steuerberaters darlegt, daß aufgrund der Höhe seines Einkommens Arbeitslosenhilfe an den Unterhaltsberechtigten nicht zu zahlen ist. Auch wenn sich jemand nur arbeitslos meldet, um die Anrechnung für die Rentenversicherung zu sichern, sind Einkommensangaben entbehrlich.

Nach dem Außerkrafttreten des § 137 Abs. 1a AFG zum 31. Dezember 1991 sind bei der Arbeitslosenhilfe im Rahmen der Bedürftigkeitsprüfung keine „fiktiven" Unterhaltsansprüche mehr zu berücksichtigen. Dies vermindert erfreulicherweise die Zahl der Fälle — und gerade die problematischen —, in denen Unterhaltspflichtige überhaupt zu Auskunft über ihr Einkommen verpflichtet sind. Insoweit hat sich das von mir aufgezeigte Problem deutlich entschärft.

Zur Frage, inwieweit der auf dem Rechtsstaatsprinzip beruhende Rechtsschutzgedanke eine routinemäßige Offenlegung bereits im Leistungs- und nicht erst im Widerspruchsbescheid erfordert, haben mir BMA und BMJ mitgeteilt, daß diese Offenlegung im Interesse einer umfassenden Überprüfungs- und Verteidigungsmöglichkeit des Unterhaltsberechtigten bereits im Ausgangsverfahren erforderlich ist. Dies muß hingenommen werden.

11.5 Ärztlicher Dienst der Bundesanstalt für Arbeit

11.5.1 Ärztliche Untersuchung und Begutachtung gegen den Willen eines Arbeitssuchenden

Ein Petent wandte sich gegen das Vorgehen eines Arbeitsamtes im Zusammenhang mit der Erstellung eines arbeitsamtsärztlichen Gutachtens. Hintergrund der Eingabe war eine im Jahre 1985 durchgeführte

arbeitsamtsärztliche Untersuchung. Aufgrund des Untersuchungsergebnisses wurde der Petent aufgefordert, Maßnahmen zur beruflichen Rehabilitation zu beantragen. Nachdem er dieser Aufforderung nicht Folge geleistet hatte, stellte das Arbeitsamt seine Zahlungen an den Betroffenen ein. Nach Meinung des Arbeitsamtes bestanden wegen Verhaltensauffälligkeiten Zweifel an der Verfügbarkeit des Petenten für die Arbeitsvermittlung. Seitens der Bundesanstalt wurde sogar angenommen, daß auch eine Gefährdung von Angestellten beim Umgang mit dem Petenten nicht auszuschließen sei. Er wurde mehrfach zur Durchführung einer ärztlichen und psychologischen Untersuchung aufgefordert, was er stets ablehnte. Durch ein persönlich gehaltendes Schreiben des Medizinischen Dienstes des Arbeitsamtes gelang es schließlich, den Petenten zu einer Vorsprache beim Medizinischen Dienst zu bewegen. In dem Schreiben unterblieb offenbar bewußt ein Hinweis darauf, daß bei dem Besuch des Petenten eine nervenärztliche Untersuchung vorgesehen war. Dieser Schluß muß aus einem Schreiben gezogen werden, das der Medizinische Dienst des Arbeitsamtes an den Leiter des Ärztlichen Dienstes der Bundesanstalt über das beabsichtigte Vorgehen richtete.

Tatsächlich wurde der Petent dann von dem zur Besprechung des Petenten mit der Arbeitsamtsärztin hinzukommenden Nervenarzt untersucht, ohne daß der Betroffene diesen Vorgang als nervenärztliche Untersuchung erkennen konnte. Der Nervenarzt erstattete anschließend ein mehrseitiges Gutachten.

Zur Rechtfertigung dieses Vorgehens hat die BA vorgetragen, daß sie von dem dringenden Verdacht ausgegangen sei, der Petent sei psychisch erkrankt, deswegen nicht mehr leistungsfähig und damit für die Arbeitsvermittlung nicht mehr verfügbar. Sie habe damit dem Petenten den weiteren Bezug von Sozialhilfe ersparen und ihm einen Rentenbezug ermöglichen wollen. Aus der langjährigen Erfahrung in der Zusammenarbeit mit den Rentenversicherungsträgern ergebe sich jedoch, daß deren ärztliche Dienste einen sehr hohen Maßstab an die ärztlichen Unterlagen legten. Um die Erfolgsaussichten des Petenten bei der Rentengewährung zu erhöhen, habe sich die BA zu dem Versuch entschlossen, den Petenten zu einer ärztlichen Untersuchung einzuladen. Es sei Ausdruck des sozialen Engagements der BA gewesen, daß sie die Einladung zu einer ärztlichen Untersuchung nicht in einem unpersönlichen Formblatt, sondern in einem persönlichen Brief ausgesprochen hat.

Die hier praktizierte Erhebung der nervenärztlichen Befunddaten des Petenten habe ich gemäß § 25 BDSG als einen Verstoß gegen Artikel 6 der Datenschutzkonvention des Europarates, des § 14 Abs. 2 und des § 27 Abs. 2 AFG und des § 1a der Berufsordnung für die Deutschen Ärzte beanstandet.

Nach Artikel 6 der von der Bundesrepublik Deutschland ratifizierten Datenschutzkonvention des Europarates müssen Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden. Die Vorgehensweise der BA gegenüber dem Petenten widerspricht dem Grundsatz von Treu und Glauben. Sie war insofern unrechtmäßig, als die nervenärztliche Untersuchung ohne die Einwilligung und sogar gegen den ausdrücklich erklärten Willen des Petenten erfolgte. Diese Beurteilung ergibt sich auch aus § 1a der Berufsordnung für die deutschen Ärzte; dort ist festgelegt, daß der Arzt das Selbstbestimmungsrecht des Patienten zu achten hat und zu jeder Behandlung der Einwilligung des Patienten bedarf. Der Einwilligung hat grundsätzlich eine Aufklärung im persönlichen Gespräch vorauszugehen.

Das vom Arbeitsamt angewandte Verfahren verstieß auch eindeutig gegen § 14 des Arbeitsförderungsgesetzes, der in Absatz 2 ausdrücklich bestimmt, daß die Bundesanstalt im Rahmen der Arbeitsvermittlung Arbeitssuchende nur mit deren Einverständnis ärztlich untersuchen und begutachten darf. Die allgemeine Geltung des Grundsatzes wird durch § 27 des Arbeitsförderungsgesetzes bestätigt.

Eine gültige Einwilligung, die hier nicht vorlag, hätte eine ausreichende Aufklärung vorausgesetzt. Eine solche ist ebenfalls nicht erfolgt.

Auch beim Petitionsausschuß des Deutschen Bundestages, der sich mit dem Vorgang befaßt hat, ist das Vorgehen der Bundesanstalt auf Unverständnis gestoßen. Der Ausschuß hat daher empfohlen sicherzustellen, daß zukünftig keine arbeitsamtsärztlichen Untersuchungen gegen den Willen der Leistungsempfänger durchgeführt werden. Aufgrund der Stellungnahmen der Bundesanstalt für Arbeit zu meiner Beanstandung gehe ich davon aus, daß vergleichbare Datenerhebungen im Bereich der BA zukünftig nicht mehr vorkommen. Der leitende Arzt der BA hat die Vorgänge zum Anlaß genommen, in Dienstbesprechungen und Informationen des Ärztlichen Dienstes noch einmal auf die strikt einzuhaltende, deutlich zu artikulierende und rechtzeitige Aufklärung der Arbeits- oder Ratsuchenden durch die Arbeitsamtsärzte hinzuweisen.

11.5.2 Besserer Umgang mit ärztlichen Gutachten

Mit Vertretern der BA habe ich eingehende Gespräche darüber geführt, welchen Inhalt die vom Ärztlichen Dienst oder in dessen Auftrag erstellten ärztlichen Gutachten haben sollen. Diese Gespräche führten im Ergebnis zu einer begrüßenswerten Fassung des Runderlasses der BA für die Erstellung solcher Gutachten.

Jetzt ist ausdrücklich geregelt, daß bei der Prüfung und Entscheidung, welche ärztlichen Daten der Arbeitsvermittler/-berater für seine ordnungsgemäße Aufgabenerfüllung benötigt, ein strenger Maßstab anzulegen ist. So gehören beispielsweise Anamnesedaten nicht in das ärztliche Gutachten; Gesundheitsstörungen sind laienverständlich anzugeben und auf das unbedingt notwendige Minimum zu beschränken.

Um diese Zielsetzung zu unterstützen, wurden die Formulare, die bei der Erstellung ärztlicher Gutachten verwendet werden, abgeändert und umgestaltet. Im ersten Abschnitt hat der Arzt Eintragungen — im wesentlichen in Form des Ankreuzens vorformulierter Merkmale — im Hinblick auf ein positives oder negatives Leistungsbild des Versicherten zu fertigen.

Hier ist insbesondere Stellung zu nehmen zu Fragen, welche Arbeiten der Versicherte verrichten kann (insbesondere im Hinblick auf Arbeitsschwere und Arbeitshaltung) sowie welche Arbeiten und Belastungen auszuschließen sind. Im zweiten Abschnitt, der bisher am Anfang der ärztlichen Gutachten stand, erstellt der Arzt eine ergänzende kurzgefaßte und laienverständliche Darstellung vorhandener Gesundheitsstörungen.

In dem Vordruck wird ausdrücklich darauf hingewiesen, daß die zusätzliche Beschreibung der Gesundheitsstörungen nur erforderlich ist, wenn dies für die Verständlichkeit des Leistungsbildes im Einzelfall geboten ist.

Durch entsprechende Formulargestaltung ist ferner sichergestellt, daß die Leistungsabteilungen der Arbeitsämter künftig Angaben über Gesundheitsstörungen nicht mehr erhalten, weil sie diese nicht benötigen.

Um sicherzustellen, daß bereits vorhandene Leistungsakten keine unnötigen Daten über Gesundheitsstörungen und Prognosen enthalten, hat die BA angeordnet, diese im Zuge der nächsten fachlichen Bearbeitung auf entsprechende ärztliche Angaben zu überprüfen und diese ggf. unkenntlich zu machen.

11.6 Maßnahmeträger diskriminiert Arbeitslose im Zusammenhang mit deren Umschulung und Fortbildung

Die Bundesanstalt für Arbeit (BA) schaltet freie oder gemeinnützige Einrichtungen als sogenannte Maßnahmeträger bei der Umschulung und Fortbildung von Arbeitslosen ein. Dadurch sollen die Vermittlungschancen der Teilnehmer auf dem Arbeitsmarkt verbessert werden. Teilnehmer an solchen Maßnahmen haben sich mit Beschwerden an mich gewandt:

Es wurde behauptet, die Maßnahmeträger leiteten ihre Äußerungen, Stellungnahmen und Erläuterungen zur persönlichen Situation des Arbeitslosen an die Arbeitsämter weiter und zwar ohne Kenntnis der Betroffenen, ja vereinzelt entgegen einer ausdrücklichen Zusicherung der Maßnahmeträger. Auch würden sogenannte „Sozial-Dossiers", d. h. Beurteilungen des Sozialverhaltens von Arbeitslosen erstellt und an das Arbeitsamt übermittelt. Schließlich habe das Arbeitsamt Mitarbeitern der Maßnahmeträger Einsicht in die Arbeitsamtsakten der Teilnehmer gewährt.

Eine Kontrolle in einem Arbeitsamt ergab, daß einige der von den Maßnahmeträgern über die einzelnen Teilnehmer erstellten Abschlußberichte diskriminierende Ausführungen über Arbeitslose enthielten sowie in die Persönlichkeit eingreifende psychologische Bewertungen, die über die Aufgaben eines Maßnahmeträgers hinausgehen (z. B. „Eine der schillerndsten Figuren der Maßnahme schlechthin", „Ein Desperado in Sachen Lebensplanung", „Treibgut auf dem Arbeitsmarkt", „Haarsträubende Abhängigkeit von seiner Mutter", „Exaltierter Hypochonder").

Die Aufbewahrung dieser Unterlagen in den Maßnahmeakten des Arbeitsamtes habe ich als unzulässige Datenspeicherung wegen Verstoßes gegen § 14 Abs. 1 BDSG beanstandet.

Ich verkenne nicht, daß es sinnvoll und wichtig ist, daß der Maßnahmeträger nach Beendigung der Maßnahme einen Abschlußbericht an die Arbeitsverwaltung gibt. Dabei muß sich der Maßnahmeträger aber Ausführungen über Erfolge oder Mißerfolge der Maßnahme sowie auf Fragen, die mit der Vermittlung des Arbeitslosen zusammenhängen, beschränken.

Die Bundesanstalt hat inzwischen 10 der 26 von diesem Träger durchgeführten Maßnahmen überprüft und die vorgefundenen Berichte vollständig vernichtet; die Überprüfung wird fortgesetzt. Die Bundesanstalt wird ihre weitere Zusammenarbeit mit diesem Träger überprüfen, zumal jetzt auch die Aufsichtsbehörde wegen eines Verstoßes gegen Datenschutzbestimmungen ermittelt.

In jüngster Zeit haben sich weitere Maßnahmeteilnehmer über Datenschutzverstöße beschwert, denen ich nachgehe. Dies macht es notwendig, die Einhaltung bestehender datenschutzrechtlicher Bestimmungen durch Maßnahmeträger generell besser sicherzustellen. Hierfür werde ich mich im Rahmen der Erörterungen eines Entwurfes eines 2. Änderungsgesetzes zum Sozialgesetzbuch weiterhin einsetzen. Darüber hinaus erwarte ich vom BMA, daß er sich dafür verwendet, daß der Datenschutz im Rahmen der Vertragsgestaltung zwischen Bundesanstalt für Arbeit und Maßnahmeträgern stärker berücksichtigt wird.

11.7 Bewerberdaten können ins Ausland gehen — SEDOC-Verfahren der Bundesanstalt für Arbeit —

Die deutsche Arbeitsverwaltung ist seit Juni 1980 an das „Europäische System zur Übermittlung von Stellen und Bewerberangeboten im internationalen Ausgleich" (SEDOC) angeschlossen. Ziel des Systems — als solches ein Datenübermittlungsverfahren — ist es, die Zusammenführung der Stellen- und Bewerberangebote auf EG-Ebene zu erleichtern, die gegenseitige Kenntnis der Arbeitsmärkte in diesem Rahmen zu verbessern und so Arbeitnehmern aus Ländern der Gemeinschaft gegenüber Arbeitnehmern aus dritten Staaten eine vorrangige Beschäftigung zu sichern. Mit Organisation und Durchführung des Verfahrens, die in Deutschland der Zentralstelle für Arbeitsvermittlung (ZAV) in Frankfurt übertragen wurde, habe ich mich vor Ort vertraut gemacht.

Die internen Dienstanweisungen der Bundesanstalt bestimmen, daß die Arbeitsämter die Stellen- und Bewerberangebote nur dann an die ZAV weiterleiten, wenn die Betroffenen mit der Bekanntgabe an die SEDOC-Dienststellen der anderen Gemeinschaftsländer einverstanden sind. Sofern sich eine konkrete Vermittlung anbahnt, übersendet die ZAV die ausgefüllten Formulare und in der Regel die Unterlagen des Bewerbers an die SEDOC- Partnerverwaltung, verbunden mit der Bitte, die Vermittlung einzuleiten.

Die dargestellte Offenbarung personenbezogener Daten gegenüber Personen oder Stellen im Ausland basiert auf der Einwilligung des jeweiligen Stellenbewerbers (§ 67 Nr. 1 SGB X). Auf sie allein kann sich die Bundesanstalt aber jedenfalls dann nicht zurückziehen, wenn eine datenschutzgerechte Verwendung der Unterlagen im Ausland nicht gewährleistet ist. Sie hat dann gegenüber den Stellenbewerbern eine Beratungspflicht. Dazu ist aber erforderlich, daß die zuständigen Bediensteten der ZAV die datenschutzrechtliche Situation in dem Land, in das die Daten übermittelt werden sollen, auch wirklich kennen. Datenschutzrechtliche Risiken sind insbesondere dann nicht von der Hand zu weisen, wenn die Vermittlung — wie in einigen EG-Staaten praktiziert — teilweise privaten Stellen überlassen wird. Bisher weist die ZAV den Bewerber darauf hin, daß er der Datenübermittlung an die SEDOC-Partnerverwaltung widersprechen kann, um so Aufschluß über etwaige entgegenstehende schutzwürdige Interessen im Sinne des § 77 SGB X zu erhalten.

Die Bundesanstalt für Arbeit hat mir nunmehr mitgeteilt, daß die datenschutzrechtlichen Anforderungen an das SEDOC-System durch Umorganisation der Auslandsabteilung der ZAV künftig besser berücksichtigt werden sollen. Die Vermittler sollen sich nämlich auf bestimmte Länder spezialisieren und sich dabei auch ein besonderes länderkundliches Fachwissen in bezug auf den Datenschutz aneignen. Damit bestehen bessere Voraussetzungen, Bewerber vor Übermittlung ihrer Daten an eine SEDOC-Partnerverwaltung gezielt auf etwaige datenschutzrechtliche Risiken hinzuweisen.

12 Krankenversicherung

12.1 Der gläserne Patient kommt nicht — Gesundheitsstrukturgesetz —

Mit dem Gesundheitsstrukturgesetz will der Gesetzgeber die dramatische Ausgabenentwicklung in der gesetzlichen Krankenversicherung eindämmen und damit die finanzielle Grundlage dieses Zweiges der Sozialversicherung erhalten.

Die Neuregelungen eröffnen auch Möglichkeiten zu einer intensiveren Kontrolle personenbezogener Daten. Mit ihnen sind auch teils veränderte, teils völlig neue Datenübermittlungen verbunden. Deren Notwendigkeit wurde plausibel begründet. Insoweit war es mein wesentliches Anliegen, die Datenübermittlungen auf das unerläßliche Maß einzuschränken und so zu gestalten, daß sie nicht zu einem versichertenbezogenen Leistungskonto bei den Krankenkassen führen konnten. Der „gläserne Patient" sollte unter allen Umständen verhindert werden (s. auch Anlage 7, Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Gesundheits-Strukturgesetz). Dies ist auch gelungen:

— § 295 Abs.2 SGB V legt jetzt ausdrücklich fest, daß die Übermittlung von Abrechnungsunterlagen durch die Kassenärztlichen Vereinigungen an die Krankenkassen *nicht versichertenbezogen* erfolgt. Mit dieser Klarstellung wird gewährleitst, daß die Krankenkassen keine umfassenden „Versichertenkonten" über die bei ihnen Versicherten anlegen können.

— Einen weiteren Beitrag zur Verhinderung des „gläsernen Patienten" leistet eine Klarstellung innerhalb der neu gefaßten Vorschrift des § 305 SGB V. Der Gesetzgeber legte großen Wert darauf, daß die Versicherten über die durch sie entstandenen Kosten unterrichtet werden können. Er bestimmte deshalb, daß die Krankenkassen die Versicherten auf deren Antrag über die im jeweils letzten Geschäftsjahr in Anspruch genommenen Leistungen und deren Kosten unterrichten. Hierzu zählen auch die bei den Kassenärztlichen und Kassenzahnärztlichen Vereinigungen angefallenen versichertenbezogenen Daten. Daraus ergab sich folgender Zielkonflikt:

  Einerseits mußte den Krankenkassen die Möglichkeit eröffnet werden, ihrer Unterrichtungspflicht gegenüber dem Versicherten in vollem Umfang nachzukommen. Andererseits durften sie aber nicht unbefugt Kenntnis von versichertenbezogenen Daten aus dem Bereich der Kassenärztlichen/Kassenzahnärztlichen Vereinigungen nehmen (vgl. meine obigen Ausführungen zu § 295 Abs. 2 SGB V). Zur Lösung dieses Zielkonflikts stellt § 305 SGB V klar, daß die Übermittlung der Daten der Kassenärztlichen/Kassenzahnärztlichen Vereinigungen an die Krankenkassen, die diese für ihre Unterrichtungspflicht gegenüber den Versicherten benötigen, nur so erfolgen darf, daß die Krankenkassen diese Daten nicht zur Kenntnis nehmen können (z. B. im verschlossenen Umschlag).

— Im Rahmen der Organisationsreform der gesetzlichen Krankenversicherung wird ein finanzieller Risikostrukturausgleich zwischen finanzstarken und finanzschwachen Krankenkassen vorgenommen. Um den Risikostrukturausgleich durchführen zu können, bedarf es genauer Kenntnisse über die Leistungsausgaben und Beitragseinnahmen der jeweiligen Krankenkassen.

  Meine Bemühungen um angemessene datenschutzrechtliche Regelungen hierzu waren erfolgreich: Daten über Leistungsausgaben und beitragspflichtige Einnahmen dürfen die Krankenkassen nicht versichertenbezogen erheben. Auch auf dieser Ebene wurde der „gläserne Patient" also verhindert, der bei einer versichertenbezogenen Erhebung der Daten (dies war im ersten Entwurf des Gesetzes noch vorgesehen) Wirklichkeit zu werden drohte.

— Um die vertragsärztliche Versorgung auch dann sicherzustellen, wenn mehr als 50 % aller in einem Zulassungsbezirk oder in einem regionalen Planungsbereich niedergelassenen Vertragsärzte auf ihre Zulassung verzichten oder die vertragsärztliche Versorgung verweigern, dürfen Krankenkassen nunmehr entweder Eigeneinrichtungen betreiben oder Einzel- oder Gruppenverträge mit versorgungsberechtigten Ärzten, Zahnärzten,

Krankenhäusern oder sonstigen geeigneten Einrichtungen schließen.

Hier galt es zu verhindern, daß die Krankenkassen in einer solchen Situation dadurch mehr versichertenbezogene Daten erhalten, daß die Abrechnung direkt mit den Krankenkassen erfolgt und nicht mehr über Kassenärztliche/Kassenzahnärztliche Vereinigungen läuft. Dies wird jetzt dadurch erreicht, daß Ärzte oder Einrichtungen, derer sich die Krankenkassen zur Erfüllung des auf sie übergegangenen Sicherstellungsauftrages bedienen, nur die für die Erfüllung der Aufgaben der Krankenkassen und die für die Abrechnung der vertraglichen Vergütungen notwendigen Angaben aufzeichnen und den Krankenkassen mitteilen dürfen.

— Zur Stärkung der Position des Hausarztes im System der vertragsärztlichen Versorgung umfaßt die hausärztliche Versorgung künftig auch die Dokumentation der wesentlichsten Behandlungsdaten über Befunde und Berichte, die den Versicherten betreffen, durch den Hausarzt. Daraus ergibt sich eine Pflicht zur gegenseitigen Information von Haus- und Facharzt bei Überweisungen, die Pflicht des Facharztes, den Hausarzt über die wesentlichen Behandlungsdaten und Befunde zum Zweck der Dokumentation zu unterrichten und — bei einem Hausarztwechsel — die Verpflichtung des früheren Hausarztes, die über den Patienten vorhandenen Unterlagen einem neuen Hausarzt zur Verfügung zu stellen. Diese Datenübermittlungen sind auf meine Initiative hin in § 73 Abs. 1 b SGB V geregelt worden. Damit sind Verarbeitungen und Nutzungen medizinischer Daten in diesem Bereich erstmalig in einem Gesetz derart präzise bestimmt worden. Das Standesrecht der Ärzte tritt dann insoweit zurück. Außerdem wurde in § 76 Abs. 3 SGB V auf meine Initiative klargestellt, wer Hausarzt im Sinne des § 73 SGB V ist. Entscheidend ist der Wille des Versicherten.

— Für die Prüfung der Ausgaben, die Vertragsärzte für Arznei-, Verband- und Heilmittel zu Lasten der gesetzlichen Krankenversicherung veranlassen, werden die erforderlichen Daten nicht versichertenbezogen erfaßt, weil dies zur Erfüllung der Prüfungsaufgaben nicht notwendig ist.

— § 115 b Abs. 2 SGB V legt fest, daß Krankenkassen die Wirtschaftlichkeit und Qualität ambulanter Operationen nur anhand der gleichen Daten prüfen dürfen, die die Krankenhäuser den Krankenkassen für die entsprechende Überprüfung der stationären Versorgung übermitteln.

— Krankenkassen haben in jedem Bundesland mit Zustimmung der nach § 275 a Abs. 2 SGB V jeweils zu bestimmenden Krankenhäuser unter bestimmten Voraussetzungen die Notwendigkeit von Krankenhausbehandlungen durch den Medizinischen Dienst als sogenannte Modellvorhaben prüfen zu lassen.

Die für ein Modellvorhaben erforderlichen Daten, die dem Medizinischen Dienst von Krankenkassen und Krankenhäusern zur Verfügung zu stellenden Unterlagen sowie die zu erteilenden Auskünfte und deren Beschaffung durch den Medizinischen Dienst sind im Gesetz bestimmt. Die beim Medizinischen Dienst angefallenen personenbezogenen Daten sind ein Jahr nach Abschluß des Modellvorhabens zu löschen. Der Medizinische Dienst der Spitzenverbände der Krankenkassen erhält die Auswertungsergebnisse nur in anonymisierter Form, da er für seine Aufgaben keine personenbezogenen Daten der Versicherten benötigt.

— Krankenhausärzte, die zur gesonderten Berechnung wahlärztlicher Leistungen berechtigt sind (dies sind in der Regel Chefärzte), dürfen nach der Bundespflegesatzverordnung auch eine private Abrechnungsstelle mit der Abrechnung der von ihnen erbrachten, wahlärztlichen Leistungen beauftragen. Die Übermittlung personenbezogener Daten von Patienten an eine Abrechnungsstelle darf jedoch nur mit Einwilligung der jeweils betroffenen Patienten erfolgen, also nicht ohne deren Wissen und Wollen.

— Um den Personalbedarf im Pflegebereich besser ermitteln zu können, müssen Krankenhäuser künftig täglich für jeden Patienten auf Patienten-Erhebungsbögen pflegerische Leistungen anhand bestimmter Kriterien dokumentieren. Die Patienten-Erhebungsbögen werden anschließend von der Arbeitsgemeinschaft der Spitzenverbände der Krankenkassen zum Zweck der Prüfung der Schlüssigkeit der Zuordnung der Patienten zu den Pflegestufen und für Vergleichszwecke ausgewertet. Die Ergebnisse der Auswertung werden den Parteien, die jeweils über die Höhe der Pflegesätze eines Krankenhauses verhandeln, zur Verfügung gestellt. Haben sich bei der Auswertung der Unterlagen über die Zuordnung zu den Pflegestufen Abweichungen ergeben, darf der jeweilige Medizinische Dienst auf Veranlassung der Krankenkassen unter bestimmten Voraussetzungen die Zuordnungen prüfen lassen.

Zur datenschutzgerechten Gestaltung dieses Verfahrens wurden u. a. folgende Regelungen in der Pflege-Personal-Regelung und in § 275 Abs. 3a SGB V getroffen:

Die Arbeitsgemeinschaft der Spitzenverbände der Krankenkassen darf die Patienten-Erhebungsbögen ausschließlich zu den oben beschriebenen Zwecken prüfen. Ferner muß die Arbeitsgemeinschaft die Patienten-Erhebungsbögen spätestens nach Abschluß einer Schlüssigkeitsprüfung vernichten. Das den Krankenkassen mitgeteilte Ergebnis der vom Medizinischen Dienst durchgeführten Schlüssigkeitsprüfung darf keine personenbezogenen Daten enthalten, da solche Daten für die Aufgabenerfüllung der Krankenkassen in diesem Zusammenhang nicht erforderlich sind. Die Krankenhäuser haben das bei ihnen verbleibende Exemplar des Erhebungsbogens nach Eingang der Auswertung zu anonymisieren. Bis zu diesem Zeitpunkt dürfen die personenbezogenen Daten auf den Erhebungsbögen nur für die Ermittlung des Bedarfs an Fachpersonal für den Pflegedienst verwendet werden.

12.2 Dürfen Krankenkassen der Bundesanstalt für Arbeit und der Zollverwaltung Mitgliederbestandslisten überlassen?

Der Bundesanstalt für Arbeit obliegt es, bei Arbeitgebern zu kontrollieren, ob die Beschäftigten gemäß § 28a SGB IV zur Sozialversicherung angemeldet sind. Sie ist hierbei u. a. von den Krankenkassen und den Hauptzollämtern zu unterstützen. Im Rahmen dieser Unterstützung sind die Behörden befugt, die erforderlichen Daten untereinander auszutauschen (§ 107 Abs. 1 letzter Satz SGB IV).

An die AOK für das Land Brandenburg sind ein Arbeitsamt und ein Hauptzollamt mit der Bitte herangetreten, ihnen Mitgliederbestandslisten mit Namen und Anschriften sämtlicher in der Vergangenheit und in der Gegenwart beschäftigten Arbeitnehmer einzelner Betriebe zu übersenden. Die AOK hatte Bedenken gegen die Übermittlung im Hinblick auf § 306 Satz 4 SGB V. Danach ist eine Unterrichtung über personenbezogene Daten unzulässig, die nach den §§ 284 bis 302 SGB V von Versicherten (z. B. zur Feststellung eines Versicherungsverhältnisses) erhoben werden.

Ich habe die Auffassung vertreten, daß § 306 SGB V der gewünschten Datenübermittlung — ihre Erforderlichkeit vorausgesetzt — nicht entgegensteht, soweit davon Daten betroffen sind, die auf der Grundlage des § 28 a SGB IV vom Arbeitgeber an die Krankenkasse gemeldet worden sind, denn diese Daten sind nicht nach den §§ 284 bis 302 SGB V von Versicherten erhoben. Eine Anwendung des § 306 Satz 4 SGB V auf diese Daten kommt daher nicht in Betracht.

Ich habe jedoch Bedenken geäußert — insbesondere bezüglich der Namen und Anschriften von *in der Vergangenheit* beschäftigten Arbeitnehmern —, ob die Offenbarung der vollständigen Mitgliederbestandslisten für die Aufgabenerfüllung der Arbeitsämter/Hauptzollämter wirklich erforderlich ist. Die Erforderlichkeit ist nur dann zu bejahen, wenn die Behörde ohne die betreffenden Daten eine Aufgabe nicht oder nicht sachgerecht erfüllen kann. Es genügt nicht, daß die Daten hilfreich und für die Aufgabenerfüllung geeignet sind. Von der übermittelnden Behörde, hier der AOK, muß dies in jedem Einzelfall geprüft werden.

Ich habe daher die AOK gebeten, eine entsprechende Erforderlichkeitsprüfung, ggf. durch weitere Nachfragen bei den anfordernden Behörden, vorzunehmen.

12.3 Krankenkasse beschaffte sich bei Betriebsprüfung Arbeitnehmerdaten für Werbezwecke

Mehrfach mußte ich mich mit Vorgängen befassen, bei denen Arbeitgeber Namen und Anschriften von Bewerbern und neuen Mitarbeitern Ersatzkassen zu Werbezwecken überlassen hatten (vgl. 9. TB S. 54; 10. TB S. 68 und 12. TB S. 69). Anläßlich eines Kontroll- und Informationsbesuchs bei der Geschäftsstelle einer Ersatz-Krankenkasse stellte ich fest, daß Kassenmitarbeiter Behörden- und Firmenbesuche, die dem Zwecke der Beratung und Betriebsprüfung dienten, zum Anlaß genommen hatten, von den Mitarbeitern des besuchten Betriebes Namen möglicher Interessenten für ihre Krankenkasse in Erfahrung zu bringen. Die so gewonnenen Informationen wurden in der Geschäftsstelle der Krankenkasse konventionell in einer Kartei „Interessenten" geführt.

In Übereinstimmung mit dem BMA vertrete ich die Auffassung, daß die Übermittlung von Arbeitnehmerdaten an Ersatzkassen zu Werbezwecken allenfalls mit Einwilligung der Betroffenen zulässig ist. Die Ersatzkasse ist dagegen der Ansicht, § 28 Abs. 2 Nr. 1 Buchstabe a und b BDSG seien Rechtsgrundlage für die Datenübermittlung durch den Arbeitgeber an sie und meint, es bestehe kein Grund zu der Annahme, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat. Nach Auffassung der Krankenkasse hat der Betroffene nur ein Widerspruchsrecht gegen die Datenübermittlung gemäß § 28 Abs. 3 BDSG.

Gegen diese Auffassung sprechen mehrere Gesichtspunkte:

Eine Übermittlung von Arbeitnehmerdaten durch den Arbeitgeber an eine Krankenkasse kann schon deshalb nicht auf § 28 BDSG gestützt werden, weil dessen Regelungen durch die von der Rechtsprechung entwickelten Grundsätze über den Umgang mit Arbeitnehmerdaten (z. B. BAG RDV 87, 129) verdrängt werden. Der Arbeitgeber darf aber Arbeitnehmerdaten grundsätzlich nur verarbeiten, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Arbeitsverhältnisses erforderlich ist. Dies wird nicht nur in § 90 Abs. 4 BBG, sondern auch in den Landesdatenschutzgesetzen, die besondere Regelungen über den Arbeitnehmerdatenschutz enthalten, ausdrücklich gesagt (vgl. z. B. § 22 DSG Bremen, § 28 DSG Hamburg, § 34 DSG Hessen, § 29 DSG NRW). Eine Datenübermittlung für andere Zwecke bedarf einer besonderen, bereichsspezifischen Rechtsgrundlage. Eine solche ist hier nicht ersichtlich.

Selbst eine Anwendung des § 28 BDSG würde aber zu keinem anderen Ergebnis führen. Eine Offenbarung der Daten zur Wahrung berechtigter Interessen der Krankenkassen (§ 28 Abs. 2 Nr. 1a BDSG) scheidet aus, weil sie diesem Zweck nicht nur dienlich, sondern zu seiner Wahrung erforderlich sein muß. Dies bedeutet, daß die berechtigten Interessen auf andere Weise nicht oder zumindest nicht angemessen gewahrt werden können. Vorliegend ist es nicht erforderlich, sondern bestenfalls aus Sicht der Krankenkassen wirtschaftlich zweckmäßig, daß sie sich die Informationen unmittelbar bei den Arbeitgebern beschaffen.

Auch eine Übermittlung dieser Daten als listenmäßig zusammengefaßte Daten über Angehörige einer Personengruppe, die sich auf eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe beschränken (§ 28 Abs. 2 Nr. 1b 1. Spiegelstrich BDSG) ist unzulässig. Denn Name und Anschrift von Bewerbern und Arbeitnehmern sind vom Arbeitgeber im Rahmen eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses gespeichert. Nach § 28 Abs. 2 Nr. 1 b Satz 2 letzter

Spiegelstrich BDSG wird deshalb vermutet, daß ein schutzwürdiges Interesse des Bewerbers oder Arbeitnehmers der Übermittlung entgegensteht.

Damit ist eine Offenbarung von Arbeitnehmerdaten für die beschriebenen Zwecke an die Ersatzkasse nur zulässig, wenn zuvor die Einwilligung der Betroffenen eingeholt wurde. Unbedenklich wäre eine Weiterleitung von Werbematerial der Krankenkasse seitens des Arbeitgebers an die Arbeitnehmer.

Ich stehe derzeit noch in Gesprächen mit der Ersatzkasse. Es wurde mitgeteilt, daß auch das Bundesversicherungsamt zu dem Problemkreis „Mitgliederwerbung" eine umfassende Bewertung vornehmen wird.

12.4 Krankenversichertenkarte als Chipkarte

Gemäß § 291 Abs. 1 SGB V waren die Krankenkassen ursprünglich verpflichtet, ab 1. Januar 1992 (durch eine entsprechende Änderung im Gesundheitsstrukturgesetz wurde der Termin mittlerweile auf den 1. Januar 1995 verschoben) für jeden Versicherten eine Krankenversichertenkarte auszustellen, die den Krankenschein nach § 15 SGB V ersetzt. Eine Vereinbarung zwischen den Spitzenverbänden der Krankenkassen und den Kassenärztlichen Bundesvereinigungen sollte entsprechend ihrer in § 291 Abs. 3 SGB V geregelten Befugnis vertraglich das Nähere über die bundesweite Einführung und Gestaltung der Krankenversichertenkarte regeln. Die Vertragspartner strebten zunächst die Einführung der Krankenversichertenkarte auf der Basis der Magnetstreifenkartentechnologie an. Im Zuge dieser Vertragsverhandlungen war ich beratend tätig.

Die von den Vertragspartnern zunächst angestrebte Lösung auf der Basis einer Magnetstreifenkarte scheiterte kurz vor dem vom Gesetzgeber für den 1. Januar 1992 gesetzten Einführungstermin, weil die Kassenärztliche Bundesvereinigung die Einführung der Krankenversichertenkarte auf der Basis der Chipkartentechnologie forderte.

Aufgrund dieser neuen Entwicklung wurde ich von den Vertragspartnern aufgefordert, erneut beratend tätig zu werden. Im Zuge dieser Beratung habe ich den Vertragspartnern die folgende Position zur Einführung der Krankenversichertenkarte als Chipkarte deutlich gemacht:

1. Zweck der Krankenversichertenkarte soll sein, den Nachweis für die Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der kassen- oder vertragsärztlichen Versorgung zu führen. Die Karte darf auch für die Abrechnung mit den Leistungserbringern (z. B. Ärzten, Apothekern, Krankenhäusern) verwendet werden. Jede andere Nutzung ist untersagt. Aufgrund dieser Zweckbestimmung bestimmt das Gesetz in § 291 Abs. 2 SGB V abschließend die Daten, die auf der Krankenversichertenkarte eingetragen werden dürfen: Bezeichnung der ausstellenden Krankenkasse, Familienname und Vorname des Versicherten, Geburtsdatum, Anschrift, Krankenversichertennummer, Versichertenstatus, Tag des Beginns des Versicherungsschutzes, bei befristeter Gültigkeit der Karte das Datum des Fristablaufs. Andere Daten, insbesondere medizinische Daten, dürfen nach dem klaren Gesetzeswortlaut nicht auf der Karte gespeichert werden.

2. Über die technische Ausgestaltung der Karte enthält das Gesetz keine abschließenden Regelungen. Diese bleibt der oben erwähnten Vereinbarung zwischen den Spitzenverbänden der Krankenkassen und den Kassenärztlichen Bundesvereinigungen vorbehalten.

3. Um aber jeden Anreiz für eine über die in § 291 Abs. 2 SGB V gesetzlich festgelegten und zulässigen Daten hinausgehende und damit unzulässige Speicherung weiterer Daten zu verhindern, muß die Speicherkapazität des verwendeten Chips auf die Aufnahme dieser Daten begrenzt werden. Sie darf also eine Speicherung weiterer Daten grundsätzlich nicht zulassen.

4. Es muß technisch gewährleistet sein, daß kein Unbefugter den Inhalt der auf der Chipkarte gespeicherten Daten verändern kann; dies darf nur der hierfür autorisierten Krankenkasse möglich sein.

5. Der einzelne Versicherte muß die Möglichkeit haben, sich jederzeit selbst über den Umfang der über ihn auf der Chipkarte gespeicherten Daten zu informieren; er muß sich — z. B. mit Hilfe eines entsprechenden Geräts bei der Krankenkasse — überzeugen können, daß die Karte keine unzulässigen Speicherungen enthält und weder gefälscht noch verfälscht ist.

Im Laufe der Verhandlungen mit den Spitzenorganisationen wurde die Frage immer wichtiger, mit welchem technischen Sicherheitsstandard die Krankenversichertenkarte gegen Mißbrauch, Fälschung und Verfälschung geschützt werden soll und wie der Versicherte Kenntnis über das Vorliegen eines der drei unter 5. genannten Tatbestände erlangen kann.

Dabei habe ich den Vertragspartnern — als die aus meiner Sicht beste Lösung — die sogenannte kryptographische Versiegelung der Krankenversichertenkarte empfohlen. Diesem Vorschlag sind die Vertragspartner mit der Begründung, eine solche technische Sicherung verursache zu hohe Kosten, nicht gefolgt. Nach mehrfachen intensiven Gesprächen mit den Vertragspartnern — zuletzt unter Beteiligung des Bundesministeriums für Gesundheit — konnte ich aber erreichen, daß sich die Vertragspartner bereit erklärt haben, — wenn schon nicht für die aus meiner Sicht nach wie vor beste Lösung der kryptographischen Versiegelung — so doch für die bis zum 1. Januar 1995 dauernde Phase der Einführung der Krankenversichertenkarte für die Sicherstellung des im folgenden dargestellten technischen Sicherheitsstandards zu sorgen:

1. Nur die ausstellende Krankenkasse darf Eintragungen auf der Karte vornehmen und — soweit erforderlich — ändern. Ärzte und andere Leistungserbringer dürfen nur solche Hard- und Soft-

ware einsetzen, die ausschließlich ein Lesen der Karte, also kein Beschreiben, ermöglicht.

2. Die Vertragspartner stellen sicher, daß jeder Versicherte jederzeit sowohl den Inhalt der über ihn auf der Krankenversichertenkarte gespeicherten Daten bei einem Arzt oder einem Krankenversicherungsträger als auch den unbeschriebenen Teil der Krankenversichertenkarte bei einem Krankenversicherungsträger überprüfen kann. Bei dieser Überprüfung dürfen weder der Inhalt der Krankenversichertenkarte noch die Tatsache der Überprüfung gespeichert werden.

3. Die Vertragspartner stellen des weiteren sicher, daß die über den vorhandenen Datensatz des Versicherten nach § 291 Abs. 2 SGB V hinaus auf der Krankenversichertenkarte jeweils verbleibenden, nicht benötigten Speicherplätze des Kartenchips mit einem definierten Zeichen belegt und nicht unbefugt beschrieben werden. Es muß technisch sichergestellt sein, daß ein Versicherter anläßlich der unter 2. erwähnten Überprüfung erkennen kann, ob die Karte mit nicht zulässigen Daten beschrieben oder ob ein nach § 291 Abs. 2 SGB V grundsätzlich zulässiges Datum unbefugt neugeschrieben oder verändert worden ist.

Die Vertragspartner haben mir zugesichert, daß gegen Ende der notwendigen Einführungsphase der technische Sicherheitsstandard der Krankenversichertenkarte unter Berücksichtigung der gewonnenen Erfahrungen noch einmal gemeinsam überprüft und ggfs. weiter verbessert wird.

12.5 Patientendaten auf Müllkippe — Kontrolle eines Knappschaftskrankenhauses —

Eine Bundesknappschaftsklinik wurde von mir aufgrund eines Hinweises, daß auf einer Mülldeponie datenschutzrelevantes Material gefunden worden sei, unangekündigt kontrolliert.

Bei dem auf einer Mülldeponie gefundenen Abfall handelte es sich nach Angaben der Klinikmitarbeiter um sogenannte Laborzettel aus dem Laborbereich der Klinik. Diese seien vermutlich aufgrund einer Unachtsamkeit eines Mitarbeiters im Labor entgegen entsprechenden klinikinternen Weisungen zur Entsorgung datenschutzrelevanten Materials entsorgt worden.

Die Müllentsorgung war in der Klinik wie folgt organisiert:

Der Müll wurde in die Kategorien Hausmüll (zu dieser Kategorie zählte auch der datenschutzrelevante Müll) und krankenhausspezifischer Müll (z. B. Wundverbände) unterteilt. Beide Müllsorten wurden getrennt gesammelt. Sie wurden anschließend in verschiedene, den beiden Kategorien jeweils zuzuordnende Müllcontainer auf dem Krankenhausgelände verbracht.

Dabei wurde der datenschutzrelevante Müll zwar vorab in separaten Säcken gesammelt, dann aber zusammen mit dem sonstigen Hausmüll in einen für diesen bestimmmten Container geworfen.

Bis Dezember 1991 wurden beide Müllkategorien gepreßt. Der Hausmüll wurde anschließend in einer Müllverbrennungsanlage verbrannt, der Krankenhausmüll speziell entsorgt. Da dies ab Dezember 1991 nicht mehr möglich war, entschloß sich die Klinik, den Müll insgesamt auf der Mülldeponie zu entsorgen, auf der letztlich die Laborzettel gefunden wurden.

Diese Organisation der Entsorgung entsprach nicht den gesetzlichen Anforderungen an einen sicheren Datenumgang (§ 79 SGB X i. V. m. § 9 BDSG). Zur Gewährleistung der datenschutzgerechten Entsorgung des Abfalls habe ich der Bundesknappschaft empfohlen, einen Vertrag mit einem Entsorgungsunternehmen zu schließen (§ 80 SGB X i. V. m. § 11 BDSG).

Die datenschutzrechtliche Organisation im Laborbereich und der Datenumfang auf den Laborzetteln, die ich überprüft habe, begegneten keinen Bedenken.

Beim Patientenarchiv war zu bemängeln, daß die Akten älterer Jahrgänge in erheblichem Umfang Unterlagen enthielten, für die die Aufbewahrungsfristen abgelaufen waren. Die fristgerechte Aussonderung der Unterlagen wurde dadurch erschwert, daß die Akten nach dem Datum der Erstaufnahme und dem Namen des Patienten — nicht jedoch nach Jahrgängen — registriert und archiviert sind. Eine Überprüfung der Akten zwecks Aussortierung wegen des Ablaufes der Aufbewahrungsfrist hat seit vier Jahren nicht mehr stattgefunden. Darin sehe ich einen Organisationsmangel und einen Verstoß gegen §§ 84, 79 SGB X i. V. m. § 9 BDSG.

Der Zugang zu den entsprechenden Archivräumen war hingegen so geregelt, daß ein unkontrolliertes Betreten nach meiner Einschätzung praktisch ausgeschlossen war.

Da die Klinik zum Zeitpunkt der Kontrolle dabei war, ein datenschutzgerechtes Organisationsmodell zu entwickeln, habe ich mitgeteilt, daß ich dieses in meine endgültige datenschutzrechtliche Bewertung einbeziehen möchte.

Auch im Hinblick auf die Organisation des Datenschutzes und die hiermit im Zusammenhang stehende Aus- und Fortbildung bestanden in der kontrollierten Knappschaftsklinik Defizite. So sind interne Datenschutzanweisungen vor Ort nicht vorhanden.

Nach Angaben der Klinikmitarbeiter erfolgten regelmäßig arbeitsplatzbezogene mündliche Erläuterungen durch den internen Datenschutzbeauftragten oder den Abteilungsleiter Rechnungswesen; prüfbare Unterlagen dazu existieren aber nicht.

Ich habe die Bundesknappschaft aufgefordert, die festgestellten Mängel zu beseitigen und mir eine Beanstandung vorbehalten. Ferner habe ich die Bundesknappschaft um Stellungnahme — auch zur Situation in den anderen Knappschaftskrankenhäusern — gebeten.

In einer mittlerweile eingegangenen Stellungnahme hat mir die Bundesknappschaft mitgeteilt, daß der

Abschluß eines Entsorgungsvertrages mit einer Entsorgungsfirma unmittelbar bevorstehe. Außerdem sei in der Knappschaftsklinik mit der Vernichtung von Patientenakten begonnen worden, für die die entsprechenden Aufbewahrungsfristen abgelaufen sind. Außerdem werden künftig die mündlichen Datenschutzbelehrungen der Mitarbeiter schriftlich dokumentiert.

Zu den übrigen Punkten stehen endgültige Ergebnisse noch aus, so daß der Dialog mit der Bundesknappschaft insoweit noch andauert.

12.6 Ein Spitzenverband der Krankenkassen beanstandet

Ein Spitzenverband aus dem Bereich der gesetzlichen Krankenkassen hat trotz mehrfacher, schriftlicher — zuletzt unter Fristsetzung erfolgter — Erinnerungen meiner Bitte um Stellungnahme im Hinblick auf eine sich anläßlich einer Bürgereingabe ergebenden Frage nicht entsprochen.

Gemäß § 24 Abs. 4 BDSG sind die öffentlichen Stellen des Bundes verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Hierzu zählt auch die Verpflichtung, Auskunft zu den Fragen des Bundesbeauftragten und seiner Beauftragten zu gewähren (§ 24 Abs. 4 Satz 2 Nr. 1, erste Alternative BDSG).

Den durch die Nichtabgabe der von mir erbetenen Stellungnahme vorliegenden Verstoß gegen § 24 Abs. 4 BDSG habe ich beanstandet. Nach der Beanstandung hat der Spitzenverband recht schnell reagiert.

13 Rentenversicherung

13.1 Die Dateien der Datenstelle des Verbandes Deutscher Rentenversicherungsträger (VDR) sind kein zentrales Auskunftsregister

Der Verband Deutscher Rentenversicherungsträger (VDR) verfügt über einen riesigen Datenbestand von Sozialversicherten, der durch die Datenstelle der Rentenversicherungsträger verwaltet wird.

Allein in der Stammsatzdatei sind etwa 84 Mio. Datensätze mit personenbezogenen Daten gespeichert. Es ist verständlich, daß dieser Datenbestand das Interesse zahlreicher Fachverwaltungen findet, insbesondere wenn es darum geht, den Aufenthalt einer Person festzustellen. Da die gespeicherten Daten aber dem Sozialgeheimnis unterliegen, hat der Gesetzgeber in § 68 SGB X bestimmt, daß im Wege der Amtshilfe Vor- und Familiennamen, Geburtsdatum, Geburtsort, derzeitige Anschrift des Betroffenen sowie Namen und Anschrift seines derzeitigen Arbeitgebers offenbart werden können, soweit kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Ergänzend bestimmt § 81 SGB X, daß die §§ 10 und 11 BDSG (alt) nicht für die Offenbarung personenbezogener Daten nach den §§ 69 bis 77 SGB X gelten, woraus mit Recht geschlossen wurde, daß diese Vorschriften des alten BDSG für eine Datenübermittlung auf der Grundlage des § 68 SGB X anzuwenden waren. Von Bedeutung war dabei besonders § 10 Abs. 1 Satz 2 BDSG (alt), wonach personenbezogene Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen und der übermittelnden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Dienst- oder Amtspflicht übermittelt worden sind, nur weiter übermittelt werden dürfen, wenn der Empfänger die Daten zur Erfüllung des gleichen Zweckes benötigt, zu dem sie die übermittelnde Stelle erhalten hat. Da mit Recht davon ausgegangen wurde, daß die beim VDR gespeicherten Daten schon vor ihrer Übermittlung an den VDR dem Sozialgeheimnis unterlagen, wurde unter der Geltung des alten Bundesdatenschutzgesetzes fast einhellig die Auffassung vertreten, daß eine Datenweiterübermittlung durch den VDR im Wege der Amtshilfe nach § 68 SGB X, die ja praktisch stets für einen anderen Zweck als den Speicherungszweck des VDR erbeten wird, nahezu ausscheidet.

Deshalb hat die Datenstelle bis zum Jahre 1990 praktisch keine Auskünfte aus diesem Datenbestand auf der Grundlage des § 68 SGB X (Amtshilfe) erteilt. Da diese Praxis allgemein bekannt war, gab es auch kaum Auskunftsersuchen an den VDR. Dies hat sich geändert. Bereits im Jahre 1991 sind bei der Datenstelle 17 Anfragen, die auf § 68 SGB X gestützt wurden, eingegangen. Von Januar bis Juli 1992 ist die Zahl dieser Auskunftssuchenden sprunghaft auf insgesamt 145 angestiegen.

Ursache für diesen Anstieg ist offensichtlich die inzwischen vom BMA vertretene und bekannt gewordene Rechtsauffassung, das neue Bundesdatenschutzgesetz enthalte nicht mehr die gleiche strenge Zweckbindungsregelung für an den VDR übermittelte personenbezogene Daten, die dem Sozialgeheimnis unterliegen. Dieser Rechtsauffassung haben sich die Gremien des VDR angeschlossen.

Die geänderte Rechtsauffassung des BMA war für mich nicht nachvollziehbar, weil § 39 des neuen BDSG eine für diesen Fall eher noch klarere, ebenso stringente Zweckbindungsregelung enthält und kein Grund für die Annahme spricht, § 81 SGB X wolle in Zukunft eine Anwendung dieser Vorschrift bei Datenübermittlungen nach § 68 SGB X ausschließen.

Um die praktischen Auswirkungen der geänderten Rechtsauffassung festzustellen, habe ich eine Kontrolle der auf der Grundlage des § 68 SGB X durchgeführten Datenübermittlungen des VDR durchgeführt. Dabei wurde festgestellt, daß die beim VDR eingegangenen Auskunftsersuchen die unterschiedlichsten Zwecke betrafen:

- Ermittlung von Gebührenschuldnern einer staatlichen Unterkunftsverwaltung;
- Feststellung geringfügig Beschäftigter durch einen Landkreis, um eine ausreichende Pflege und Versorgung eines Alten- und Pflegeheimes sicherzustellen;
- Daten für Vorermittlungen in einem Disziplinarverfahren durch eine Kriminalinspektion;

— Anfrage über den derzeitigen Aufenthalt verschiedener Personen durch den Suchdienst des Deutschen Roten Kreuzes;

— Anfragen über den Aufenthalt von Personen durch die zentrale Ermittlungsstelle für Regierungs- und Vereinigungskriminalität.

Die Auskunftspraxis wird nach folgenden Grundsätzen abgewickelt:

Die Datenstelle gibt im wesentlichen *un*mittelbar Auskunft an die ersuchende Stelle

— über Daten aus dem Stammsatzbestand (in der Praxis die Postleitzahl der Anschrift) und

— aus der Sonderdatei für geringfügig Beschäftigte (§ 8 SGB IV), weil die dort gespeicherten Daten (z. B. Versicherungsnummer, Zeitraum und Art der Beschäftigung, Betriebsnummer des Arbeitgebers und Kennzeichen der Krankenkasse) von der Datenstelle unabhängig von den Rentenversicherungsträgern erhoben, verarbeitet und genutzt werden.

Die Datenstelle des VDR gibt das Ersuchen an den von ihr festgestellten zuständigen Rentenversicherungsträger weiter, wenn es Daten betrifft, die nur bei diesem, nicht aber beim VDR vorhanden sind. Über die Versicherungsnummer im Stammsatzdatenbestand bei der Datenstelle kann festgestellt werden, welcher Rentenversicherungsträger im einzelnen zuständig ist.

Sofern im Stammsatzdatenbestand keine Versicherungsnummer vorhanden ist, kann keine Auskunft gegeben werden. Dies wird der ersuchenden Stelle mitgeteilt.

Das Amtshilfeersuchen wird unmittelbar abgelehnt, wenn eine Auskunft über andere als in § 68 SGB X genannten Daten erbeten wird. Eine Ablehnung erfolgt auch dann, wenn weitere in § 68 SGB X genannte Offenbarungseinschränkungen vorliegen, wenn also beispielsweise Grund zu der Annahme besteht, daß durch die Datenweitergabe „schutzwürdige Belange des Betroffenen beeinträchtigt" werden oder wenn sich die „ersuchende Stelle die Angaben auf andere Weise beschaffen kann".

Nach geltendem Recht halte ich aus der dargestellten Praxis die Weitergabe von Auskunftsersuchen an die zuständigen Rentenversicherungsträger grundsätzlich für zulässig. Denn die Weitergabe stellt zwar eine Offenbarung eines personenbezogenen Datums an den Rentenversicherungsträger dar. Sie erfolgt aber nur, wenn die Datenstelle der VDR die Voraussetzung des § 68 SGB X für gegeben hält. Die Weitergabe stellt in der Sache lediglich die Weiterleitung des Amtshilfeersuchens an die — allerdings von der Datenstelle erst festgestellte — zuständige Stelle dar. Damit ist sie zur Aufgabenerfüllung des Rechtenversicherungsträgers erforderlich und zulässig.

Wenn der Leistungsträger anschließend von ihm selbst erhobene (ihm also nicht übermittelte) Daten nach § 68 SGB X offenbart, ist dagegen nichts einzuwenden, weil die weitergehende Zweckbindung des § 39 BDSG nicht greift. Allerdings sehe ich wegen der von vielen Millionen Versicherten gespeicherten Daten das Risiko, daß die Datenstelle der Rentenversicherungsträger im Laufe der Zeit zu einem — vom Gesetzgeber sonst nicht gewollten — bundesweiten „Ersatzmelderegister" wird.

Zu dem übrigen Verfahren habe ich dem VDR mitgeteilt, daß ich nach wie vor erhebliche Bedenken gegen eine Offenbarung von dem Sozialgeheimnis unterliegenden personenbezogenen Daten auf der Grundlage des § 68 SGB X habe, die ihm von Leistungsträgern übermittelt worden sind.

Im übrigen habe ich Zweifel, ob die Datenstelle des VDR eine Datenübermittlung überhaupt auf § 68 SGB X stützen kann. Diese Vorschrift läßt eine Offenbarung der dort genannten Daten nur im Rahmen „der Amtshilfe" zu. Amtshilfe können nur Behörden leisten (§ 3 Abs. 1 SGB X). Der VDR ist aber ein eingetragener Verein. Ich neige deshalb der Ansicht zu, daß er eine Offenbarung von Sozialdaten nicht auf § 68 SGB X stützen kann. Dieser Rechtsmeinung hat der VDR widersprochen. Das BMA hat sich hierzu nicht eindeutig geäußert. Es unterscheidet, ob der VDR als „beliehener Unternehmer" oder im Rahmen eines Auftragsverhältnisses tätig wird. Bei letzterem hänge die Behördeneigenschaft vom Einzelfall ab, wobei maßgebendes Differenzierungskriterium der Wille von Auftraggeber und Auftragnehmer sei.

Angesichts der unklaren Rechtslage sollte der Gesetzgeber sich bei nächster Gelegenheit des Problems annehmen. Er sollte dabei berücksichtigen, daß § 68 SGB X aus der Zeit vor dem Volkszählungsurteil stammt, das eine „amtshilfefeste" Zweckbindung personenbezogener Daten fordert.

Die derzeitige Formulierung des § 68 SGB X, die eine völlig zweckbindungsfreie Datenweitergabe im Wege der Amtshilfe zuläßt, ist deshalb zu weitgehend. Ich habe daher angeregt, im Zuge des 2. SGB-Änderungsgesetzes den § 68 SGB X auf Auskunftsersuchen durch die Polizei sowie zur Realisierung öffentlich-rechtlicher Forderungen zu beschränken. Außerdem sollte auf den Begriff der Amtshilfe verzichtet werden. Die für das Änderungsgesetz maßgebenden Ressorts unterstützen meinen Vorschlag. Er wurde mittlerweile in den Gesetzesentwurf aufgenommen (vgl. 10.1).

13.2 Datenabgleich zur Aufdeckung unberechtigter Versorgungsbezüge

Die Rechtsfolgen des Zusammentreffens von Versorgungsbezügen und Renten aus der gesetzlichen Rentenversicherung sind im Beamtenversorgungsgesetz geregelt (§ 55 BeamtVG). Danach werden die Versorgungsbezüge neben einer Rente nur bis zum Erreichen einer bestimmten Höchstgrenze gezahlt. Diese Vorschrift dient dazu, eine Doppelversorgung aus öffentlichen Kassen zu vermeiden. Die gesetzliche Regelung kann in der Praxis nur angewandt werden, wenn die für die Zahlung der Versorgungsbezüge zuständige Stelle Kenntnis vom Bezug der Rente erhält. Deshalb ist der Versorgungsempfänger nach § 62 Abs. 2 BeamtVG verpflichtet, den Bezug einer Rente anzuzeigen. Auf diese Verpflichtung werden

die Versorgungsberechtigten von den Pensionsfestsetzungsbehörden ausdrücklich hingewiesen. Dennoch gibt es nach Kenntnis des Bundesrechnungshofes viele Fälle, in denen ein Rentenbezug nicht angezeigt wird. Er hat daher einen Abgleich der Datenbestände über Versorgungs- und Rentenleistungen in dem nachstehend beschriebenen Verfahren angeregt:

— Die Pensionsbehörden erstellen aus ihrem Datenbestand eine Datei, die die Personalnummer/Kenn-Nummer, den Namen, den Vornamen, das Geburtsdatum und den Wohnsitz des Versorgungsempfängers enthält. Hierbei werden nur die Versorgungsempfänger berücksichtigt, die einen Rentenbezug bisher nicht angezeigt haben.

— Diese Datei wird (z. B. auf Magnetband) an die Rentenrechnungsstelle der Deutschen Bundespost in Hannover gesandt und dort mit den Daten der Rentenempfänger abgeglichen. Bei Treffern wird die Datei der Pensionsempfänger um die jeweilige Rentenversicherungsnummer ergänzt.

— Die Pensionsbehörden fertigen dann aus dieser Datei Listen, anhand derer die für die Versorgungsregelung jeweils zuständigen Behörden den Sachverhalt abschließend klären, z. B. indem der Versorgungsempfänger gebeten wird, den Rentenbescheid vorzulegen. Das Auskunftsband wird unmittelbar nach Fertigung der Listen gelöscht, die Listen werden nach Klärung des Sachverhaltes vernichtet.

— Um das Verfahren transparent zu machen, sollen die Versorgungsempfänger auf die Möglichkeit des Datenabgleichs zum Zwecke der Regelung nach § 55 BeamtVG hingewiesen werden.

Zur Begründung der Zulässigkeit des Verfahrens verweist der Bundesrechnungshof auf das Urteil des Bundesverfassungsgerichtes vom 27. Juni 1991 (BVerfGE 84, 239ff.) zur Besteuerung von Zinseinkünften. Er meint, nach den dort aufgestellten Grundsätzen dürfe die Verwaltung nicht schlechthin die Richtigkeit einer Erklärung unterstellen, sondern müsse diese, um einer Vollzugsungleichheit zu begegnen, durch geeignete Kontrollen überprüfen. Das „Deklarationsprinzip" bedürfe der Ergänzung durch das „Verifikationsprinzip".

Gegen das vorgeschlagene Verfahren habe ich Bedenken erhoben. Dabei verkenne ich nicht die Notwendigkeit, die Einhaltung des § 55 BeamtVG praktisch sicherzustellen und damit überhöhte Zahlungen zu Lasten der öffentlichen Haushalte zu vermeiden.

Es stellt sich jedoch die Frage, ob dazu ein solch intensives Kontrollverfahren erforderlich ist, wie es der Bundesrechnungshof vorschlägt.

Das vorgeschlagene Kontrollverfahren wäre also nur auf der Basis einer besonderen Rechtsvorschrift zulässig. Bevor der Gesetzgeber daran geht, eine solche zu schaffen, sollte aber sorgfältig geprüft werden, ob dies wirklich erforderlich ist, die bestehenden Rechtsgrundlagen für notwendige Kontrollen also nicht doch ausreichen.

Auch aus den bereichsspezifischen Vorschriften in den §§ 90ff. BBG ergibt sich nicht die Zulässigkeit des vom Bundesrechnungshof vorgeschlagenen Verfahrens. Die von ihm angeführte Entscheidung des Bundesverfassungsgerichtes kann nach den mir bisher vorliegenden Informationen kaum als Rechtfertigung herangezogen werden, da sie sich mit der Frage der steuerlichen Belastungsgleichheit bei der Besteuerung von Kapitaleinkünften auseinandersetzt und ausdrücklich bereichspezifisch für den Bereich des Steuerrechts argumentiert. Auch bin ich bisher nicht überzeugt, daß der Gleichheitsgrundsatz ohne den geforderten Datenabgleich auch nur entfernt in ähnlicher Weise gefährdet wäre, wie das Bundesverfassungsgericht dies für das Verfahren der Zinsbesteuerung festgestellt hat. Dort war davon auszugehen, daß die Fehlerquote bei den Zinserträgen im Besteuerungsverfahren mindestens 40%, wahrscheinlich deutlich mehr, betrug.

Ich halte es für erforderlich, den Dialog mit dem Bundesrechnungshof fortzusetzen. Dabei sind für mich folgende Punkte von zentraler Bedeutung:

— Ist der gewünschte generelle Datenabgleich zur Abwehr einer erheblichen Beeinträchtigung des Gemeinwohles zwingend erforderlich und damit der Verhältnismäßigkeitsgrundsatz gewahrt?

— Gibt es nicht Verfahren, die weniger schwerwiegend in das Recht auf informationelle Selbstbestimmung — insbesondere der Vielzahl der betroffenen, aber völlig unverdächtigen Versorgungsempfänger — eingreifen?

— Auf welche Weise wird sichergestellt, daß der Betroffene im Hinblick auf den Transparenzgrundsatz rechtzeitig, also vor Durchführung, von dem Datenabgleich erfährt?

Für den Gesetzgeber dürfte von Interesse sein, daß im Ausland (z. B. USA, Australien, Neuseeland) Modelle entwickelt worden sind, auf die wir zurückgreifen könnten. Diese zählen vor allem auf eine auch wirtschaftlich vernünftige Begrenzung von Datenabgleichen, auf eine frühzeitige Information und eine ausreichende Beteiligung der Betroffenen sowie auf begleitende Maßnahmen zur Sicherung eines datenschutzgerechten Ablaufs.

13.3 Kontrolle bei der Bundesversicherungsanstalt für Angestellte (BfA)

Eine Kontrolle bei der BfA gab Anlaß, u. a. Fragen zu folgenden Bereichen zu erörtern:

— Weitergabe ärztlicher Unterlagen von Versicherten

— Offenbarungen bei Verrechnungsersuchen anderer Sozialversicherungsträger

— personalärztliche Fragebogen

Den ersten zwei Punkten lagen Eingaben zugrunde. Die dadurch aufgeworfenen Fragen sind aber über die behandelten Einzelfälle hinaus von allgemeiner Bedeutung. Sie geben bei der BfA auch insgesamt Anlaß, die Organisation zu prüfen. Ungeachtet einiger

festgestellter Mängel ist die Organisation des Datenschutzes bei der BfA insgesamt überzeugend. Positiv hervorzuheben ist, daß der Datenschutzbeauftragte der BfA jährliche Tätigkeitsberichte erstellt, die wertvolle Anregungen und praktische Hinweise für die Mitarbeiter enthalten.

13.3.1 Ärztliche Unterlagen trotz Widerspruchs des Versicherten weitergegeben

Für die BfA sind Gutachterärzte tätig, die nicht bei ihr angestellt sind. Sie erstellen beispielsweise Gutachten über den Gesundheitszustand und die Leistungsfähigkeit von Personen, die eine Berufsunfähigkeitsrente beantragt haben. Ein Petent, dem es um die Weitergewährung einer Berufsunfähigkeitsrente ging, hatte sich zunächst mit einem Schreiben an die BfA gewandt und gefordert, daß — wenn überhaupt ein weiteres Gutachten erforderlich sei — nicht — wie früher — ein Nervenarzt, sondern ein als Psychotherapeut arbeitender Arzt oder ein Diplom-Psychologe damit betraut werde. Trotzdem beauftragte die BfA eine Gutachterärztin, die nicht diesem Personenkreis angehörte. Daraufhin wandte sich der Petent erneut an die BfA und erklärte, er werde in Zukunft nicht mehr dulden, daß seine Anschrift und ihn betreffende Unterlagen in irgendeiner Form weitergereicht werden. Dessen ungeachtet übergab die BfA einem weiteren Gutachter ihr vorliegende Gutachten, da aus ihrer Sicht die Vorgutachten nicht ausreichten.

Ich habe die Weitergabe der ärztlichen Unterlagen an die Gutachterärztin und an den Gutachterarzt als eine Verletzung des Sozialgeheimnisses bewertet (§ 35 Abs. 1 SGB I i. V. m. § 76 Abs. 2 Nr. 1 SGB X), da der Petent einer Offenbarung seiner dem Patientengeheimnis unterliegenden und daher dem Schutzbereich des § 76 SGB X unterfallenden personenbezogenen Daten widersprochen hatte. Dabei habe ich die Weitergabe in einem Fall nach § 25 Abs. 1 BDSG beanstandet. Im anderen Fall habe ich von einer Beanstandung Abstand genommen, nachdem die BfA insoweit einen Rechtsverstoß anerkannt und sichergestellt hat, daß sich ein solcher Fall nicht wiederholt.

In einem anderen Fall leitete die BfA trotz eines Widerspruches die Durchschrift eines ärztlichen Gutachtens, welches anläßlich eines Kurantrages erstellt worden war, an eine Ersatzkasse weiter; und zwar zusammen mit dem Bewilligungsbescheid eines Heilverfahrens. Die BfA wurde aufgrund der Eingabe der Petentin auf den Widerspruch aufmerksam und bat die Kasse, die Durchschrift des ärztlichen Gutachtens zurückzusenden, ohne sich eine Ablichtung für die dortigen Vorgänge anzufertigen und dies schriftlich zu bestätigen. Dem entsprach diese.

Die Weitergabe der auszugsweisen Durchschrift des ärztlichen Gutachtens an die Ersatzkasse verstieß gegen das Sozialgeheimnis (§ 35 Abs. 1 SGB I i. V. m. § 76 Abs. 2 Nr. 1 SGB X). Dies hat die BfA auch eingeräumt. Die BfA hat sich jedoch um Schadensbegrenzung bemüht. Ich habe daher von einer förmlichen Beanstandung abgesehen.

13.3.2 Abtretungsgläubigern darf keine Kenntnis von nachrangigen Gläubigern eines Rentenempfängers gegeben werden

Die Bundesbahnversicherungsanstalt stellte an die BfA ein Verrechnungsersuchen (§ 52 SGB I i. V. m. § 51 SGB I), woraufhin die BfA dem Petenten, der eine Rente von ihr erhielt, ein Anhörungsschreiben übermittelte (§ 24 SGB X). Darin führte sie drei Gläubiger auf, denen der Petent seinen Rentenanspruch abgetreten hatte. Dieses Schreiben sandte die BfA in Kopie auch an die drei Abtretungsgläubiger.

Darin lag insoweit ein Verstoß gegen datenschutzrechtliche Bestimmungen, als Abtretungsgläubigern Namen und Anschriften *nachrangiger* Abtretungsgläubiger offenbart wurden. Dies war für die Wahrnehmung der Rechte der vorrangigen Abtretungsgläubiger nicht erforderlich. Die BfA hat das Verfahren entsprechend korrigiert, d. h. sie offenbart nur noch Daten vorrangiger Gläubiger.

13.3.3 Nach der „letzten Regel" wird nicht mehr gefragt

Die BfA hat in dem von ihr entwickelten personalärztlichen Fragebogen nach der „letzten Regel" gefragt.

Ich habe Bedenken dagegen erhoben. Die Frage betrifft den Intimbereich. Die Antwort könnte als Indiz für eine Schwangerschaft gewertet werden und zu nicht gerechtfertigten Nachteilen führen. In diesem Zusammenhang ist zu berücksichtigen, daß der Europäische Gerichtshof für Menschenrechte eine Frage des Arbeitgebers nach dem Bestehen einer Schwangerschaft als unzulässig bewertet hat. Die BfA wird die Frage, wie sie mir mitgeteilt hat, „unter Zurückstellung erheblicher Bedenken aus medizinischer Sicht" aus ihrem Fragebogen streichen.

14 Unfallversicherung

14.1 Voraussetzungen für eine wirksame Einwilligung von Versicherten der gesetzlichen Unfallversicherung bei Erhebung, Verarbeitung und Nutzung ihrer Daten

Vor jeder Erhebung, Verarbeitung oder Nutzung von Sozialdaten, die ohne entsprechende Rechtsgrundlage erfolgt, bedarf es einer Einwilligungserklärung des Betroffenen (vgl. für den Fall der Offenbarung von Sozialdaten § 67 SGB X).

Im Zusammenhang mit der Bearbeitung mehrerer Petitionen aus dem Bereich der die Unfallversicherung durchführenden Berufsgenossenschaften, bin ich auf manche Muster von Einwilligungserklärungen und entsprechende Erläuterungsschreiben hierzu an die Versicherten gestoßen, die den datenschutzrechtlichen Anforderungen nicht genügen. Daher habe ich mich entschlossen, dieses Problem generell anzugehen. Eine für den Bereich der Unfallversicherung übergreifende Lösung ist gerade dort geboten, weil das Recht der Unfallversicherung nach wie vor in der

Reichsversicherungsordnung (RVO) geregelt ist und es an bereichsspezifischen, datenschutzrechtlichen Regelungen für diesen Zweig der Sozialversicherung fehlt. Deshalb werden dort von Betroffenen nicht selten Einwilligungen zur Erhebung, Verarbeitung und Nutzung von Sozialdaten gefordert.

Die von vielen Berufsgenossenschaften meines Zuständigkeitsbereichs verwendeten Muster weisen im wesentlichen folgende Mängel auf:

1. Im Hinblick darauf, daß auch eine Berufsgenossenschaft nur die zur Erfüllung ihrer Aufgaben erforderlichen Daten erheben, verarbeiten und nutzen darf, sind nahezu alle Einwilligungserklärungen zu pauschal formuliert.
2. In den Fällen vorgesehener Datenerhebungen und -übermittlungen werden in den Einwilligungserkärungen und den entsprechenden Erläuterungsschreiben die Stellen, bei denen Daten erhoben und jene, an die Daten übermittelt werden sollen, oftmals nicht genau genug bezeichnet.
3. Die notwendigen Hinweise an den Versicherten auf seine Mitwirkungspflicht (§ 60 SGB I) und die Folgen einer Verweigerung der Mitwirkung (§ 66 SGB I) sowie auf das Recht, einer Offenbarung von dem Patientengeheimnis unterliegenden personenbezogenen Daten zu widersprechen (§ 76 Abs. 2 SGB X), sind teils unvollständig, teils unrichtig und fehlen manchmal ganz.
4. Bei einer Reihe von Vordrucken für Einwilligungserklärungen fehlen Angaben, welche Daten zu welchem Zweck, d. h. zur Erfüllung welcher gesetzlichen Aufgabe der Berufsgenossenschaft, erhoben oder übermittelt werden sollen.
5. Einige Einwilligungserklärungen enthalten in diesem Umfang nicht notwendige und deshalb zu weitgehende Entbindungen von Berufs- oder besonderen Amtsgeheimnissen (wie etwa von der ärztlichen Schweigepflicht oder dem Steuergeheimnis). So lautete eine solche Erklärung z. B. wie folgt:

   „Ich erkläre mich damit einverstanden, daß die XY-Berufsgenossenschaft jederzeit Auskünfte von Dritten einholt. Diese Dritten befreie ich hiermit von Ihrer Schweigepflicht und ermächtige sie, der Berufsgenossenschaft alle erforderlichen Auskünfte zu erteilen. Dies gilt insbesondere für

   1. Einholung eines vollständigen Auszugs aus den Mitglieds- und Leistungskarten der Krankenkassen seit meiner Schulentlassung über meine Krankheits- und Behandlungszeiten mit Angabe der Diagnosen und der behandelnden Ärzte,
   2. ärztliche Auskünfte, Berichte und Krankengeschichten sowie Röntgenaufnahmen,
   3. Berichte über die Befunde der arbeitsmedizinischen und sonstigen ärztlichen Untersuchungen, einschließlich der Untersuchungen nach dem Arbeitssicherheitsgesetz,
   4. Einsichtnahme in die Gesundheitsakten der Landesversicherungsanstalt/Bundesversicherungsanstalt für Angestellte/Bundesknappschaft sowie die Akten des Versorgungsamtes."

   Ein dieser Einwilligungserklärung beigefügtes Informationsschreiben der Berufsgenossenschaft war nicht geeignet, den oben beschriebenen Umfang der Schweigepflichtentbindung ausreichend zu begründen.
6. Einige Einwilligungserklärungen sollten auch für die Zukunft gelten, d. h., die Versicherten sollten in Übermittlungen und Erhebungen von Daten einwilligen, die ihnen zum Zeitpunkt der Abgabe der Einwilligungserklärungen noch nicht bekannt waren oder die es noch nicht gab.

Ich habe dem Hauptverband der gewerblichen Berufsgenossenschaften eine Ausarbeitung zum Thema übersandt und angeregt, gemeinsam einheitliche datenschutzrechtliche Standards für alle Berufsgenossenschaften zu entwickeln. Darin habe ich u. a. zum Ausdruck gebracht, die Texte von Einwilligungserklärungen müßten so eindeutig abgefaßt werden, daß für den Betroffenen erkennbar ist, welche Daten zur Erfüllung welcher gesetzlichen Aufgaben bei wem von den jeweiligen Berufsgenossenschaften erhoben, oder an wen sie übermittelt werden sollen. Daher muß der Text der Einwilligung den Inhalt der Unterlagen, die erhoben oder übermittelt werden sollen, hinreichend konkret bezeichnen.

14.2 Teilweise Verbesserung des Datenschutzes bei der Berufsgenossenschaft der chemischen Industrie

Im Jahre 1990 habe ich die Berufsgenossenschaft der chemischen Industrie, Heidelberg, kontrolliert (13. TB S. 68/69). Meiner Empfehlung, das Öffnen der an die Bezirksverwaltung Heidelberg (dort ist auch der Sitz der Hauptverwaltung) gerichteten Post nur von eigenen Mitarbeitern vornehmen zu lassen, ist die Berufsgenossenschaft auch nach intensiver Erörterung und Hinweisen auf entsprechende Lösungen bei anderen Sozialversicherungsträgern nicht gefolgt. Damit besteht die Möglichkeit einer unbefugten Kenntnisnahme durch Mitarbeiter der Hauptverwaltung weiter. Den darin liegenden Verstoß gegen das Sozialgeheimnis (§ 35 SGB I) und gegen einen sicheren Umgang mit Sozialdaten (§ 79 SGB X i. V. m. § 9 BDSG) habe ich beanstandet.

Auch meinen Empfehlungen oder Forderungen in den folgenden Punkten ist die Berufsgenossenschaft bislang nicht oder nicht in hinreichendem Umfang nachgekommen:

— Unter Bezugnahme auf die Dateienübersicht der Berufsgenossenschaft habe ich letztere um eine Stellungnahme zur Zulässigkeit der Erhebung und Verarbeitung einzelner Dateien gebeten. Im Laufe des hierzu geführten Dialogs konnte die Berufsgenossenschaft insoweit teilweise befriedigende Erklärungen abgeben, teilweise hat sie sich bereit erklärt, einzelne für ihre Aufgabenerfüllung nicht erforderliche Daten künftig nicht mehr zu erheben

und zu verarbeiten. Zu einzelnen weiteren Daten dauert der Dialog noch an.

— Unterstützung des Datenschutzbeauftragten durch EDV-kundiges Personal

— Benennung von Ansprechpartnern für den Datenschutz im Bereich der Bezirksverwaltungen der Berufsgenossenschaft und den Hauptabteilungen der Hauptverwaltung als jeweils „verlängerten Arm" des Datenschutzbeauftragten (s. auch 14.3).

Zu den ebenfalls noch ungeklärten Punkten zählt die von mir geforderte datenschutzgerechte Überarbeitung von Einwilligungserklärungen zur Datenverarbeitung, insbesondere soweit sie eine Entbindung von der ärztlichen Schweigepflicht enthalten (s. auch oben 14.1).

Im Berichtszeitraum konnten hingegen die folgenden Punkte so weit geklärt werden, daß eine weitere Diskussion nicht mehr erforderlich ist:

1. *Dienstanweisung für die Geheimhaltung bei der Berufsgenossenschaft der chemischen Industrie:*

Die Dienstanweisung wurde ergänzt. Sie verlangt jetzt vom internen Datenschutzbeauftragten auch die Durchführung interner (Stichprobe-)Kontrollen und die Auswertung der Logon-Protokolle. Sie regelt außerdem die Beteiligung des Personalrats in datenschutzrechtlichen Fragen.

2. *Ergänzung und Änderung der „Aufstellung über die Zulässigkeit der Offenbarung von Sozialdaten":*

Meinen Änderungswünschen wurde entsprochen. So hat die Berufsgenossenschaft z. B. den bisher fehlenden Hinweis auf das Widerspruchsrecht der Betroffenen nach § 76 Abs. 2 SGB X und die Erforderlichkeit eines entsprechenden Hinweises auf dieses Widerspruchsrecht schriftlich fixiert. Weitergehende Änderungen und Anpassungen werden nach Inkrafttreten des 2. SGB-Änderungsgesetzes erfolgen.

3. *Abbruchprozedur nach drei fehlerhaften Paßwort-Eingaben:*

Es wurde eine Abbruchprozedur installiert, die nach drei fehlerhaften Paßwort-Eingaben reagiert (s. auch 30.2). Der interne Datenschutzbeauftragte erhält nach jedem dritten Fehlversuch ein Protokoll (mit Terminal-Identifikation, Datum, Uhrzeit und Personalnummer) und nimmt dann mit dem zuständigen Abteilungsleiter oder Geschäftsführer (bei Bezirksverwaltungen) Kontakt auf. Er fordert einen Bericht an und veranlaßt eine zeitnahe Prüfung.

4. *Diagnosedaten auf den Außenseiten von Aktendeckeln*

Um eine unbefugte Kenntnisnahme — etwa durch Boten, Registratoren oder Besucher — zu erschweren, werden künftig auf den Außenseiten der Aktendeckel Diagnosen von Versicherten nicht mehr vermerkt. Aufkleber zur Kennzeichnung der Aktendeckel dürfen nur noch den Namen des Versicherten und die Unfallnummer enthalten. Laufende Vorgänge werden aus Anlaß einer neuen Bearbeitung entsprechend korrigiert.

5. *Datenträgerentsorgung*

Eigenes Personal der Berufsgenossenschaft transportiert datenschutzrelevantes Papier zu einer Entsorgungsfirma und wirft es dort in eine Zerkleinerungsanlage. Datenträger wie Magnetbänder, Magnetbandkassetten und Disketten werden in einer Müllverbrennungsanlage ausschließlich von eigenen Mitarbeitern der Berufsgenossenschaft ohne dortige Zwischenlagerung verbrannt.

Mit diesen Regelungen wurde ein deutlicher datenschutzrechtlicher Fortschritt erzielt.

14.3 Ansprechpartner für Datenschutz in räumlich getrennten Organisationseinheiten von Berufsgenossenschaften

Im Zuge meiner Beratungstätigkeit habe ich auch für den Bereich der Unfallversicherung die Empfehlung ausgesprochen (vgl. 13. TB S. 69), auf der Ebene der Bezirksverwaltungen Ansprechpartner für den Datenschutz als „verlängerten Arm" des internen Datenschutzbeauftragten zu benennen.

Diese Empfehlung wurde unterschiedlich aufgenommen.

Eine vorbildliche Umsetzung habe ich anläßlich der datenschutzrechtlichen Kontrolle der Berufsgenossenschaft für Fahrzeughaltungen registrieren können. Deren Dienstanweisung „Aufgabenbeschreibung des Ansprechpartners für Datenschutz in Bezirksverwaltungen" greift meine Anregungen aus dem 13. Tätigkeitsbericht (S. 69) auf und sieht unter anderem vor, daß der Geschäftsführer jeder der sieben Bezirksverwaltungen eine geeignete Person als Ansprechpartner für den Datenschutz schriftlich benennt. Sie beschreibt auch dessen Qualifikationsvoraussetzungen, Aufgaben und Befugnisse. Die Ansprechpartner für den Datenschutz sind inzwischen bereits benannt.

Dagegen zeigt die Berufsgenossenschaft der chemischen Industrie (vgl. dazu auch 13. TB S. 69) bisher keine Neigung Ansprechpartner für den Datenschutz in den Hauptabteilungen der Hauptverwaltung und in ihren Bezirksverwaltungen zu bestellen. Vielmehr hat sie mitgeteilt, die primären Ansprechpartner für den Bereich Datenschutz seien in den Bezirksverwaltungen die Geschäftsführer und in der Hauptverwaltung die Hauptabteilungsleiter; daneben stünden den Bezirksverwaltungen die EDV-Ansprechpartner auch als Ansprechpartner für den Datenschutz zur Verfügung. Dies hält sie für ausreichend. Ich bedauere dies.

Wenn der Entwurf eines Zweiten Gesetzes zur Änderung des Sozialgesetzbuch Gesetz werden sollte, wird das aufgezeigte Problem durch den Gesetzgeber gelöst.

Der Entwurf des § 81 Abs. 4 Satz 2 SGB X sieht vor: „In räumlich getrennten Organisationseinheiten ist sicherzustellen, daß der Beauftragte für den Daten-

schutz bei der Erfüllung seiner Aufgaben unterstützt wird." Dies würde die von mir schon jetzt vertretene Auffassung unterstützen und eine im Grundsatz einheitliche Organisation des Datenschutzes bei den Leistungsträgern fördern.

14.4 Kein Einsichtsrecht des Arbeitgebers in die Unfallakte seines Arbeitnehmers bei der Berufsgenossenschaft

Eine Berufsgenossenschaft hat mich um eine Stellungnahme zu der Frage gebeten, ob ein Arbeitgeber mit Einwilligung seines Arbeitnehmers Einsicht in dessen Unfallakte nehmen kann.

Der Arbeitgeber ist Mitglied der Berufsgenossenschaft und hat gemäß § 725 RVO Beiträge zu dieser zu entrichten. Nach der Satzung der Berufsgenossenschaft (in Verbindung mit § 725 Abs. 2 RVO) besteht die Möglichkeit, einen Nachlaß auf den Beitrag zu erhalten, wenn die Eigenunfallbelastung des einzelnen Unternehmens niedriger ist als die Durchschnittsbelastung aller Mitgliedsbetriebe der Berufsgenossenschaft (sog. Beitragsausgleichsverfahren). Berechnungsgrundlage für die Eigen- und Durchschnittsbelastungsziffer sind die Kosten der einzelnen Arbeitsunfälle. Um diese Berechnungsgrundlage nachvollziehen zu können, verlangte der betroffene Arbeitgeber Einsicht in einzelne Unfallakten seiner Mitarbeiter. Entsprechende Einwilligungserklärungen der Arbeitnehmer lagen vor.

Ich habe in dem zur Entscheidung stehenden Fall die Einsichtnahme aus datenschutzrechtlicher Sicht als unzulässig bewertet, weil es hierfür keine Rechtsgrundlage gab.

Der Arbeitgeber war kein Beteiligter i. S. des § 12 Abs. 1 SGB X an dem Unfallverfahren zwischen seinem Arbeitnehmer und der Berufsgenossenschaft. Ihm stand daher ein Einsichtsrecht nach § 25 Abs. 1 SGB X in die Akte über dieses Verfahren nicht zu. Die nach der Satzung der Berufsgenossenschaft bestehende Möglichkeit eines Beitragsnachlasses hätte für sich allein im übrigen auch nicht die Möglichkeit eröffnet, den Arbeitgeber gemäß § 12 Abs. 2 SGB X zu dem Unfallverfahren hinzuzuziehen.

Für das Beitragsverfahren ist es ausreichend, wenn dem Arbeitgeber mit dem Beitragsfestsetzungsbescheid von der Berufsgenossenschaft die Eigen- und die Durchschnittsbelastungsziffer mitgeteilt wird. Zur Kontrolle dürfte in Fällen, in denen Zweifel an der Höhe der Eigenbelastungsziffer bestehen, dem Arbeitgeber das Recht einzuräumen sein, auf Anfrage von der Berufsgenossenschaft die Anzahl der berücksichtigten Unfälle, die Gesamthöhe der Aufwendungen und notfalls auch Aufwendungen für einzelne Unfälle mitgeteilt zu erhalten. Eine Einsichtnahme in vollständige Unfallakten einschließlich der ärztlichen Befunde ist aber nicht erforderlich.

Auch eine Einwilligung des Arbeitnehmers (§ 67 Nr. 1 SGB X) in die Einsichtnahme kann die mit der Einsichtnahme verbundene Offenbarung von Sozialdaten über das Maß des Erforderlichen hinaus nicht rechtfertigen. Im Rahmen eines Arbeitsverhältnisses besteht die Gefahr einer faktischen Zwangssituation, die eine freie Einwilligungsentscheidung des Betroffenen ausschließt. Auch ist zu berücksichtigen, daß der Arbeitnehmer gegenüber der Berufsgenossenschaft die Stellung eines Sozialleistungsberechtigten hat. Daher ist der Schutzgedanke des § 32 SGB I zu beachten. Danach darf durch eine privatrechtliche Vereinbarung nicht weiter in die Rechte des Betroffenen — hier auf informationelle Selbstbestimmung — eingegriffen werden, als dies aufgrund einer ausdrücklichen Regelung im Sozialgesetzbuch — hier § 25 SGB X — zulässig ist. Auch ein einseitiger Verzicht auf Mindestrechte beim Umgang mit personenbezogenen Daten eines Versicherten ist nach dem Rechtsgedanken des § 31 SGB I nicht zulässig.

15 Verteidigung

15.1 Besserer Schutz für Personalakten der Soldaten

Mit dem im Rahmen des Neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften vom 11. Juni 1992 (BGBl. I 1992 S. 1030ff., 1034ff.) neugefaßten § 29 des Soldatengesetzes (SG) hat der Gesetzgeber das Personalaktenrecht für Soldaten neu geordnet und soweit wie möglich den Regelungen für Beamte angeglichen (vgl. 9.2 und 13. TB S. 43). Ziel dabei war die rechtliche Gleichstellung der Soldaten mit den Beamten unter Beachtung der für Soldaten geltenden Besonderheiten (zu den ungedienten Wehrpflichtigen s. 15.2). Das Soldatengesetz hat allerdings — anders als das Beamtenrecht — die einschlägigen Vorschriften nur zum Teil im Gesetz selbst ausformuliert und im übrigen in § 29 Abs. 9 SG die Bundesregierung ermächtigt, weitere erforderliche Vorschriften im Wege einer Rechtsverordnung zu erlassen.

Bei der Erarbeitung der nach § 29 Abs. 9 SG zu erlassenden Rechtsverordnung (Personalaktenverordnung) habe ich mit dem Bundesministerium der Verteidigung noch nicht in allen Punkten Einvernehmen erzielen können. Nach meiner Auffassung enthält z. B. § 29 Abs. 3 Satz 5 SG keine Rechtsgrundlage für die im Verordnungsentwurf vorgesehene Übermittlung von Namen, Dienstgrad und Anschrift von Soldaten an den *Verband der Reservisten der Bundeswehr*, eine nichtstaatliche Organisation mit freiwilliger Mitgliedschaft. Ich bin auch der Meinung, daß die Betroffenen bei erstmaliger Speicherung ihrer Personaldaten durch die Bundeswehr *generell* über die Art der gespeicherten Daten zu unterrichten sind. Das Bundesministerium der Verteidigung beabsichtigt, hiervon abzusehen, wenn der Betroffene auf andere Weise Kenntnis von der Speicherung erlangt hat. Einen Grund für diese Abweichung von der für die Beamten geltenden Bestimmungen des § 90 g Abs. 5 BBG, die eine solche Einschränkung nicht vorsieht, vermag ich nicht zu erkennen. Mein Vorschlag entspricht auch weit besser dem Gebot der Transparenz der Datenverarbeitung, weil eine Kenntnis des Betroffenen von der Speicherung in aller Regel nicht bedeutet, daß er auch über die Art der gespeicherten Daten Bescheid weiß. Ich habe das Bundesministerium der

Verteidigung um Stellungnahme gebeten. Die Antwort hierzu liegt mir noch nicht vor.

15.2 Besserer Schutz, aber auch Probleme beim Umgang mit Personalakten von Wehrpflichtigen und Zivildienstpflichtigen

Mit dem Neunten Gesetz zur Änderung dienstrechtlicher Vorschriften wurde das Personalaktenrecht für Beamte, Soldaten, gediente Wehrpflichtige und Zivildienstpflichtige neu gefaßt, um den Schutz des Persönlichkeitsrechts der Betroffenen beim Umgang mit ihren Personalakten zu verbessern (s.o. 15.1). Demselben Ziel dient ein Entwurf der Bundesregierung für ein Zweites Gesetz zur Änderung des Wehrpflichtgesetzes, der unter anderem für die *ungedienten* Wehrpflichtigen entsprechende Regelungen trifft, wobei die wesentlichen Bestimmungen des § 29 Soldatengesetz über das Führen von Personalakten übernommen werden. Mit dem Entwurf soll erfreulicherweise eine Regelungslücke geschlossen werden, da das Wehrpflichtgesetz bisher keine Vorschriften über das Führen der Personalakten ungedienter Wehrpflichtiger enthält.

Das Bundesministerium der Verteidigung ist meinen Anregungen zum Gesetzentwurf bereits teilweise gefolgt. In dem jetzt überarbeiteten Entwurf wurden z. B. die Fristen für die Aufbewahrung der Personalakten konkretisiert und die Nutzung der Personalaktendaten ohne Einwilligung des Wehrpflichtigen auf die Zwecke des Wehrersatzwesens sowie der Personalführung und -bearbeitung beschränkt.

Weitere datenschutzrechtlich relevante Schwerpunkte des Entwurfs sind Änderungen der Vorschriften über die Erfassung, die Musterung, die Eignungsuntersuchung (bisher Eignungs- und Verwendungsprüfung) sowie eine Regelung über die Behandlung der Personalakten von Kriegsdienstverweigerern.

In meiner Stellungnahme gegenüber dem Bundesministerium der Verteidigung habe ich auf Nr. 3 der Beschlußempfehlung des Innenausschusses des Deutschen Bundestages (BT-Drucksache 12/1384, vom 28. Oktober 1991) hingewiesen und gebeten, durch eine entsprechende Ergänzung der Vorschrift über die Eignungsuntersuchung und Eignungsfeststellung (§ 20a Wehrpflichtgesetz) sicherzustellen, daß ein Wehrpflichtiger, der erst während des Musterungsverfahrens einen Antrag auf Kriegsdienstverweigerung stellt, neben der Musterung nicht auch noch der Eignungsuntersuchung unterzogen wird. Dieser Hinweis ist bisher noch nicht berücksichtigt.

Auch meine Bedenken zu den Regelungen über die Behandlung der Unterlagen von Kriegsdienstverweigerern haben noch keine Berücksichtigung gefunden. Bisher ist vorgesehen, die Akten über das Anerkennungsverfahren von Wehrpflichtigen, deren Antrag auf Anerkennung als Kriegsdienstverweigerer abgelehnt, während des Verfahrens zurückgenommen oder infolge Verzichts nach Anerkennung — dies ist jederzeit durch einfache Erklärung möglich — gegenstandslos geworden ist, solange aufzubewahren, wie dies zur Erfüllung der Wehrpflicht „erforderlich" ist. Ich habe dagegen die Vernichtung dieser Unterlagen spätestens sechs Monate nach der rechtskräftigen Entscheidung über den Antrag oder die Erklärung des Betroffenen empfohlen. Leider hat das Kabinett den Gesetzentwurf insoweit unverändert verabschiedet. Ich werde mein datenschutzrechtliches Anliegen im Laufe des Gesetzgebungsverfahrens weiter verfolgen.

16 Zivildienst

16.1 Regelungen über Umgang mit Personalakten der Zivildienstpflichtigen und Zivildienstleistenden verbessert

In das Zivildienstgesetz (ZDG) wurde eine datenschutzrechtlich erfreuliche Regelung über den Umgang mit Personalakten von Zivildienstpflichtigen und Zivildienstleistenden aufgenommen (im Rahmen des 9. Gesetzes zur Änderung dienstrechtlicher Vorschriften, s. o. 9.2, 15.1 und 13. TB S. 43).

Die Eingabe eines Arztes, die auch in der Presse Beachtung fand, hat gegen Ende des Gesetzgebungsverfahrens auf meine Initiative hin noch zu einer wichtigen Ergänzung des § 36 ZDG geführt. Der *Privatarzt* hatte einen Zivildienstleistenden im Rahmen der nach § 35 ZDG geltenden freien Heilfürsorge — anders als Soldaten haben Zivildienstleistende, da im Zivildienst eigene medizinische Versorgungseinrichtungen fehlen, freie Arztwahl — dienstunfähig geschrieben. Das Bundesamt für den Zivildienst (BAZ) hatte ihn aufgefordert, auch die *Diagnose* mitzuteilen. Dazu war er nicht bereit.

Meine Überprüfung ergab, daß das für den Zivildienst zuständige Bundesministerium für Frauen und Jugend (BMFJ) und das BAZ *in allen Krankheitsfällen*, in denen Dienstunfähigkeit bescheinigt wird, auch die Diagnosen für die Bearbeitung der Krankschreibungen im Ärztlichen Dienst des BAZ verlangen und für erforderlich ansehen. Bei einem Eingang von jährlich ca. 240 000 Arbeits-/Dienstunfähigkeitsbescheinigungen befanden sich damit Millionen dieser Unterlagen mit sensiblen personenbezogenen Daten in den Gesundheitsunterlagen der (auch ehemaligen) Zivildienstleistenden, ohne daß dafür eine Rechtsgrundlage vorhanden war.

Das BMFJ und das BAZ waren der unzutreffenden Ansicht, eine Rechtsgrundlage für die Erhebung und Übermittlung der medizinischen Daten der Zivildienstleistenden durch Privatärzte ergäbe sich aus § 39 Abs. 1 Nr. 3 ZDG in Verbindung mit dem auf der Grundlage des § 75 Abs. 3 SGB V geschlossenen Vertrag mit der Kassenärztlichen Bundesvereinigung (KBV), der die ärztliche Versorgung der Zivildienstleistenden sicherstellen soll. Die Kassenärzte werden zwar durch § 75 Abs. 3 SGB V in Verbindung mit diesem Vertrag verpflichtet, Behandlungen der Zivildienstleistenden durchzuführen, nicht aber zur Bekanntgabe der Diagnosen ermächtigt, auch wenn dies auf einem von den Vertragspartnern BMFJ/BAZ und KBV entwickelten *Formular Dienstunfähigkeitsbescheinigung* so vorgesehen ist. Behandlungen im Rahmen der Erkrankung eines Zivildienstleistenden

sind aber auch von den von Amts wegen durchzuführenden Untersuchungen nach § 39 ZDG zu unterscheiden, die die Prüfung der Zivildienstfähigkeit zum Gegenstand haben und die Grundlage für das Ausscheiden eines Zivildienstleistenden aus dem Zivildienst bei — inzwischen eingetretener — Zivildienstunfähigkeit sein können. Diese Untersuchungen sind dem Ärztlichen Dienst des BAZ und besonderen von ihm benannten regional zuständigen sogenannten Beauftragten Ärzten vorbehalten.

In § 36 Abs. 8 Nr. 5 ZDG ist nunmehr — näheres ist durch eine Rechtsverordnung zu bestimmen — die grundsätzliche Befugnis zur Offenbarung von medizinischen Daten durch Personen i. S. d. § 203 Abs. 1 Nr. 1 und 2 StGB enthalten: *Unter der Voraussetzung der Erforderlichkeit* für die Aufgabenerfüllung des BAZ dürfen danach private Ärzte und private Zahnärzte medizinische Daten einschließlich der Diagnosen gegenüber dem BAZ — Ärztlichem Dienst und der für die Abrechnung der Heilfürsorgeleistungen zuständige Organisationseinheit — im Rahmen der unentgeltlichen ärztlichen Versorgung der Zivildienstleistenden offenbaren. Dies gilt nach dem Wortlaut der Vorschrift auch für die Beauftragten Ärzte, die vom BAZ mit der Untersuchung von Dienstpflichtigen oder mit der Erstellung von Gutachten beauftragt worden sind.

Das BMFJ hat bisher die in § 36 Abs. 8 Nr. 5 ZDG vorgesehene Rechtsverordnung noch nicht erlassen. In diesem Rahmen habe ich erneut die Frage aufgegriffen, ob Diagnosen *in jedem Einzelfall* einer Dienstunfähigkeit wirklich erforderlich sind. Die vom BMFJ bisher hierfür vorgetragenen Gründe haben mich z. B. für die Fälle eindeutig kurzfristiger Erkrankungen noch nicht überzeugt. Ich strebe deshalb eine Reduzierung der Datenübermittlung in diesen Fällen an.

16.2 Akten von Kriegsdienstverweigerern

16.2.1 Bundesamt für den Zivildienst zeigt erfreuliche Praxis bei Vernichtung von Akten aus laufenden Verfahren

Die Akten über das Anerkennungsverfahren von Kriegsdienstverweigerern sind mit Ausnahme des Anerkennungsbescheides spätestens sechs Monate nach Ableistung des Zivildienstes zu vernichten; wird ein anerkannter Kriegsdienstverweigerer nicht herangezogen, sind diese Akten nach Ablauf des Jahres zu vernichten, in dem er das 32. Lebensjahr vollendet hat. Diese Regelung in § 2 Abs. 6 des Kriegsdienstverweigerungsgesetzes (KDVG) dient dem Schutz der persönlichen Angaben des Betroffenen in den Akten über seine Gewissensentscheidung (vgl. 12. TB S.24).

Auf meine Empfehlung und entsprechende Weisung des damaligen Bundesministers für Jugend, Familie, Frauen und Gesundheit hin vernichtet das Bundesamt für den Zivildienst seit dem 1. Februar 1990 die Anerkennungsunterlagen mit Ausnahme des Anerkennungsbescheides bereits *unmittelbar nach Bestandskraft des Bescheides* in der für das Anerkennungsverfahren zuständigen Abteilung (vgl. 11. TB S.19). Die für den Einsatz der Kriegsdienstverweigerer zuständige Abteilung erhält somit aus dem Anerkennungsverfahren nur diesen Bescheid. Diese erfreuliche Praxis geht über die erwähnte gesetzliche Anforderung hinaus und entspricht dem Gebot funktionalen Datenschutzes, wonach innerhalb der Behörde die jeweiligen Organisationseinheiten nur die Daten erhalten dürfen, die sie für die Erfüllung ihrer Aufgaben benötigen. In gleicher Weise wird inzwischen mit den Anerkennungsunterlagen der durch die Ausschüsse für Kriegsdienstverweigerung, die Kammern für Kriegsdienstverweigerung und durch Verwaltungsgerichte anerkannten Kriegsdienstverweigerer verfahren; diese Unterlagen werden unmittelbar nach Eingang im Bundesamt für den Zivildienst mit Ausnahme des Anerkennungsbescheides vernichtet.

16.2.2 Bundesamt für den Zivildienst konnte Frist für Vernichtung von Unterlagen aus Verfahren vor 1989 nicht einhalten

Nach § 23 KDVG sind die Akten aus Anerkennungsverfahren derjenigen anerkannten Kriegsdienstverweigerer, die ihren Zivildienst bereits vor dem Inkrafttreten des vorgenannten § 2 Abs. 6 KDVG abgeleistet haben, innerhalb von drei Jahren nach dem Inkrafttreten dieser Vorschrift zu vernichten. Diese Frist ist Anfang Juli 1992 abgelaufen. Auf meine entsprechenden frühzeitigen Hinweise und Nachfragen wurde mir vom Bundesministerium für Frauen und Jugend mitgeteilt, daß das Bundesamt für den Zivildienst wegen besonderer Belastungen durch die Herstellung der deutschen Einheit und wegen des steilen Anstiegs der Zahl von Anerkennungsverfahren im Zusammenhang mit dem Golfkrieg nicht in der Lage war, den Termin einzuhalten. Insgesamt geht es hierbei um Unterlagen von ca. 300 000 Kriegsdienstverweigerern.

Auf meine dringende Empfehlung hin hat das Bundesministerium für Frauen und Jugend das Bundesamt für den Zivildienst angewiesen, die Vernichtung der Anerkennungsteile der Personalunterlagen der Kriegsdienstverweigerer mit dem größtmöglichen Personaleinsatz weiterzutreiben. Zu diesem Zweck ist eine Arbeitsgruppe mit elf Zeitangestellten gebildet worden. Das Verfahren wird nach Angaben des Bundesministeriums für Frauen und Jugend in spätestens drei Jahren abgeschlossen sein. Bis dahin sind die Daten in den Unterlagen auf meine Veranlassung hin gesperrt worden, d. h. sie dürfen ohne Einwilligung des Betroffenen grundsätzlich nicht verarbeitet oder genutzt, insbesondere nicht an Dritte übermittelt werden.

Besondere Schwierigkeiten ergeben sich bei ca. 60 000 Altakten, die nur noch mikroverfilmt vorliegen. Nach eingehender Prüfung habe ich mich davon überzeugen lassen, daß es hingenommen werden muß, an die Stelle der vom Gesetz an sich geforderten Vernichtung für eine gewisse Zeit eine Sperrung der Daten treten zu lassen (§§ 12 Abs. 4, 35 Abs. 3 Nr. 3 BDSG). Bei der Mikroverfilmung wurden auf jeder Seite der Personalunterlagen Bildmarken (Blips) angebracht, die ein Wiederauffinden mit Hilfe automatisiert gespeicherter Fundstellennachweise ermöglichen. Die Reihenfolge der Blips darf aus technischen

Gründen nicht unterbrochen werden; würden einzelne Blips auch nur geringfügig beschädigt, wäre ein Wiederauffinden aller Personalunterlagen auf dem jeweiligen Film nicht mehr möglich. Dies verbietet es, Teile des Films herauszutrennen. Aber auch das Risiko, Blips beim Schwärzen einzelner Bilder oder beim Abkratzen der Bildoberfläche zu beschädigen, ist hoch. Eine Löschung der entsprechenden Teile der Mikrofilme wäre somit nur mit einem unverhältnismäßig hohen Aufwand möglich.

Ich werde die Angelegenheit weiter verfolgen und gemeinsam mit den beteiligten Stellen nach einer Lösung suchen.

17 Gesundheitswesen

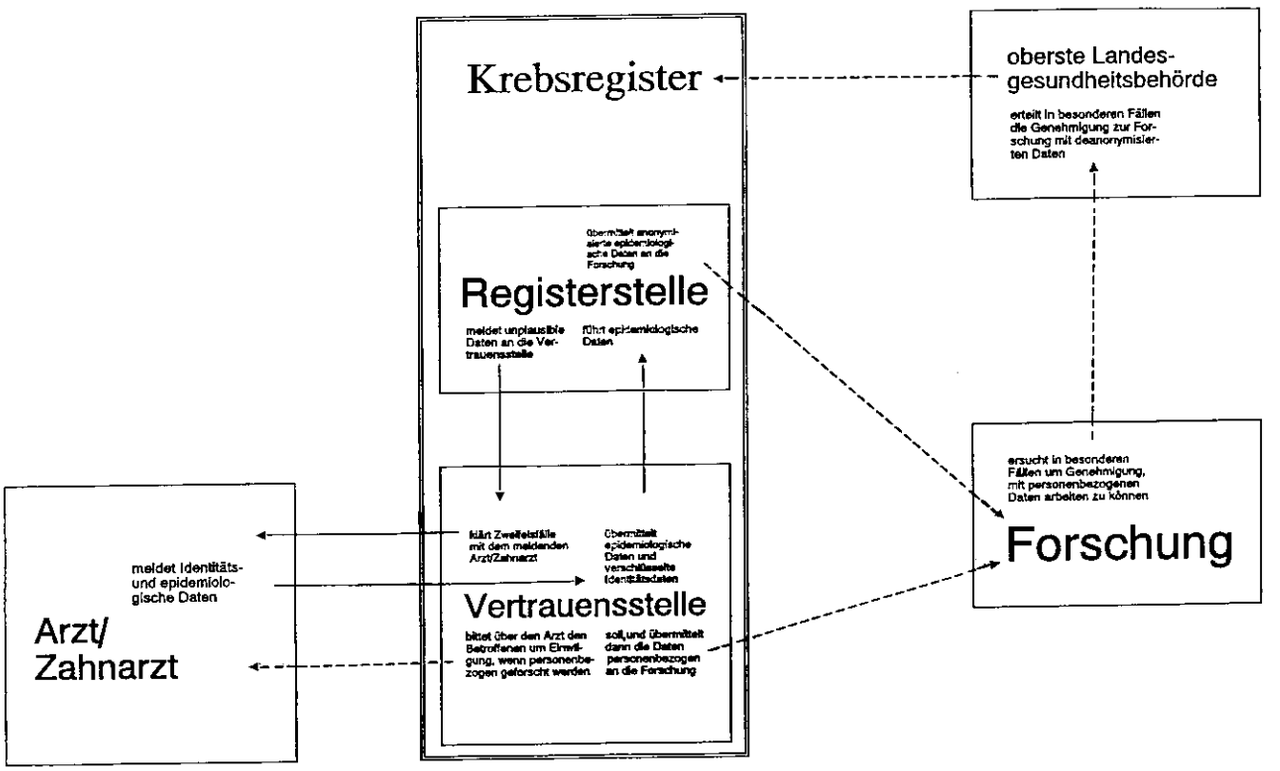
17.1 Bundeskrebsregistergesetz

Das Bundesministerium für Gesundheit hat einen Entwurf eines Bundeskrebsregistergesetzes übersandt, der auf dem an der Mainzer Universitätsklinik entwickelten Treuhandmodell basiert. Der Leiter des Kinderkrebsregisters, das dort geführt wird, hat das Treuhandmodell im Berichtszeitraum den Datenschutzbeauftragten des Bundes und der Länder vorgestellt und mit diesen intensiv und mit guten Ergebnissen für eine praktikable Lösung diskutiert.

Nach dem Gesetzentwurf des BMG sollen die Länder flächendeckend bevölkerungsbezogene Krebsregister führen, die organisatorisch aus selbständigen Vertrauens- und Registerstellen bestehen (vgl. Abb. unten). Ärzte und Zahnärzte sollen berechtigt sein, an die regional zuständige Vertrauensstelle Krebserkrankungen personenbezogen zu melden. Zur Sicherung der Aussagefähigkeit der Krebsregister sollen die Gesundheitsämter die amtlichen Leichenschauscheine den Vertrauensstellen zuleiten. In der Vertrauensstelle werden die den Krebskranken identifizierenden Daten (Identitätsdaten wie Name, Vorname, Anschrift sowie Geburts- und ggf. Sterbedatum) von den die Krebserkrankung betreffenden Daten (epidemiologischen Daten wie z. B. Geschlecht, Monat und Jahr der Geburt und ggf. des Todes, Beruf, Tumordiagnose, Art der Therapie) getrennt. Die Identitätsdaten werden verschlüsselt. Die epidemiologischen Daten und die verschlüsselten Identitätsdaten werden zusammen mit einer gemeinsamen, auf der Basis von Identitfikationsdaten gebildeten Kontrollnummer an die zugehörige Registerstelle übermittelt. Dort werden die Daten zu etwa bereits vorhandenen Daten mit derselben Kontrollnummer hinzugefügt und auf Plausibilität geprüft. Zweifelsfälle werden der Vertrauensstelle vorgelegt, die sie mit dem meldenden Arzt klärt.

Bei der Vertrauensstelle sollen die Daten unverzüglich nach der abschließenden Bearbeitung durch die Registerstelle, spätestens jedoch drei Monate nach der Übermittlung gelöscht und die den Meldungen zugrunde liegenden schriftlichen Unterlagen vernichtet werden, so daß dort keine personenbezogenen Daten verbleiben.

Eine Entschlüsselung der Identitätsdaten ist nur für Maßnahmen des Gesundheitsschutzes und bei wichtigen und auf andere Weise nicht durchzuführenden, im öffentlichen Interesse stehenden Forschungsvorhaben vorgesehen und bedarf der Genehmigung der obersten Landesgesundheitsbehörde.



Diesen Ansatz zur Schaffung eines Krebsregisters halte ich für sinnvoll, auch wenn aus datenschutzrechtlicher Sicht ein Melderecht der Ärzte das zu beachtende Selbstbestimmungsrecht der Patienten nicht ohne weiteres zur Geltung kommen läßt. Der BMG hat jedoch Regelungen vorgeschlagen, die dem Recht der Patienten an seinen Daten Rechnung tragen. So haben die meldenden Ärzte und Zahnärzte den Patienten von der Meldung zu unterrichten, soweit nicht zu erwarten ist, daß diesem dadurch gesundheitliche Nachteile entstehen können. Widerspricht der Patient der Meldung, hat die Meldung zu unterbleiben. Ist die Meldung bereits erfolgt, sind die gemeldeten Daten im Krebsregister zu löschen. Darüber hinaus hat der Patient das Recht, sich über einen von ihm benannten Arzt oder Zahnarzt mündlich umfassend darüber zu informieren, ob und welche Daten zu seiner Person im Krebsregister gespeichert werden. Diese an § 42 Bundeszentralregistergesetz orientierte Regelung halte ich im Sinne des Patienten für sachgerecht. Sie gewährleistet einerseits die medizinische Beratung und berücksichtigt insofern die besondere Situation, in der sich ein an Krebs Erkrankter befindet. Andererseits verhindert sie die Möglichkeit sog. Negativatteste, d. h. Atteste, die bestätigen, daß eine Person nicht wegen einer Krebserkrankung registriert ist. Auch die Forschung mit personenbezogenen Daten ist nur nach Einholung der schriftlichen Zustimmung des Patienten möglich.

Das Prinzip des von mir schon früher unterstützten Verschlüsselungsmodells (vgl. 12. TB S. 71 und 13. TB S. 105) wird dadurch verwirklicht, daß die Identitätsdaten verschlüsselt werden.

Auch mit Blick auf das Krebsregistersicherungsgesetz (s. o. 2.9) möchte ich hervorheben, daß die konstruktive Zusammenarbeit zwischen dem federführenden Ressort (hier: Bundesministerium für Gesundheit), den Datennutzern (hier: Forschern) und den Datenschutzbeauftragten zu guten Ergebnissen geführt hat. Umso größer war meine Verwunderung über Pressemeldungen, nach denen der Einführung eines flächendeckenden Krebsregisters in Hessen Datenschutzgründe entgegenstünden. Der Hessische Datenschutzbeauftragte ist dem zu Recht entgegengetreten.

17.2 Genomanalyse

Die parlamentarische Diskussion über die Chancen und Risiken der Gentechnologie war im Berichtszeitraum überwiegend von der Forderung nach einer Novellierung des Gentechnikgesetzes geprägt. Dieses Gesetz betrifft im wesentlichen Sicherheitsfragen beim Umgang mit genetisch veränderten Organismen und damit keine Datenschutzfragen. Aus Anlaß dieser Beratungen wurden in den Ausschüssen des Deutschen Bundestages aber auch Entscheidungen des Gesetzgebers über Grundfragen der Analyse des menschlichen Genoms angemahnt (s. BT-Drucksache 12/3658). Denn die Bemühungen um die Entschlüsselung der Desoxyribonukleinsäure — engl.: desoxyribonucleinacid (DNA) —, in der die Erbanlagen verkörpert sind, lassen erwarten, daß bald aus der Struktur der DNA eines Menschen auf dessen Eigenschaften geschlossen werden kann. Für solche DNA-Analysen werden kleine Blut- oder Gewebeproben ausreichen und die möglichen Erkenntnisse werden noch über das hinausgehen, was heute durch andere Formen der Genomanalyse, wie z. B. die Chromosomenanalyse, an Informationen über einen Menschen gewonnen werden kann. Die Zulässigkeit ihrer Anwendung und die Grenzen der Nutzung der dabei gewonnenen Erkenntnisse müssen durch den Gesetzgeber verantwortlich festgelegt werden.

Wegen des damit gegebenen Entscheidungsbedarfs begrüße ich die „Entschließung des Bundesrates zur Anwendung gentechnischer Methoden am Menschen" (BR-Drucksache 424/92 [Beschluß]) vom 16. Oktober 1992, mit der dieser auf Einzelprobleme und Lösungsansätze hinweist und in der es u. a. heißt:

> „Angesichts der grundlegenden Bedeutung dieser Fragen auch für die zukünftigen Generationen ist der Bundesrat der Auffassung, daß vorhandene Regelungslücken außerhalb des Gentechnikgesetzes unverzüglich beseitigt werden müssen und eine umfassende Konzeption für bundeseinheitliche Regelungen zu erarbeiten ist, die einen ethisch und verfassungsrechtlich unbedenklichen Umgang mit der Humangenetik gewährleisten."

Zur Vorbereitung von rechtlichen Regelungen beschäftigen sich Experten verschiedener Fachrichtungen im Rahmen von Diskussionen und Forschungsprojekten, die z. T. vom BMFT gefördert werden, mit den Folgen der durch die DNA-Analyse erreichbaren Erkenntnisse über den Menschen. Ich halte dies für geboten und habe mich im Rahmen meiner Möglichkeiten daran beteiligt. Denn wenn sogar mit erheblicher staatlicher Förderung die Kartierung und Entschlüsselung der in den Chromosomen liegenden Erbanlagen als internationales Projekt betrieben wird, dann müssen auch Lösungen für die mit dieser Ausforschungsmöglichkeit des Menschen verbundenen ethischen und rechtlichen Probleme gesucht werden, wozu auch der Umgang mit den zu gewinnenden Daten gehört.

Bei der DNA-Analyse geht es häufig um Gesundheitsdaten, z. B. um die Frage, mit welcher Wahrscheinlichkeit eine bestimmte genetisch bedingte Erkrankung beim Betroffenen zu erwarten ist. Deshalb sind Ärzte an diesen Diskussionen nicht nur interessiert, sondern auch aktiv beteiligt. Dies hat dazu beigetragen, daß dem Datenschutz, der das Patientengeheimnis schützt und ergänzt, von Anfang an eine erhebliche Bedeutung zugemessen wurde.

Obwohl die Erörterungen noch längst nicht abgeschlossen sind und auch immer neue Gesichtspunkte einzubeziehen sind, lassen sich trotz der deswegen nötigen Vorbehalte schon jetzt einige Forderungen formulieren:

— *Gesetzesvorbehalt*

DNA-Analysen sind empfindliche Eingriffe in die Privatsphäre. Sie dürfen nur durchgeführt und ihre Ergebnisse dürfen nur verwendet werden, soweit der Betroffene eingewilligt hat oder ein Gesetz dies aus-

drücklich erlaubt, z. B. im Rahmen eines Strafverfahrens (s. dazu 5.1.5). Die Gewährung eines Vorteils darf nur in den Fällen von der Einwilligung des Betroffenen in eine DNA-Analyse abhängig gemacht werden, in denen dies bereichsspezifisch gesetzlich geregelt ist.

— *Arbeitsverhältnis*

Zur Zeit gibt es keinen überzeugenden Grund für eine gesetzliche Erlaubnis, vor dem Abschluß eines Arbeitsvertrages die Ergebnisse einer DNA-Analyse zu verlangen. Falls für ein bestehendes Arbeitsverhältnis — z. B. aus Gründen des Arbeitsschutzes — eine DNA-Analyse in bestimmten Fällen erlaubt werden sollte, ist präzise vorzugeben, worauf sich die Analyse im jeweiligen Fall richten darf und wie mit den daraus gewonnenen Erkenntnissen umzugehen ist.

— *Versicherungsverhältnisse*

Nach den heutigen Erkenntnissen ist die Nutzung von DNA-Analysen für den Abschluß oder die Prämienberechnung von Versicherungen nicht erforderlich. Dies wird auch — jedenfalls in der deutschen — Versicherungswirtschaft so gesehen. Trotzdem halte ich im Hinblick auf Entwicklungen im internationalen Bereich eine entsprechende Festlegung im Versicherungsvertragsgesetz für zweckmäßig. Wir sollten nicht dahin kommen, daß Eltern sich überlegen müssen, ob sie einem Kind das Leben schenken können, weil sie für dieses keinen Versicherungsschutz in einer privaten Krankenversicherung erhalten.

— *Konkretisierung der Erlaubnisse*

Weil die Verhältnismäßigkeit — und damit Zulässigkeit — einer gesetzlichen Erlaubnis zur Durchführung von DNA-Analysen stets aus der Nützlichkeit der Untersuchungsergebnisse für einen konkreten Zweck begründet werden muß, können und müssen Erlaubnisse exakt begrenzt sein. Die damit gebotenen kasuistischen, am jeweiligen Stand der Erkenntnismöglichkeiten orientierten Regelungen scheinen am ehesten geeignet, die Probleme von DNA-Analysen zu beherrschen. Dazu gehört auch, daß stets nur die Anwendung solcher Analyseverfahren erlaubt wird, die so eng wie möglich am jeweiligen Untersuchungszweck orientiert sind, um von vornherein die beiläufige Miterhebung nicht erforderlicher Daten über Erbanlagen soweit irgend möglich zu vermeiden.

— *Löschung*

Unverzüglich nach dem Erreichen des unmittelbaren Zwecks der Analyse, also z. B. nachdem eine darauf beruhende Entscheidung getroffen ist, sind die durch DNA-Analyse gewonnenen Daten über den Betroffenen einschließlich etwaiger Neben- und Zwischenergebnisse zu löschen. Dies ist vertretbar, weil bei Bedarf die Analyse unter denselben Bedingungen wiederholt werden kann, und es ist geboten, weil jede längere Aufbewahrung der Einzeldaten das Risiko der zweckfremden Nutzung vergrößert. Entfällt der rechtfertigende Grund für eine DNA-Analyse, z. B. weil der Betroffene seine Einwilligung widerrufen hat, so sind auch die gewonnenen Daten und die daraus gezogenen Folgerungen zu löschen, soweit sie nicht, z. B. zur Abwicklung eines Vertrages, noch benötigt werden.

— *Strafandrohung*

Jede unerlaubte Durchführung einer DNA-Analyse und auch jede unerlaubte Nutzung der aus einer DNA-Analyse gewonnenen personenbezogenen Daten muß unter einer wirksamen Strafandrohung stehen. Dies ist geboten, weil das Analysematerial leicht und unauffällig gewonnen werden kann und der Betroffene nach diesem Zeitpunkt keine Möglichkeit hat, die Durchführung der Analyse zu verhindern.

— *Forschung*

Mit den aus DNA-Analysen gewonnenen personenbezogenen Daten über Erbanlagen darf weder ohne Wissen noch gegen den Willen des Betroffenen geforscht werden. Deshalb muß für die Verarbeitung dieser Daten für Forschungszwecke die Einwilligung der Betroffenen eingeholt werden, soweit nicht von Anfang an mit völlig anonymen Daten gearbeitet wird.

18 Verkehrswesen

18.1 Offenbarung von Verfahrensbeteiligten im Gesetzgebungsverfahren abgestellt (Stendal-Umfahrung)

An den Beratungen der Bundesregierung zu dem Entwurf eines Gesetzes über den Bau der „Südumfahrung Stendal" der Eisenbahnstrecke Berlin-Oebisfelde war ich nicht beteiligt worden. Erst nach Veröffentlichung des Gesetzentwurfs als Bundesrats-Drucksache wurde erkannt, daß die dem Entwurf beigefügten Anlagen eine Reihe von zum Teil sensiblen personenbezogenen Daten enthielten. So war den Niederschriften über bereits stattgefundene Informationsveranstaltungen z. B. zu entnehmen, wer — nachdem für in Anspruch zu nehmende Grundstücke Qudratmeterpreise von DM 1,00 bis DM 1,80 DM genannt worden waren — die ketzerische Frage nach den entsprechenden Preisen bei der Strecke Hannover–Würzburg gestellt hatte. Datenschutzrechtlich sensible Angaben enthielten auch das Grunderwerbsverzeichnis und die veröffentlichten Unterlagen über die Einwendungen von Betroffenen. Im Grunderwerbsverzeichnis befanden sich beispielsweise die Namen und Adressen der Grundstückseigentümer mit den dazugehörigen Angaben über Altenteile einschließlich der Höhe der Beträge und der Namen der Begünstigten sowie Angaben über dingliche Rechte an den Grundstücken. In Einzelfällen waren auch die Personen mit Name und Adresse genau bezeichnet, die eine Rückübertragung von Grundstücken beantragt hatten.

Auf die Unzulässigkeit der Veröffentlichung dieser personenbezogenen Daten — auch in der Form eines Gesetzentwurfs — habe ich die Bundesregierung hingewiesen. Dabei konnte über die Rechtslage gar kein Zweifel bestehen. Bereits in Beschlüssen vom 14. Oktober 1987 (BVerfGE 77, S. 121) und vom

27. Juli 1990 (NVwZ 1990, S. 1162) hatte das Bundesverfassungsgericht festgestellt, daß die öffentliche Bekanntmachung vergleichbarer Daten in einem Planfeststellungsverfahren unzulässig in Grundrechte der Betroffenen eingreift. Bei der Abfassung und Veröffentlichung des Gesetzentwurfes war dies jedoch nicht bedacht worden.

Auf mein Schreiben und nach Intervention einiger Bundesländer hat der Bundesrat die weitere Versendung der Bundesrats-Drucksache gestoppt, die noch beim Bundesrat vorhandenen Exemplare der Drucksache vernichtet und die Bundesregierung aufgefordert, das Recht auf informationelle Selbstbestimmung der betroffenen Bürger sicherzustellen. Das federführende Bundesministerium für Verkehr hat in der Neuauflage des Gesetzentwurfs die Namen aller natürlichen Personen, insbesondere der Eigentümer und Einwender, durch Schlüsselnummern ersetzt. Das Schlüsselverzeichnis steht lediglich den Mitgliedern der gesetzgebenden Körperschaften auf Anfrage zur Verfügung. Dagegen bestehen keine Bedenken. Entsprechend wurde bei später vorgelegten Gesetzentwürfen ähnlichen Inhalts verfahren.

18.2 Nur wenige Probleme mit dem Konzept von ZEVIS — Der ZEVIS-Bericht der Bundesregierung —

Über das Zentrale Verkehrsinformationssystem ZEVIS habe ich in den vergangen Jahren schon mehrfach berichtet (s. zuletzt: 13. TB S. 55ff.). Inzwischen liegt der auf Anforderung des Bundestages erstellte ZEVIS-Bericht der Bundesregierung vor, an dessen Erarbeitung ich beteiligt war.

Insgesamt hat sich ZEVIS als zweckmäßiges System mit auch aus datenschutzrechtlicher Sicht tragfähiger Rechtsgrundlage bewährt. Von den gleichwohl bestehenden Problemen greife ich an dieser Stelle nur zwei heraus:

1. Entgegen der gesetzlichen Anforderung (§ 13 Abs. 1 FRV i. V. m. § 36 Abs. 5 Nr. 2 StVG) ist für das Kraftfahrt-Bundesamt (KBA) nicht immer erkennbar, welche Dienststelle einen Abruf tätigt. So werden von Bayern seit Jahren regionale Vermittlungsrechner eingesetzt, die sich dem KBA gegenüber wie abrufende Terminals verhalten und deshalb auch virtuelle Terminals genannt werden. Die über das virtuelle Terminal auf den Datenbestand zugreifenden Terminals bleiben dem KBA unbekannt. Es kann daher auch nicht feststellen, ob die bereitgehaltenen Daten ihrer Art nach für jede so zugreifende Dienststelle erforderlich sind und die Einrichtung des automatisierten Abrufverfahrens in diesen Fällen angemessen ist, wie es § 36 Abs. 5 Nr. 1 StVG verlangt. Es hätte den Anschluß von virtuellen Terminals deshalb ablehnen müssen. Zwar hält das Bayerische Landeskriminalamt für jeden Abruf die Identität des abrufenden Beamten sowie zusätzliche Angaben fest, die der — sonst nur stichprobenweisen — Zusatzprotokollierung nach § 36 Abs. 7 StVG entsprechen. Bedenklich ist aber, daß die Verwaltung seit Jahren die Rechtslage nicht beachtet, sich aber auch nicht um eine Änderung bemüht hat.

   Die Bundesregierung hat in dem Bericht ihre Absicht bekundet, mit Bayern über die technische Anpassung des Systems oder — wenn dies unverhältnismäßig wäre — über eine Anpassung der Rechtslage zu verhandeln. Eine Lösung ist dringend geboten und wohl auch möglich, zumal nach meiner Kenntnis in anderen Bundesländern technisch ähnliche Vermittlungsverfahren unter Beachtung des geltenden Rechts angewandt werden.

2. Das Bayerische Polizei-Datenverarbeitungsnetz erlaubt dem Nutzer bei der Anmeldung im System bis zu vier folgenlose Fehlversuche; erst beim fünften Fehlversuch wird der Anschluß gesperrt. Nach der Rechtslage dürfen für ZEVIS aber höchstens zwei Fehlversuche zugelassen werden (§ 13 Abs. 2 FRV i.V.m. § 36 Abs. 5 StVG). Das wird vom KBA auch beachtet. Der Vermittlungsrechner gibt die Kennung für ein virtuelles Terminal gegenüber dem KBA aber automatisch und damit immer richtig ein. Über das bayerische Polizeisystem, das bei der Anwahl des Vermittlungsrechners vier Fehlversuche zuläßt, kann ZEVIS daher mit dieser Zahl von Fehlversuchen genutzt werden. Ich sehe darin die Mindererfüllung einer durch Rechtsnorm vorgeschriebenen Sicherheitsauflage. Ich habe das KBA nachdrücklich aufgefordert, das Problem unter Einschaltung des Bundesministeriums für Verkehr baldmöglichst zu lösen. Der Bayerische Landesbeauftragte für den Datenschutz unterstützt meine Position.

18.3 Fragen aus der ZEVIS-Praxis

Beim Betrieb von ZEVIS treten verschiedene Einzelprobleme auf, was bei einem System mit weit über 60 Mio. Datensätzen und rund 10 Mio. Abfragen pro Jahr nicht verwundern kann.

18.3.1 Zentrale Fragen des ZEVIS-Betriebes

Wenn eine Behörde um die Einrichtung eines ZEVIS-online-Anschlusses ersucht, nimmt das Kraftfahrt-Bundesamt konkrete Prüfungen, ob die Zugangsvoraussetzungen zu ZEVIS nach § 36 Abs. 5 Nr. 1 StVG vorliegen, nicht vor. Es prüft nur die Plausibilität und verläßt sich im übrigen auf die Erklärungen der fachaufsichtsführenden Dienststellen der abrufberechtigten Behörden. Darin fehlte aber bisher ein Hinweis auf diese Zugangsvoraussetzungen; es war deshalb zumindest möglich, daß keine der beiden Seiten die Zulässigkeit des online-Anschlusses geprüft hatte. Das KBA ist inzwischen meiner Empfehlung gefolgt und verwendet nun einen Vordruck, in dem die ersuchende Stelle ausdrücklich versichert, daß die gesetzlich geforderten Voraussetzungen für den ZEVIS-Anschluß vorliegen.

Weiter habe ich das Kraftfahrt-Bundesamt darauf hingewiesen, daß die Abrufe zwar protokolliert werden, die Zulässigkeit der Abrufe aber noch nicht im

gebotenen Umfang tatsächlich überprüft wird. Ein Überprüfungsverfahren wurde nur einmal vor längerer Zeit durchgeführt. Effektiv ist dieses Verfahren jedoch nur, wenn es jederzeit ohne größere Probleme einsatzbereit ist und deshalb auch tatsächlich mit einer gewissen Regelmäßigkeit eingesetzt wird. Hierzu ist das KBA aber auf die Mitwirkung der ZEVIS-Nutzer angewiesen.

18.3.2 Die Nutzung von Funkterminals

Besondere Risiken liegen in dem zunehmenden Einsatz von Funkterminals bei der ZEVIS-Nutzung. In Bayern und Nordrhein-Westfalen sind Datenfunkverfahren schon realisiert. Seit langem fordere ich bei ZEVIS-Abfragen eine Verschlüsselung des Datenfunks. Neue Aktualität hat diese Forderung durch die Freigabe der Allbandempfänger (Scanner) erhalten (s. auch 21.10), mit denen dieser Datenfunk problemlos abgehört und aufgezeichnet werden kann. Konkrete Schritte in Richtung auf die kryptographische Verschlüsselung halte ich auch hier für geboten.

18.3.3 ZEVIS-Nutzung durch das Bundeskriminalamt

Die Zusatzprotokollierung erfolgte beim Bundeskriminalamt (BKA) nicht in allen Fällen entsprechend der Regelung des § 14 FRV. Insbesondere fehlte häufig die für eine Überprüfung des Abrufs notwendige Angabe des Aktenzeichens oder eines ähnlich konkreten Fallbezugs. Ich habe das BKA darauf hingewiesen, daß diese Fehler rechtzeitig hätten festgestellt werden können, wenn die vom Kraftfahrt-Bundesamt erstellten Protokolle angefordert worden wären. Aufgrund meiner Anregung werden die Zusatzprotokollierungen jetzt zentral dokumentiert und so ausgewertet, daß solche Fehler zukünftig schnell abgestellt werden können.

Zu seiner Schulungspraxis hat mir das BKA mitgeteilt, daß bei ZEVIS-Einweisungen besonders darauf geachtet wird, das Verständnis für die Schutzwürdigkeit der Daten und die daraus resultierenden Datenschutzanforderungen zu wecken. ZEVIS-Anfragen an den Echtbestand erfolgen nur durch den Dozenten selbst oder unter seiner Aufsicht mit seinen eigenen Daten oder denen des Schülers, wenn dieser zugestimmt hat.

Wenn das BKA als nationales Zentralbüro von Interpol Daten aus ZEVIS an ausländische Dienststellen übermittelt, greifen die Regelungen des § 37 StVG z. B. über die Zulässigkeitsprüfung und die Zweckbindung aus formalen Gründen nicht (s. 13. TB S. 56). Das Bundeskriminalamt schlägt zur Lösung dieses Problems vor, ihm für die Erfüllung seiner Aufgaben als nationales Zentralbüro für Interpol eine gesetzlich geregelte Abrufmöglichkeit zu schaffen. Hiergegen habe ich keine grundsätzlichen Bedenken, solange diese inhaltlich dem § 37 StVG entspricht.

18.3.4 ZEVIS-Nutzung durch den Bundesgrenzschutz

Bei der Kontrolle und Beratung eines Grenzschutzamtes habe ich mich über den Ausbaustand und die Nutzung des Grenzterminalsystems (GTS) unterrichtet, wobei der Schwerpunkt auf der damit möglichen Nutzung von ZEVIS für Zwecke der Grenzkontrolle lag. Ich konnte feststellen, daß sowohl die Konzeption des GTS als auch dessen Nutzung durch den Grenzschutzeinzeldienst keinen datenschutzrechtlichen Bedenken begegnen. Das gleiche traf für die Datensicherung und die interne Datenschutzkontrolle zu.

18.4 Kraftfahrt-Bundesamt

Nicht nur wegen der Beratungen über die Bewährung und Weiterentwicklung von ZEVIS (s. dazu 18.2 und 18.3) waren die Kontakte zum Kraftfahrt-Bundesamt (KBA) sehr eng. Meine Beratung betraf auch Fragen der Datensicherung, insbesondere gegen unberechtigte Zugriffe auf die umfangreichen Datenbestände. In diesem Zusammenhang habe ich angeregt, künftig die geheimzuhaltenden Benutzerkennungen innerhalb des Systems kryptographisch zu verschlüsseln, und ich gehe davon aus, daß das KBA diese Anregung umsetzen wird.

Die insgesamt gute Zusammenarbeit schließt jedoch nicht aus, daß zu einzelnen Fragen auch unterschiedliche Meinungen fortbestehen.

18.4.1 Dieselbe Fahrzeug-Identifizierungsnummer bei mehreren Kraftfahrzeugen

Die zur Identifizierung von Fahrzeugen verwendeten Nummern — früher oft Fahrgestellnummern genannt — enthalten erst seit einigen Jahren auch eine Buchstabenfolge, die den Hersteller bezeichnet. Über die Aufnahme der Herstellerbezeichnung gibt es jedoch keine verbindliche Regelung, so daß einzelne, kleinere Hersteller noch eine eigene Systematik zur Numerierung ihrer Fahrzeuge verwenden. Deshalb existieren noch viele Fahrzeuge mit Fahrzeug-Identifizierungsnummern (FIN), die auch von anderen Herstellern für ebenfalls existierende Fahrzeuge vergeben wurden. Das führte zu Problemen bei der Datenabfrage. Wurde nämlich z. B. beim Auffinden eines irregulär entsorgten Fahrzeugs mit einer solchen FIN nach dem letzten Halter gefragt, so erschienen am Bildschirm auch die Daten anderer Fahrzeuge mit derselben FIN und auch die Angaben über deren Halter. Diese Angaben waren für den Anfragenden nicht erforderlich, ihre Übermittlung deshalb unzulässig.

Auf meine Anregung hin hat das KBA inzwischen ein Verfahren eingeführt, mit dem in solchen Fällen über eine Synopse lediglich technische Daten der Fahrzeuge sowie die Herstellerbezeichnung übermittelt werden. Damit kann die Anfrage präzisiert werden, und erst dann erscheinen die vollständigen Angaben zu dem nunmehr eindeutig identifizierten Fahrzeug. Diese Lösung ist angemessen. Sie entspricht dem Verfahren, mit dem das passende Fahrzeug bei nur unvollständig bekanntem Kennzeichen gesucht wird

und kann als Muster auch für andere Anfragetypen mit Mehrfach-Auskünften dienen.

18.4.2 Übermittlung von Halterdaten an die Automobilindustrie für umweltfördernde Maßnahmen

Durch das Gesetz zur Änderung des Kraftfahrzeugsteuergesetzes und des Straßenverkehrsgesetzes vom 15. Dezember 1990 wurde in § 35 Abs. 2 Nr. 1 des Straßenverkehrsgesetzes auch eine Rechtsgrundlage für die Übermittlung von Fahrzeug- und Halterdaten „für staatlich geförderte Maßnahmen zur Verbesserung des Schutzes vor schädlichen Umwelteinwirkungen durch bereits ausgelieferte Fahrzeuge" geschaffen. Sie ist zeitlich befristet und gilt bis zum 31. Dezember 1995. Meine ursprünglichen Bedenken gegen diese Regelung habe ich angesichts der Bedeutung des Umweltschutzes für die Allgemeinheit und wegen ihrer zeitlichen Befristung zurückgestellt.

In der Praxis wurde die Regelung vor allem von der Automobilindustrie zur Direktwerbung bei Fahrzeughaltern für den Einbau von Katalysatoren genutzt. Viele Betroffene nehmen daran jedoch Anstoß und fragen mich, ob die Übermittlung ihrer Daten durch staatliche Stellen an die Automobilindustrie mit datenschutzrechtlichen Grundsätzen vereinbar sei. Auch hier zeigt sich, daß die Bürger zunehmend datenschutzbewußt werden. Es liegt nicht zuletzt im Eigeninteresse der werbenden Unternehmen, den Bürgern die Hintergründe der Datennutzung zu erläutern. Ich habe das KBA daher gebeten, künftig bei den Herstellern auf eine entsprechende Informationspolitik zu dringen.

18.5 Muß der Geburtstag im Fahrzeugschein stehen? — Eintragungen in Fahrzeugpapieren —

In jeden Fahrzeugbrief werden nach § 25 Abs. 1 Straßenverkehrszulassungsordnung (StVZO) die Personalien des Halters eingetragen, für den das Fahrzeug zugelassen wird. Beim Halterwechsel bleibt die Eintragung der Vorhalter bestehen. Bei den heute verwendeten Brief-Vordrucken kann ein Brief bis zu fünf Vorhalter wiedergeben. Erst wenn kein Raum für neue Eintragungen mehr ist, wird ein neuer Brief ausgestellt, in dem dann nur noch die Anzahl der Vorhalter registriert wird.

Die Aussicht, daß damit ihre Namen mit Anschrift und Geburtsdatum auf längere Sicht wie Zubehör zum Fahrzeug mitverkauft werden, war für einige Bürger so unangenehm, daß sie sich mit der Bitte um Abhilfe an mich gewandt haben.

Ein wirklich wichtiger Grund für diese seit vielen Jahren geübte Verwaltungspraxis ist bisher auch vom Bundesministerium für Verkehr (BMV) nicht genannt worden. Unstreitig hat der Fahrzeugbrief das aktuelle Eigentum am Fahrzeug zu dokumentieren. Hinsichtlich der früheren Halter gibt es dagegen vielleicht beim Gebrauchtwagenkauf ein gewisses wirtschaftliches Interesse des Erwerbers am früheren Schicksal des Fahrzeugs, und die Lektüre des Fahrzeugbriefs mag im Einzelfall auch amüsant sein. Dies reicht als Grund für den *Zwang* zur Ausweisung aller früheren Halter aber nicht aus. Denn die privaten Interessen können unter den Beteiligten beim Fahrzeugverkauf auch ohne die Zwangseintragungen der Vorhalter im Kraftfahrzeugbrief gewahrt werden. Außerdem wird schon jetzt bei Verlust eines Briefes ein Ersatzbrief ausgestellt, in dem die Vorhalter nicht genannt sind, ohne daß dies zu nennenswerten Schwierigkeiten geführt hätte.

Obwohl es keine gesetzliche Verpflichtung gibt, an der kritisierten Verwaltungspraxis festzuhalten, reagierte das BMV auf meine Anregung, das Verfahren datenschutzfreundlicher zu gestalten, bisher nur zurückhaltend. Dies mag auch daran liegen, daß die zu erwartende europäische Harmonisierung vielleicht ohnehin bald eine Änderung der Vordrucke erzwingt. Es bleibt zu hoffen, daß dabei die bisherige unnötige Datenspeicherung in den Kraftfahrzeugbriefen nicht festgeschrieben wird. Weil offen ist, wann eine EG-Regelung getroffen und wirksam wird, habe ich angeregt, einstweilen (wie im Verlustfall) auf Wunsch des Halters einen Ersatzbrief auszustellen, in dem die Vorhalter nicht genannt sind. Der Verkäufer eines Fahrzeugs könnte sich dann ausbedingen, daß der Käufer davon Gebrauch macht.

Ähnlich verhält es sich bei der Frage, ob das Geburtsdatum des Halters im Fahrzeugschein eingetragen sein muß. Der Nutzen dieser Angabe ist begrenzt, denn sie sagt nichts darüber aus, ob der jeweilige Fahrer zur Führung dieses Fahrzeugs berechtigt ist, und auch die Eignung als Ausweis wird dadurch nicht verbessert. Dagegen kann es für eine Gewerbetreibende vielleicht störend sein, wenn ihre Kraftfahrer so ihr Geburtsdatum erfahren. Auf Wunsch des Betroffenen sollte daher auf die Eintragung verzichtet werden.

18.6 Rechtsgrundlage für Datei über Ordnungswidrigkeiten im Güterkraftverkehr

An dem Entwurf eines Gesetzes zur Aufhebung der Tarife im Güterverkehr (Tarifaufhebungsgesetz) hatte das Bundesministerium für Verkehr mich nicht beteiligt. In diesem Gesetz sollte mit der lapidaren Begründung, es handele sich um „die notwendige Datenschutzregelung", das Bundesamt für Güterverkehr (BAG) u. a. ermächtigt werden, Dateien mit personenbezogenen Daten über bestimmte Ordnungswidrigkeiten-Verfahren zu führen.

Um zu klären, ob für das Führen einer solchen Datei — neben dem Verkehrszentralregister und dem Gewerbezentralregister — überhaupt ein Bedarf besteht, habe ich mich bei einer Außenstelle der Bundesanstalt für Güterkraftverkehr von der dort praktizierten Speicherung von Angaben über Ordnungswidrigkeitenverfahren unterrichtet. Mit Hilfe einer Kartei werden Akten über Ordnungswidrigkeiten unternehmensbezogen erschlossen. Die Akten sind für die Beurteilung der Zuverlässigkeit von Unternehmen erforderlich. Dabei werden aber nicht nur die Verstöße des Unternehmens oder des Unternehmers selbst registriert, sondern auch die gewerberechtlichen Verstöße der

Mitarbeiter. Die Datensammlung ist damit personenbezogen und besonders schutzbedürfig. Aus Zahl und Umfang der Verstöße pro Mitarbeiter und im Verhältnis zu anderen Unternehmen schließt die Bundesanstalt auf die Wirksamkeit organisatorischer Maßnahmen zur Einhaltung z. B. der Sicherheitsvorschriften in diesem Unternehmen und damit auf dessen Zuverlässigkeit. Diese Angaben sind durch eine Abfrage des Verkehrszentralregisters oder des Gewerbezentralregisters in der Regel nicht zu beschaffen, weil sie dort — wenn überhaupt — zur Person des Betroffenen und nicht zum Unternehmen gespeichert werden. Deshalb ist es sinnvoll, diese Angaben in eine besondere Datei zu übernehmen und in gewissem Umfang auch an bestimmte andere öffentliche Stellen zu übermitteln, wobei in den meisten Fällen zumindest die Identität von Mitarbeitern keine Rolle spielt.

Im Regierungsentwurf ist nunmehr aufgrund meiner Beratung eine normenklare Regelung enthalten, die Übermittlungen aus der Datei an öffentliche Stellen zuläßt, „soweit die Daten für die Entscheidung über den Zugang zum Beruf des Güter- und Personenkraftunternehmers erforderlich sind". Dies wird für die Dateibestandteile „Name, Anschrift und Geburtsdatum des Betroffenen" überwiegend der Fall sein, wenn es sich um den Unternehmer selbst handelt. Darüber hinaus dürfen nur in den im Gesetz genau beschriebenen Fällen Auskünfte an Gerichte und Behörden gegeben werden. Die Speicherungszeit wurde auf zwei Jahre verkürzt. Mit dieser Regelung kann das BAG seinen Aufgaben insbesondere auch im Hinblick auf die Verkehrssicherheit voll gerecht werden, ohne die Belange betroffener Mitarbeiter von Unternehmen mehr als erforderlich zu beeinträchtigen. Ich begrüße das erzielte Ergebnis, das sicher mit wesentlich weniger Reibungsverlusten hätte erzielt werden können, wenn ich schon in einem früheren Stadium beteiligt worden wäre.

18.7 Verkehrszentralregister

18.7.1 Erteilung von Auskünften bei Zweifeln an der Personenidentität

Auf Anfrage der dazu berechtigten Stellen übermittelt das Kraftfahrt-Bundesamt die zu einer genannten Person im Verkehrszentralregister (VZR) geführten Angaben auch dann, wenn zwischen den Anfragedaten und den im VZR geführten Personalien geringe und deshalb vermutlich unwesentliche Unterschiede bestehen. So werden bei sonst identischen Daten bei Anfragen nach „Karl-Otto" die Angaben zu „Karl" herausgegeben, bei einer Anfrage mit Geburtsort Harburg wird auch Hamburg berücksichtigt und auch „Martini" wird ausnahmsweise zugelassen, wenn bei sonst gleichen Daten das Register „Martiny" kennt. In allen diesen Fällen wird der Empfänger zwar aufgefordert, die Identität besonders zu prüfen. Es fehlte bisher jedoch ein Hinweis auf die Zweckbindungsvorschriften des Bundesdatenschutzgesetzes (§ 15 Abs. 3) und damit auf das Verarbeitungs- und Speicherungsverbot, sofern eine Personenidentität nicht gegeben ist. Ich habe das Kraftfahrt-Bundesamt gebeten, die Empfänger in Zukunft darauf hinzuweisen, daß die Daten bei festgestellter Nicht-Identität unverzüglich zu löschen sind. Bisher ist das Amt dieser Anregung nicht gefolgt.

18.7.2 Gebührenfreiheit für Auskünfte nach dem Bundesdatenschutzgesetz wird mißachtet

Der Gesetzgeber hat durch die Novellierung des BDSG festgelegt, daß die von öffentlichen Stellen des Bundes dem Betroffenen zu erteilende Auskunft über seine Daten unentgeltlich ist (§ 19 Abs. 7 BDSG). Anders beim Kraftfahrt-Bundesamt: Dort kostet eine Auskunft aus dem VZR weiterhin zehn DM. Ich habe zunächst das Amt selbst und dann das BMV auf die Rechtswidrigkeit dieser Gebührenerhebung hingewiesen. Das BMV verweist auf die Befugnis, für Amtshandlungen auf dem Gebiet des Straßenverkehrs Gebühren zu erheben (§ 6 a Abs. 1 StVG). Eine Auskunft an den Betroffenen ist aber keine solche Amtshandlung; sie hat keine verkehrsrechtlichen Folgen oder Wirkungen. Dies haben mir auch die Bundesministerien des Innern und der Justiz bestätigt. Auf eine Reaktion des BMV hierauf warte ich bisher vergeblich.

18.8 Brauchen wir eine zentrale Führerscheindatei?

Immer wieder wird die Frage gestellt, ob nicht im KBA eine zentrale Datei aller in der Bundesrepublik Deutschland ausgestellten Fahrerlaubnisse eingerichtet werden solle. Abgesehen von dem davon verursachten Verwaltungsaufwand ist zu bedenken, daß damit eine zentrale Datei beinahe aller erwachsenen Bürger geschaffen würde. Bevor eine solche auch datenschutzrechtlich nicht unbedenkliche zentrale Datensammlung geschaffen wird, muß deren Notwendigkeit kritisch geprüft werden, wobei das Argument, daß es eine solche Zentralisierung in der ehemaligen DDR im Zentralen Einwohnerregister schon gegebenen habe, gewiß nicht ausreicht.

Solange die Führer von Kraftfahrzeugen die Fahrerlaubnis mitführen müssen, verspricht eine zentrale Speicherung keine Erleichterung bei Kontrollen. Ob eine einmal ausgestellte Fahrerlaubnis inzwischen entzogen wurde, kann schon jetzt über ZEVIS abgefragt werden.

Noch vorhandene Schwierigkeiten, von der ausstellenden Behörde Informationen über eine Fahrerlaubnis zu erhalten, werden im Zuge der zunehmenden dezentralen Automatisierung abgebaut. Damit bestehen für eine zentrale Speicherung kaum überzeugende Argumente.

In neuerer Zeit wird nunmehr unter Hinweis auf die Zweite EG-Führerscheinrichtlinie ein neuer Anlauf unternommen, ein zentrales Fahrerlaubnisregister einzurichten. Verwiesen wird dabei zum einen darauf, daß die Richtlinie für jeden Bürger nur noch eine Fahrerlaubnis — diese aber jetzt gültig in ganz Europa — zuläßt, und zum anderen darauf, daß die Mitgliedstaaten bei Verlust, Entziehung und ähnlichem zu umfangreichen Mitteilungen verpflichtet sind. Eine zentrale Speicherung kann aber nur bei

solchen Informationen wesentliche Vorteile bringen, die sehr schnell zur Verfügung stehen müssen, sonst ist der Weg zu den Führerscheinstellen ebenso erfolgreich. Letzteres mag im Zeitalter des Telefax sogar in vielen Fällen der schnellste Weg sein, wenn der Bürger zu seiner Fahrerlaubnis, insbesondere den Prüfungsort, Angaben macht und die Fahrerlaubnis automatisiert erfaßt ist (vorher wird auch keine Speicherung in Flensburg erfolgen können!). Eine Prüfung des vorgelegten Führerscheins auf Echtheit und Gültigkeit kann, bei zweifelsfreier Identität (siehe oben) auch heute schon in kurzer Zeit über das VZR und bei Bedarf durch Anfrage bei der Führerscheinstelle erfolgen. Ist die Identität fraglich, ist der Führerschein als Personaldokument sowieso eher untauglich.

Damit bleibt der Fall, daß der Bürger in einem anderen Mitgliedstaat eine weitere Fahrerlaubnis erwerben will und überprüft werden muß, ob es für ihn schon eine deutsche Fahrerlaubnis gibt. Nur wird niemand behaupten wollen, dies müsse binnen Minuten oder Stunden geklärt werden. Sollte wirklich jemand auf die Idee kommen, viel Geld für eine zweite Schulung und Prüfung auszugeben und würde er trotz Belehrung, daß überprüft wird, ob er in einem anderen Mitgliedsland nicht schon eine Fahrerlaubnis habe, bei seinem Vorhaben bleiben, so reichte eine in solchen Fällen vom KBA zusammengestellte und quartalsmäßig oder monatlich versandte Suchliste (z. B. Diskette) aus, um den zweiten Führerschein nachträglich einzuziehen. Auch dies ist also kein Fall, in dem ein zentrales Register einen wirklichen Vorteil brächte, der Kosten und Aufwand rechtfertigen würde.

18.9 Datenübermittlung durch Luftfahrt-Bundesamt führte zu Verlust einer ausländischen Fluglizenz

Ein Bürger beantragte beim Luftfahrt-Bundesamt die Anerkennung seiner US-amerikanischen Fluglizenz. Ein Mitarbeiter des Luftfahrt-Bundesamtes setzte sich daraufhin fernmündlich mit seinem Kollegen beim amerikanischen Luftfahrt-Bundesamt (FAA) in Verbindung und übermittelte eine Reihe von negativen Angaben über den Betroffenen. In der Folge verlor der Bürger zunächst seine amerikanische Fluglizenz und erhielt diese erst durch ein Gerichtsverfahren in den USA wieder zurück.

Bei der Kontrolle im Luftfahrt-Bundesamt konnte ich feststellen, daß die meisten Vorwürfe, die das Luftfahrt-Bundesamt dem Bürger gemacht hatte, auf Gerüchten beruhten. Zwar war den Vorgängen zu entnehmen, daß der Bürger vor einigen Jahren einmal einen Suizidversuch unternommen hatte, er war später aber mehrfach flugärztlich untersucht worden und auch in den Folgejahren weiterhin geflogen, ohne daß eine Gefährdung der Luftfahrt festgestellt werden konnte. Anhaltspunkte dafür, daß aus Gründen der Luftsicherheit, insbesondere aus Gründen der Lebensgefahr für Passagiere oder sonstige Personen, ein sofortiges Handeln des Luftfahrt-Bundesamtes erforderlich gewesen wäre, wurden auch vom Luftfahrt-Bundesamt nicht behauptet. Nur in diesem Falle wäre aber eine Datenübermittlung zulässig gewesen.

In den Vorgängen des Luftfahrt-Bundesamtes befand sich auch ein telefonisch angeforderter Bericht der Polizeistation des Heimatortes des betroffenen Bürgers, der die Kopie eines von diesem verfaßten Abschiedsbriefes enthielt. Sie wurde auf meine Anregung vernichtet.

Gegenüber dem Luftfahrt-Bundesamt habe ich deutlich gemacht, daß die Übermittlung personenbezogener Daten an das amerikanische Luftfahrt-Bundesamt unzulässig war. Dem betroffenen Bürger hätte allenfalls die Anerkennung seiner amerikanischen Fluglizenz für Flüge über der Bundesrepublik Deutschland verweigert werden können. Das Verfahren dazu ist im ICAO-Abkommen geregelt. Zuständig wäre dafür allerdings nicht das Luftfahrt-Bundesamt, sondern das Bundesministerium für Verkehr gewesen. Das Luftfahrt-Bundesamt hat sich meiner rechtlichen Bewertung angeschlossen.

Der Vorgang hat bestätigt, wie notwendig es ist, bereichsspezifische Rechtsgrundlagen für die Verarbeitung und Nutzung personenbezogener Daten durch das Luftfahrt-Bundesamt zu schaffen (vgl. schon 7. TB S. 36). Anläßlich der Kontrolle habe ich mit dem Luftfahrt-Bundesamt die Möglichkeit der Übermittlung personenbezogener Daten an ausländische Stellen ausführlich besprochen und darauf hingewiesen, daß es aufgrund der Rechtsprechung des Bundesverwaltungsgerichts vertretbar erscheint, bis zum Erlaß einer bereichsspezifischen Regelung im Luftfahrt-Bundesamt-Gesetz analog zu § 37 StVG zu verfahren. Danach können Fahrzeug- und Halterdaten zur Erfüllung von Verpflichtungen aus multi- oder bilateralen Vereinbarungen übermittelt werden. Die Heranziehung der Regelungen des Straßenverkehrsgesetzes für die Übermittlung personenbezogener Daten — insbesondere in das Ausland — ist auf Dauer aber wegen der Besonderheiten im Luftverkehrswesen nicht hinnehmbar. Die Novellierung des Luftfahrt-Bundesamt-Gesetzes ist aus diesem Grund dringlich.

Hinsichtlich der in den Jahren 1984 und 1986 beanstandeten Mängel bei der Datensicherheit, die 1992 immer noch nicht abgestellt worden waren, wurde geltend gemacht, daß das Bundesministerium für Verkehr nicht genügend Haushaltsmittel zur Verfügung gestellt habe, um Unterlagen mit sensiblen Daten sicher verwahren zu können. Trotz der angespannten Haushaltslage sollte es jedoch möglich sein, diesen rechtswidrigen Zustand bald zu ändern.

18.10 Defizite im Luftverkehrsrecht

Bei den bereichsspezifischen Regelungen über die Verarbeitung personenbezogener Daten im Rahmen des Luftrechts bestehen nach wie vor erhebliche Defizite. Abgesehen von der Wiedereinbringung und Verabschiedung des Zehnten Gesetzes zur Änderung des Luftverkehrsgesetzes wurde für deren Abbau auch im Berichtszeitraum wenig erreicht. Dabei ist die Beseitigung der Defizite dringlich. Denn sonst könnte

der Eindruck entstehen, die jetzt ohne ausreichende Rechtsgrundlage betriebenen Datenverarbeitungen seien auch aus der Sicht des Gesetzgebers nicht erforderlich, mit der Folge, daß sie mangels Rechtsgrundlage von den Gerichten als unzulässig bewertet werden.

18.10.1 Luftverkehrsgesetz — Überprüfung des Luftfahrtpersonals —

Über meine Beteiligung bei der Beratung des Zehnten Gesetzes zur Änderung des Luftverkehrsgesetzes habe ich berichtet (13. TB S. 57). Bei der Wiedereinbringung dieses Gesetzes habe ich an den Regelungen über die Prüfung der Zuverlässigkeit des Luftfahrtpersonals (§ 29d LuftVG) mitgewirkt, die im Rahmen des Gesetzes zur Übertragung der Aufgaben der Bahnpolizei und der Luftsicherheit auf den Bundesgrenzschutz mittlerweile in Kraft getreten sind.

Die Vorschrift ist bei redaktioneller Anlehnung an § 12 b AtomG teilweise modifiziert worden. Für eine Überprüfung ist grundsätzlich die Zustimmung des Betroffenen erforderlich. Eine Ausnahme gilt in Fällen der Wiederholungs- oder der nachgeholten erstmaligen Überprüfung von bereits zugangsberechtigtem Personal, wenn sie sich auf die Auswertung des bereits vorhandenen Wissens der Beschäftigungsstelle oder von Polizei- und Verfassungsschutzbehörden beschränkt. Die Regelung weist einen erfreulichen Datenschutzstandard auf und ist ein gutes Beispiel dafür, daß die Belange der öffentlichen Sicherheit und des Datenschutzes miteinander vereinbar sind.

Das Bundesministerium für Verkehr hat mittlerweile auch die Rechtsverordnung zur Ausführung dieser Vorschrift im Entwurf vorgelegt. Auf meine Anregung wurde die Aufbewahrungsdauer für die personenbezogenen Daten bei der Luftfahrtbehörde der fünfjährigen Gültigkeit der Überprüfung angepaßt und klargestellt, daß für Daten über Verurteilungen, deren Eintragung im Bundeszentralregister getilgt ist, auch von der Luftfahrtbehörde die engen Verwendungsbeschränkungen des § 52 BZRG einzuhalten sind.

18.10.2 Gesetzliche Regelung der Datenerfassung über Luftfahrer fehlt weiter

Das Bundesministerium für Verkehr hat mir inzwischen einen Entwurf zur gesetzlichen Regelung der Datenerfassung über Luftfahrer (Positiv/Negativdatei) übermittelt. Er bietet eine gute Grundlage, die seit langem bestehenden Probleme (s. 13. TB S. 57) zu beheben. Ich habe darauf hingewiesen, daß die wesentlichen Regelungen im Gesetz selbst zu treffen sind und die Verordnung lediglich die näheren Einzelheiten zur Ausführung des Gesetzes enthalten sollte.

Leider muß ich feststellen, daß das Bundesministerium für Verkehr auch über ein Jahr nach meiner Stellungnahme noch keinen weiteren Entwurf vorgelegt hat, so daß die von mir schon in meinem 13. TB (s. o.) bedauerten Defizite auf diesem Gebiet fortbestehen.

18.10.3 Veröffentlichung von Daten aus der Luftfahrzeugrolle

Auf die Notwendigkeit, die Veröffentlichung von personenbezogenen Daten der Eigentümer von Luftfahrzeugen, die im Rahmen der Verkehrszulassung erhoben und in der Luftfahrzeugrolle eingetragen sind, auf eine ausreichende gesetzliche Grundlage zu stellen, habe ich schon 1990 hingewiesen (12. TB S. 51f.). Trotz einer zwischenzeitlich vom für das Luftrecht zuständigen Fachreferat des BMV vorgeschlagenen Änderung zum Entwurf eines Gesetzes zur Änderung des Gesetzes über das Luftfahrt-Bundesamt und der Luftverkehrs-Zulassungsordnung sind die Arbeiten über die Abstimmung innerhalb des Bundesministeriums für Verkehr immer noch nicht hinausgekommen.

18.10.4 Hauptflugbuch

Auch für die Speicherung personenbezogener Daten von Luftfahrern im auf den Flugplätzen zu führenden Hauptflugbuch wird eine gesetzliche Grundlage benötigt (s. 13. TB S. 57). Das Bundesministerium für Verkehr teilte mir Anfang 1991 mit, daß als Rechtsgrundlage für den Erlaß entsprechender Verordnungen § 29 LuftVG ausreiche. Diese Auffassung teile ich nicht.

Selbst wenn man davon ausgeht, daß die Luftaufsicht im Rahmen ihrer Aufgabenzuweisung nach § 29 Abs. 1 LuftVG nicht nur allgemein präventive sowie in Notfallsituationen einzelfallbezogene Maßnahmen der Gefahrenabwehr treffen, sondern auch durch die Führung des Hauptflugbuches personenbezogene Daten auf Vorrat erheben darf, müßte § 29 Abs. 1 LuftVG ergänzt werden. Einzelheiten könnten dann durch Rechtsverordnung festgelegt werden.

18.10.5 Flugunfalluntersuchung

Das Bundesministerium für Verkehr hat mir 1992 den Entwurf einer Verordnung über die Untersuchung von Flugunfällen oder Störungen beim Betrieb von Luftfahrzeugen (Stand: November 1989) übermittelt. In einer ersten Stellungnahme habe ich darauf hingewiesen, daß die angegebene Ermächtigungsgrundlage (§ 32 Abs. 1 Satz 1 Nr. 6 LuftVG) nicht die im Entwurf vorgesehenen sehr weitreichenden Verpflichtungen der Beteiligten bei Flugunfällen und Störungen des Luftverkehrs stützt. Nach Artikel 80 Abs. 1 Satz 2 GG müssen die wesentlichen Regelungsinhalte vom Gesetzgeber selbst bestimmt werden. Zu den in diesem Sinne wesentlichen Regelungsinhalten auf dem Gebiet der Flugunfalluntersuchung gehören

- die Einrichtung der Flugunfalluntersuchungsstelle und die Festlegung ihrer Befugnisse,
- die Grundsätze für die Übertragung von Aufgaben an Dritte,
- die Erhebung personenbezogener Daten, z. B. über gesundheitliche Folgen für die Geschädigten, durch die untersuchende Stelle,

— die Grundsätze für die Verarbeitung personenbezogener Daten einschließlich der Akteneinsicht,

— die Festlegung der Ordnungswidrigkeitstatbestände.

Wegen der Bedeutung der einzelnen Maßnahmen für die Flugsicherung und der Notwendigkeit, die Privatsphäre der Betroffenen dabei angemessen zu schützen, halte ich eine tragfähige Regelung für dringlich. Mir ist unverständlich, warum das Bundesministerium für Verkehr — anders als im Bereich Straßenverkehr — hier so zögerlich agiert.

18.11 Schiffahrt

18.11.1 Lange Speicherung über Ordnungswidrigkeitsverfahren — Kontrolle der Wasser- und Schiffahrtsdirektion Südwest —

Die Strukturen der Datenverarbeitung in den Wasser- und Schiffahrtsverwaltungen sind bundesweit einheitlich. In der koordinierenden Behörde, dem Bundesamt für Wasserbau in Karlsruhe, werden für alle Wasser- und Schiffahrtsverwaltungen die Hard- und Sofware erprobt und beschafft sowie Dateien für Ausschreibungen, Lieferanten usw. geführt. Für alle Wasser- und Schiffahrtsverwaltungen gilt auch der vom Bundesminister für Verkehr herausgegebene Maßnahmenkatalog zum Datenschutz. Bei einer Kontrolle der Wasser- und Schiffahrtsdirektion (WSD) Südwest in Mainz konnte ich mich davon überzeugen, daß diese Vorgaben im allgemeinen zu datenschutzrechtlich guten Ergebnissen führen.

Nicht geregelt war im Kontrollzeitpunkt der Einsatz privater PC für dienstliche Zwecke. Die WSD Südwest hat dazu den Standpunkt vertreten, daß ein solcher dienstlich möglich und rechtlich zulässig sei. Die Projektierungszeit von wasserbaulichen und wasserwirtschaftlichen IT-Vorhaben werde damit erheblich verkürzt. Da eine ausreichende Ausstattung der Arbeitsplätze mit PC derzeit aus haushalts- und verwaltungstechnischen Gründen nicht möglich sei, möchte die Leitung der WSD den Einsatz privater PC für die o. a. Zwecke nicht untersagen. Demgegenüber habe ich Bedenken geäußert. Wenn entsprechende Regelungen fehlen, besteht ein hohes Risiko, daß bei der Benutzung privater PC dienstliche und private Angelegenheiten vermischt und dabei auch personenbezogene Daten unzulässig verarbeitet werden. Der BMV hat dem inzwischen insoweit Rechnung getragen, als er in einem Erlaß über den Einsatz von PC und Software die Verarbeitung jeglicher personenbezogener Daten auf privaten PC untersagt hat.

Die WSD Südwest erläßt für ihren Zuständigkeitsbereich jährlich ca. 2000 Bußgeldbescheide in Ordnungswidrigkeitenverfahren wegen Verstößen von Schiffsführern gegen die Rheinschiffahrtspolizeiverordnung oder gegen andere einschlägige Vorschriften. Die Bußgeldbescheide werden jahrgangsweise nach dem Datum geordnet in einem Tagebuch verzeichnet. Außerdem werden Kopien der Bußgeldbescheide jahrgangsweise sortiert in Aktenordnern für fünf Jahre aufbewahrt. Zur Dauer der Aufbewahrung hat die WSD Südwest erläutert, die von mir geforderte und an der Regelung für das Verkehrszentralregister des Kraftfahrt-Bundesamtes orientierte Aufbewahrungsfrist von lediglich zwei Jahren sei zu kurz. Besonders bei ausländischen Binnenschiffern dauere es bis zum Begleichen des Bußgeldes oft sehr lange. Von der Feststellung der Ordnungswidrigkeit über die Ausstellung des Bußgeldbescheides bis zur Zustellung an den Betroffenen, wenn sich dieser wieder im Bundesgebiet befindet, könnten Jahre vergehen. Hinzu komme noch die Zeit bis zum Bescheid über einen Widerspruch und zur Vollstreckung. Für einige Fälle mag das überzeugen, generell aber halte ich die geforderte Aufbewahrungsfrist von fünf Jahren für zu lang. Im Gespräch mit dem BMV werde ich mich um eine sachgerechte Lösung bemühen.

18.11.2 Meldesystem Gefahrguttransporte

Mitte 1992 hat die Wasser- und Schiffahrtsdirektion das „Melde- und Informationssystem für Gefahrguttransporte auf Binnenschiffahrtsstraßen/Nautischer Informationsfunk (MIB/NIF)" auf dem Streckenabschnitt Bingen — St. Goar probeweise in Betrieb genommen. Dieses Meldesystem soll dazu beitragen, bei Havarien von Schiffen mit besonders gefährlichem Frachtgut die Einsatzkräfte zu koordinieren, sie entsprechend vorbereitet für den jeweiligen Schadensfall gezielt einzusetzen, Menschenleben vor Schaden zu bewahren und die anderen Gefahren und Schäden so effektiv wie möglich zu bekämpfen. Der Abruf der gespeicherten Daten über Schiff, Ladung und Besatzung ermöglicht es, bei einer Havarie die Einsatzkräfte schneller mit den erforderlichen speziellen Mitteln zur Schadensbekämpfung auszustatten.

Laufen die Schiffe einen der Kontrollpunkte im oben angegebenen Streckenabschnitt an, so haben sich die Schiffsführer spätestens hier anzumelden und die notwendigen Daten der WSD mitzuteilen. Die wesentliche technische Voraussetzung für das MIB ist der ab 1988 errichtete Nautische Informationsfunk, der die funktechnische Verbindung zwischen den Schiffen und den Wasser- und Schiffahrtsverwaltungen oder (örtlich begrenzt) zwischen Schiffen und Schleusen herstellt.

Die rechtliche Voraussetzung für das Erheben und Verarbeiten der Daten im Rahmen des MIB wird der neue § 12.01 der Rheinschiffahrtspolizeiverordnung sein, der von der Zentralkommission für die Rheinschiffahrt (ZKR) beschlossen wurde und am 1. April 1993 in Kraft tritt. Für den gegenwärtigen Probebetrieb hat die WSD befristet Ausnahmen vom Nachtfahrverbot des § 9.07 der Rheinschiffahrtspolizeiverordnung zugelassen, wenn die zur Sicherheit der Schiffahrt erforderlichen Angaben gemacht werden. Das vorgesehene IT-gestützte Informationssystem wird voraussichtlich erst 1994 einsetzbar sein; bis dahin werden die Daten bei der WSD in Listen geführt.

Wegen der noch ausstehenden weiteren Regelungen stehe ich mit dem Bundesministerium für Verkehr in Verbindung.

19 Umweltschutz

Nicht nur der Datenschutz, sondern auch der Umweltschutz befaßt sich mit den Auswirkungen der modernen Technologie auf die Lebenssituation des Einzelnen. Datenschutz und Umweltschutz haben dabei das gemeinsame Ziel, humane Lebensbedingungen zu erhalten oder zu schaffen. Berührungspunkte ergeben sich aber auch daraus, daß für Zwecke des Umweltschutzes sowohl bei den Umweltplanungsbehörden als auch beim Vollzug von Umweltvorschriften personenbezogene Daten erhoben und verarbeitet werden.

19.1 Umwelt-Informationssysteme

Praktische Probleme und Zielkonflikte treten auf, wenn etwa personenbezogene Daten zum Aufbau vielseitig verwendbarer Umwelt-Informationssysteme erhoben oder aus Verwaltungsvorgängen zusammengeführt werden. Solche Umwelt-Informationssysteme werden in den Bundesländern, beim Bund und bei der Europäischen Gemeinschaft aufgebaut. Hierzu zählen z. B. Altlastenkataster, Biotopkataster, Bodeninformationssysteme (BIS), Geographische Informationssysteme (GIS), das Meß- und Informationssystem zur Überwachung der Umweltradioaktivität (IMIS) und das Europäische Umwelt-Informationssystem CORINE (= **Coo**rdination of **In**formation on the **E**nvironment). Personenbezogen sind in diesen Umwelt-Informationssystemen vor allem Angaben über Grundstücke, etwa der Name des Eigentümers, oder über bestimmte Bodenproben, die gegebenenfalls Rückschlüsse auf die Gesundheit der Bewohner des Grundstücks, von dem die Proben stammen, also auch der Mieter oder Pächter, zulassen.

Soweit durch die Datenerhebung und -verarbeitung für Umwelt-Informationssysteme in das Recht auf informationelle Selbstbestimmung eingegriffen wird, sind auch dafür bereichsspezifische Rechtsgrundlagen zu schaffen. Nach den bisherigen Ergebnissen der Beratungen zum Umweltinformationsgesetz (s. 19.2) und zum Umweltstatistikgesetz (s. 23.5) gehe ich davon aus, daß dabei datenschutzgerechte Lösungen erreicht werden.

19.2 Umweltinformationsgesetz

Nahezu alle Verwaltungsvorgänge der Umweltbehörden enthalten personenbezogene Daten. Dazu gehören insbesondere Daten von

- Antragstellern und Einwendern in einem Genehmigungsverfahren, z. B. nach dem Bundes-Immissionsschutzgesetz,
- Adressaten eines umweltrechtlichen Untersagungsverfahrens,
- Personen, die gegen Umweltvorschriften verstoßen haben,
- Personen, die durch Umwelteinflüsse geschädigt wurden,
- Bürgern, die auf Mißstände in der Umwelt hingewiesen haben, und
- Amtsträgern, die in dem Verwaltungsvorgang Maßnahmen im weitesten Sinne (Entscheidungen, Informationssammlungen) getroffen haben.

Die Richtlinie des Rates der Europäischen Gemeinschaften über den freien Zugang zu Informationen über die Umwelt (90/313/EWG — EG-Umweltinformationsrichtlinie, vgl. dazu 13. TB S. 78), soll im Interesse eines wirksamen Umweltschutzes für jeden den freien Zugang zu den bei Behörden vorhandenen Informationen über die Umwelt und die regelmäßige Unterrichtung der Öffentlichkeit über den Zustand der Umwelt gewährleisten. Zur Umsetzung der EG-Umweltinformationsrichtlinie hat das Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit den Referentenentwurf eines Umweltinformationsgesetzes vorgelegt.

Der Anspruch auf freien Zugang zu Informationen über die Umwelt steht in einem Spannungsverhältnis zum Grundrecht auf informationelle Selbstbestimmung, soweit Angaben über eine natürliche Person betroffen sind. Dieser Konflikt ist im Wege der „praktischen Konkordanz" zu lösen. Bei der Abwägung wird es vor allem darauf ankommen, wie stark einerseits der Betroffene durch die Offenbarung der Daten in seinen Rechten berührt wird und wie wichtig andererseits gerade eine personenbezogene Offenlegung der Daten für die Erreichung der umweltpolitischen Zielsetzung ist. Dabei ist das Nennen der Namen von Amtsträgern grundsätzlich unproblematisch, solange sie nur in ihrer amtlichen Tätigkeit betroffen sind. Hinsichtlich der Veröffentlichung personenbezogener Daten von Einwendern hat das Bundesverfassungsgericht in seinem Beschluß vom 24. Juli 1990 (BVerfG, NVwZ 1990, S.1162) erklärt, daß die Veröffentlichung nicht anonymisierter Daten das Recht der Betroffenen auf informationelle Selbstbestimmung verletzen kann (s. oben 18.1). Die dort gemachten Aussagen lassen sich auf Antragsteller in umweltrechtlichen Genehmigungsverfahren zumindest insoweit übertragen, daß diese Betroffenen nur dann öffentlich genannt werden dürfen, wenn eine ordnungsgemäße Durchführung des Genehmigungsverfahrens dies erfordert.

Bei Adressaten eines Untersagungsverfahrens und bei Personen, gegen die die Umweltbehörde wegen eines Verstoßes gegen Umwelt- und/oder Strafvorschriften vorgegangen ist, dürfte es in aller Regel vertretbar sein, die Informationen der Öffentlichkeit zugänglich zu machen. Denn Art und Ort der Umweltschädigung sind wichtige Informationen für einen meist nicht exakt abgrenzbaren Personenkreis, die oft unvermeidlich mindestens personenbeziehbar sind. Dagegen verdienen Personen, die Behörden auf Mißstände in der Umwelt hingewiesen haben, den Schutz der Geheimhaltung, der auch deswegen leicht gewährt werden kann, weil es für die Umweltfolgen nicht darauf ankommt, wer auf die Schädigung hingewiesen hat. Unterlagen über auf Umwelteinflüsse

beruhenden gesundheitlichen Schäden einzelner sind in der Regel nicht veröffentlichungsfähig.

Die EG-Umweltinformationsrichtlinie eröffnet den Mitgliedstaaten ausdrücklich die Möglichkeit, bei der Umsetzung der Richtlinie Regelungen zum Schutz personenbezogener Daten vorzusehen. Der Entwurf eines Umweltinformationsgesetzes sieht insoweit eine Abwägung vor, die verhindern soll, daß durch die Offenlegung personenbezogener Daten schutzwürdige Interessen von Betroffenen beeinträchtigt werden. Ich halte die Regelung in dieser allgemeinen Form für angemessen. Denn das Umweltinformationsgesetz kann nur allgemeine Prinzipien festlegen. Die Einzelheiten der Abwägung zwischen dem Anspruch des Bürgers auf Zugang zu Umweltinformationen und dem Anspruch anderer Bürger auf Schutz ihres Persönlichkeitsrechts und ihrer Privatsphäre muß der Gesetzgeber bei bereichsspezifischen Gesetzen näher ausgestalten. Dies ist z. B. im Bereich des Bundes für das immissionsschutzrechtliche Genehmigungsverfahren und für die Verwaltungsverfahren nach dem Bundesnaturschutzgesetz erfolgt. Auch in den Ländern gibt es bereits eine Reihe von Zugangsrechten zu Umweltinformationen. So besteht nach den Wassergesetzen einiger Bundesländer ein allgemeines Einsichtsrecht in die Wasserbücher.

Die Aufnahme des Zugangsrechts zu Umweltdaten in die Verfassungen der Länder Sachsen und Sachsen-Anhalt, noch mehr aber die Aufnahme eines allgemeinen Einsichtsrechts des Bürgers in Behördenakten und andere amtliche Unterlagen in der Verfassung des Landes Brandenburg unterstreicht die grundsätzliche Bedeutung des Themas.

20 Deutsche Bundespost — Gute Entwicklung des Datenschutzes bei Postdienst und Postbank —

Die Poststrukturreform hat zu selbständigen Organisationseinheiten für die Betriebsfunktionen der früher einheitlichen Post und zugleich zu einer Trennung vom Ministerium geführt, das nur noch für die Regulierungsfragen zuständig ist. Ungeachtet aller Schwierigkeiten, die so tiefgreifende Umstrukturierungen mit sich bringen, hat sich die Veränderung für den Datenschutz in den Bereichen Postdienst und Postbank eher günstig ausgewirkt. Denn zum einen wird die Aufgabe des Ministeriums, faire und damit datenschutzgerechte Rahmenbedingungen zu schaffen, jetzt weniger durch die früher selbst wahrgenommene Aufgabe der obersten Betriebsführung beeinflußt. Zum anderen brachte der Wandel vom Hoheitsträger zum öffentlichen Unternehmen eine stärkere Kundenorientierung, die — trotz einiger Probleme, die im Massengeschäft der Post immer wieder auftreten — auch dem Datenschutz zugute kommt.

Die Datenschutzverordnungen für den Postdienst und die Postbank haben sich in der Praxis bewährt. Der jetzt erkennbare Änderungsbedarf für den Postdienst betrifft im wesentlichen die Anpassung der Dauer der Aufbewahrung von Nachweisen über ausgelieferte Sendungen, die an die Gewährleistungsfristen anzupassen ist, was beim Erlaß der Verordnung versäumt worden war. Die Abstimmung dazu läuft, und ich bin zuversichtlich, eine datenschutzgerechte Lösung zu erreichen.

20.1 Postdienst

20.1.1 Nachsendungsanträge garantieren nicht die Geheimhaltung der neuen Anschrift

Auf Wunsch des Empfängers liefert die Post Sendungen statt unter der vom Absender angegebenen Adresse an eine vom Empfänger bestimmte andere Anschrift (Nachsendung). Diese für die meisten Sendungen innerhalb Deutschlands entgeltfreie Sonderleistung wird sowohl bei befristeter Abwesenheit als auch nach einem Umzug in Anspruch genommen. Der Bequemlichkeit vieler Bürger kommt dabei entgegen, daß die Post auf Wunsch des Absenders beim Umzug des Empfängers die Sendung mit der neuen Anschrift versieht und dem Absender zurückschickt. Aufgrund einer solchen „Vorausverfügung" des Absenders erhalten z. B. Versicherungen die neue Anschrift ihres umgezogenen Kunden, ohne daß dieser sich besonders darum bemühen müßte. Da nicht unterstellt werden kann, daß der Empfänger dies bei allen Absendern wünscht, wurde in § 4 Abs. 2 der Postdienst-Datenschutzverordnung (PD-DSV) festgelegt, daß er diesem Verfahren widersprechen kann, wovon gelegentlich auch Gebrauch gemacht wird.

Trotz der insgesamt sinnvollen Regeln kommt es doch immer wieder zu Fehlern, die für die Betroffenen so störend sind, daß sie mich um Abhilfe bitten. Die Beschwerden beziehen sich überwiegend auf die folgenden Fallgruppen:

— Wenn eine *Sendung mit neuer Anschrift an den Absender* zurückgeliefert wird, gehen viele Absender stets von einem Umzug aus, was aber nur in der Regel richtig ist. Liegt ausnahmsweise kein Umzug vor, so reagieren die Betroffenen überrascht bis verärgert, wenn z. B. eine Meldebehörde sie „zur Vermeidung eines Bußgeldes" auffordert, sich unverzüglich umzumelden, oder wenn eine Versicherung ankündigt, die Hausratsversicherung laufe aus. Die oben beschriebene Vorausverfügung des Absenders gilt zwar im Prinzip nur für Umzüge, unvollständig ausgefüllte Nachsendungsanträge werden von der Post aber oft als Umzug interpretiert, womit sie freilich eine gewisse Fehlerquote hinnimmt.

— Für das *Nachsenden wird die Sendung mit der neuen Anschrift versehen.* Erreicht sie nun ausnahmsweise dort den Empfänger doch nicht, z. B. weil er schon wieder abgereist ist, so wird sie als unzustellbar an den Absender zurückgesandt. Damit wird nicht nur ein möglicherweise eingelegter Widerspruch des Empfängers unterlaufen, sondern der Absender erhält eine „neue" Anschrift, unter der eine Zustellung gerade nicht möglich ist. Mißversteht er eine solche Rücksendung als Hinweis auf einen Umzug, so kann dies beträchtliche Fehler zur Folge haben. Deshalb habe ich bei der Generaldirektion der DBP-Postdienst angeregt, in

solchen Fällen die unbrauchbare neue Anschrift unkenntlich zu machen.

— Gelegentlich wird der *Vordruck für den Nachsendungsantrag falsch oder unvollständig ausgefüllt* oder der Antrag wird formlos gestellt und wesentliche Angaben, wie das Ende eines kurzfristig gewollten Nachsendungsantrages, fehlen. Dann ist auch beim besten Bemühen der Post das Fehlerrisiko ziemlich groß.

Fehler dieser Art sind zwar relativ selten, bei den vielen Millionen von Nachsendungen kommen sie aber doch immer wieder vor. Zusätzlich unterlaufen trotz in der Regel großer Sorgfalt auch bei der Postsortierung Fehler, etwa dadurch, daß ein Nachsendungsantrag übersehen oder falsch interpretiert wird. Dies kann z. B. geschehen, wenn nur ein Teil einer Familie umzieht und für diese Personen ein Nachsendungsantrag erteilt wird, für die anderen aber die alte Adresse richtig bleibt. Hier können nur deutliche Erklärungen die Ausführung verbessern.

Systemfehler, deren Behebung zu einer grundlegenden Verbesserung des Verfahrens führen könnte, habe ich bisher nicht feststellen können. Deshalb wird man auch in Zukunft damit rechnen müssen, daß in diesem Verfahren, das im Interesse der Kunden unentgeltlich und deshalb auch mit wenig Aufwand betrieben werden muß, gewisse Risiken bleiben, deren Folgen nur durch bessere Hinweise auf die Fehlerquellen vermindert werden können.

Wer von dem Nachsendeverfahren Gebrauch macht, muß sich darüber im klaren sein, daß seine neue Adresse kaum zuverlässig geheim gehalten werden kann. So läßt sich beispielsweise kaum verhindern, daß ein verlassener Partner die neue Adresse des Weggezogenen erfährt, wenn dieser einen Nachsendungsantrag gegeben hat. In solchen Fällen muß ein anderes Verfahren gewählt werden, wie etwa die Nachsendung an einen Postbevollmächtigten als Mittelsmann. In solchen Fällen kann die Post nur beraten; das setzt aber voraus, daß der Kunde genau darlegt, was er erreichen möchte.

20.1.2 Fehlerhafte Postzustellungen

Immer wieder sind die Bürger verärgert, wenn ihre Post fehlerhaft zugestellt wird oder sie selbst falsch zugestellte Sendungen erhalten. Ich habe im Berichtszeitraum dazu eine größere Anzahl von Eingaben erhalten, in denen die betroffenen Bürger mangelnden Datenschutz bei der Deutschen Bundespost Postdienst beklagen.

Die Gründe für die fehlerhaften Postzustellungen sind unterschiedlich; im wesentlichen sind sie in zwei Gruppen zusammenzufassen.

Zum einen handelt es sich um Fehler der Postzusteller, die richtig adressierte Sendungen, meist gewöhnliche Briefe oder Postkarten, in den falschen Briefkasten werfen. Solche Fehler sind relativ selten. Sie werden gelegentlich durch das Aneinanderhaften dünner Sendungen begünstigt; einige Fälle beruhen aber auch auf der Unachtsamkeit der Postzusteller. Derartige Fehler sind bei dieser Art von Arbeit leider nicht mit absoluter Sicherheit vermeidbar. Systematische Fehler oder gar absichtliche Fehlleitungen habe ich nicht festgestellt. Nur ganz vereinzelt traten auch Fehlerhäufungen durch Nachlässigkeit der Zusteller auf. In diesen Fällen führten mehrere Beschwerden aus demselben Zustellbezirk z. B. zur schnellen Ablösung von Aushilfskräften. Ich kann also nur empfehlen, häufigeren Fehlern dieser Art nachzugehen, damit die Post die Fehlerquellen erkennt und für Abhilfe sorgen kann.

Die andere Gruppe von Fehlern entsteht durch falsche Adressierung von Sendungen. Findet die Post zur angegebenen Anschrift überhaupt keinen mit einiger Sicherheit passenden Empfänger, so wird die Sendung als unzustellbar an den Absender zurückgesandt. Macht die Post aber einen Empfänger ausfindig, der nach ihrem Urteil mit hinreichender Sicherheit gemeint sein dürfte, so stellt sie an diesen zu. War es der Richtige, freuen sich die Beteiligten und loben die Findigkeit der Post. Es wäre auch unverständlich kleinlich, wenn die Post nur wegen einer falschen Hausnummer, eines Schreibfehlers im Straßennamen, eines Irrtums bei der Postleitzahl oder anderer Kleinigkeiten einen Brief an den Absender zurückschickte. Leider ist die trotz kleiner Abweichungen erfolgte Zustellung nicht immer richtig, und leider prüft nicht jeder Empfänger, ob die Anschrift stimmt und ob er von *diesem* Absender Post erwarten kann. Damit können am Ende dann Sendungen nicht nur in falsche Hände gelangen, sondern dort auch geöffnet werden. Die mir durch Zuschriften bekannt gewordenen Fälle dieser Art lassen aber nicht vermuten, daß die Post oder ihre Zusteller hier leichtfertig vorgehen. Deshalb möchte ich nicht zu der Alternative raten, bei jeder — auch der geringsten — Abweichung zwischen der Anschrift und den Daten des Empfängers eine Sendung als unzustellbar an den Absender zurückzuschicken.

20.1.3 Auskunft über die Anschrift des Postfachinhabers

Mehrere Postfachinhaber haben sich bei mir darüber beschwert, daß die Deutsche Bundespost Postdienst Dritten ihre Wohnanschrift mitgeteilt hat (vgl. schon 12. TB S. 47 und 13. TB S. 47). Seit dem 1. Juli 1991 ist diese Frage in § 5 der Postdienst-Datenschutzverordnung geregelt. Grundsätzlich darf die Anschrift eines Postfachinhabers danach nur mitgeteilt werden, wenn sie für den Postverkehr benötigt und dazu ein berechtigtes Interesse glaubhaft gemacht wird. Was unter berechtigtem Interesse zu verstehen ist und wie ein Dritter dieses glaubhaft machen kann, wurde nicht präzisiert. Das Postamt muß daher im Einzelfall entscheiden. Die Praxis hat bisher zu keinen Beschwerden bei mir geführt. Dazu dürfte beigetragen haben, daß jeder Postfachinhaber der Mitteilung seiner Anschrift ohne Angabe der Gründe generell schriftlich widersprechen kann; darauf wird er ausdrücklich hingewiesen.

Probleme treten dagegen auf, wenn die Abholfrist wesentlich überschritten wird oder wenn Pakete oder Päckchen an eine Postfachanschrift adressiert werden, wofür Postfachanlagen nicht vorgesehen sind.

Die Post versucht dann, bei der ihr bekannten Anschrift des Empfängers zuzustellen. Dazu wird diese Anschrift für den Postzusteller auf der Postsendung angebracht. Wird der Postfachinhaber dann unter dieser Anschrift erreicht, hatten die Bemühungen der Post Erfolg und sie erntet vielleicht sogar Dank dafür. Bleiben jedoch die Zustellversuche der Post erfolglos, so wird die Postsendung an den Absender zurückgeschickt, der dann — möglicherweise gegen den Willen des Empfängers — die Anschrift erfährt. Meist handelt es sich um die Wohnanschrift, wobei der Wert dieser Angabe aber zweifelhaft ist, weil die Zustellung ja gerade nicht möglich war. Die Verhältnisse liegen dann ähnlich wie bei erfolglosen Nachsendungen (s. o. 20.1.1), und eine Lösung könnte auch hier im Unkenntlichmachen der untauglichen Anschrift bestehen. Außerdem gilt, daß — ähnlich wie bei Nachsendungsanträgen — der Empfänger nicht unbedingt darauf vertrauen sollte, daß die Benutzung eines Postfaches in jedem Falle die Geheimhaltung seiner (Wohn-)Anschrift garantiert.

20.2 Postbank

20.2.1 Die Zusammenarbeit mit der SCHUFA

Während die Postbank früher Kontoüberziehungen allenfalls in sehr begrenztem Ausmaß duldete, räumt sie ihren Kunden jetzt in der Regel einen Dispositionskredit ein. Im engen wirtschaftlichen Zusammenhang damit steht die Ausgabe von Scheckkarten mit der Möglichkeit für die Kunden, damit aus Automaten Bargeld zu erhalten.

Die Angleichung an das Leistungsangebot anderer Banken führte auch zur Angleichung bei der Zusammenarbeit mit den jeweiligen Regionalgesellschaften der Schutzvereinigung für allgemeine Kreditsicherung, kurz: SCHUFA. Die Klausel, mit der die Kunden in die Datenübermittlung an die SCHUFA einwilligen sollen, entspricht der auch von anderen Banken verwendeten SCHUFA-Klausel. Wegen der gebotenen Vorteile haben die Kunden im allgemeinen die geforderte Einwilligung erteilt.

Zu Schwierigkeiten kam es gelegentlich dann, wenn ein Kunde, der an den neu gebotenen Leistungen kein Interesse hatte, die Einwilligung nicht geben wollte und ihm die Einrichtung eines Postgirokontos deshalb verweigert wurde. Die Betroffenen haben sich in einigen Fällen an mich gewandt, und es stellte sich dann schnell heraus, daß die Postbank nach wie vor auch die Kontoführung ohne Kredit und ohne SCHUFA-Einwilligung anbietet. Sie ist dazu auch nach § 8 des Gesetzes über das Postwesen verpflichtet. Weil ich in der letzten Zeit keine Eingaben dieser Art mehr erhielt, gehe ich davon aus, daß die Umstellungsschwierigkeiten nun überwunden sind.

Ein anderes Problem trat auf, als die Postbank einem Kunden wegen einer negativen SCHUFA-Meldung keine Scheckkarte gab und auf seine Bitte, ihm den Inhalt dieser Meldung mitzuteilen, „aus Datenschutzgründen" die erbetene Auskunft verweigerte. Meine Klärung des Sachverhalts ergab, daß die Postbank diese Angaben nicht in einer Datei speichert und als Wettbewerbsunternehmen deshalb nach der Rechtslage nicht unbedingt gezwungen war, die Auskunft zu geben. Die Rechtslage hätte diese Auskunft aber ohne weiteres zugelassen. Deshalb war die Berufung auf Datenschutzgründe bei der Verweigerung der Auskunft unzutreffend. Weil die Erteilung der Auskunft auch kundenfreundlicher gewesen wäre, hat die Generaldirektion der Postbank inzwischen die Postgiroämter angewiesen, in solchen Fällen auf Wunsch des Kunden die Auskunft zu geben.

Eine unter Umständen gebotene Berichtigung der gespeicherten Daten kann der Kunde dann im direkten Kontakt mit der SCHUFA erreichen.

20.2.2 Bankeinzugsverfahren

Einige Postkunden haben sich bei mir darüber beschwert, daß die Postbank von ihren Konten Beträge im sogenannten Bankeinzugsverfahren abgebucht hatte, ohne daß sie der Bank oder dem einziehenden Unternehmen dies erlaubt hatten. Ohne eine solche Erlaubnis ist die mit der Abbuchung verbundene Veränderung der Daten des Kontoinhabers offensichtlich unzulässig; es erweist sich jedoch als praktisch unmöglich, solche Fälle mit absoluter Sicherheit zu vermeiden.

Das Bankeinzugsverfahren ist gesetzlich nicht präzise geregelt, sondern beruht auf vertraglichen Vereinbarungen der Banken untereinander und mit ihren Kunden. Danach darf der Kunde seiner Bank einen Auftrag zum Einzug eines Betrages von einem anderen Konto nur erteilen, wenn dessen Inhaber zuvor eingewilligt hat. Die Postbank verlangt, daß die Einwilligungen der anderen Kontoinhaber schriftlich erfolgt sein müssen und behält sich (insoweit) das Recht zur Kontrolle vor, macht von diesem Recht aber nur selten Gebrauch.

Wirksamer gegen Mißbrauch ist die Haftungs- und Kostenregelung. Sie verpflichtet den auftraggebenden Kunden, im Falle des Widerrufs der Abbuchung unabhängig von dessen Berechtigung nicht nur den Abbuchungsbetrag, sondern auch einen pauschalen Zuschlag für die Kosten an seine Bank zu zahlen. Die Banken haben sich untereinander verpflichtet, Einziehungsaufträge durchzuführen und etwaige Widerrufe zu beachten, wobei das wirtschaftliche Risiko bei der Bank des Auftraggebers liegt. Diese übernimmt in der Regel dieses Risiko nur, nachdem sie sich von der Bonität des Auftraggebers überzeugt hat. Mit diesem Verfahren ist der Kunde, von dessen Konto im Einzelfall auch ohne sein Zutun der einzuziehende Betrag abgebucht wird, vor wirtschaftlichem Schaden geschützt. Er muß lediglich der Abbuchung bei seiner Bank widersprechen. In ihren Allgemeinen Geschäftsbedingungen hat die Postbank für den Widerruf zwar eine Frist von sechs Wochen bestimmt, aber diese Frist dürfte in fast allen Fällen ausreichen, und auch danach verliert der Kunde seinen Anspruch nicht ohne weiteres.

Das gesamte Verfahren hat sich zwar aus der Sicht der Kunden, von deren Konto abgebucht wird, als ausreichend sicher gegen Mißbrauch erwiesen, unbeabsich-

tigte Fehler kommen aber doch hin und wieder vor. In den mir bekannt gewordenen Fällen handelte es sich stets um Fehler des Auftraggebers, die von den beteiligten Banken aufgrund der Organisation des Verfahrens nicht erkannt worden waren. Bezogen auf die vielen Millionen richtig durchgeführter Einzugsaufträge sind solche Fehler sehr selten. Der Widerruf des betroffenen Kunden führt in der Regel auch zu dem Erfolg, daß der Auftraggeber einen solchen Auftrag nicht erneut erteilt.

Die Postbank ist darüber hinaus bereit, auf Wunsch ihres Kunden sein Konto für solche Abrufe generell oder gegen bestimmte Abrufe zu sperren. Aus der Behandlung eines Einzelfalles, in dem der Betroffene sich über wiederholt falsche Abbuchungen desselben Auftraggebers beschwert hatte und selbst mit diesem Auftraggeber nicht in Verbindung treten wollte, ist mir bekannt, daß die Postbank in so extremen Fällen sich auch an den Auftraggeber oder an dessen Bank wendet, um den Fehler zu beseitigen. Unter diesen Umständen halte ich die Vorkehrungen gegen unberechtigte Kontoänderungen für ausreichend. Denn gerade die Einfachheit des Abbuchungsverfahrens macht es für viele Kunden zu einem bequemen Zahlungsweg, der wegen des hohen Automatisierungsgrades auch kostengünstig ist. Müßte sich die abbuchende Bank in jedem der vielen Millionen richtig ablaufender Einzelvorgänge erst vom schriftlichen Einverständnis des Kunden überzeugen, so würden damit vermutlich zwar Fehler vermieden werden können. Die Kosten wären aber erheblich und gingen schließlich zu Lasten der Kunden.

20.2.3 Die Kontonummer muß nicht in der Anschrift auf dem Kontoauszugsbrief stehen

Häufig beklagen sich Bürger bei mir darüber, daß die Kontonummer ihres Postgirokontos als Teil der Anschrift auf ihre Kontoauszugsbriefe aufgeklebt oder aufgedruckt wurde. Das gleiche trifft auch bei Verwendung von Fenster-Briefumschlägen zu, weil die Kontonummer auf dem Kontoauszug so gedruckt wird, daß sie von außen lesbar ist. Ein dabei oft genannter Grund für die Besorgnis der Privatkunden ist die Befürchtung, mit der Kenntnis der Kontonummer könnten Unberechtigte Abbuchungen veranlassen, was zumindest Unannehmlichkeiten zur Folge hätte (s. o. 20.2.2).

Dieses Risiko ist zwar gering, die von außen lesbare Kontonummer ist aber störend und vermeidbar. Seit Jahren stehe ich darüber mit dem BMPT und der Generaldirektion der Postbank in Diskussion.

Weil die Kontonummer für den Postversand und für die Zustellung an den Empfänger nicht erforderlich ist und andere große Banken derartige Kontonummer-Aufdrucke nicht oder nicht mehr verwenden, scheint es an der Zeit, daß auch die Postbank darauf verzichtet.

Seit Oktober 1992 arbeiten die Postgiroämter mit einem neuen Kontoführungssystem. Neben anderen Veränderungen wurde auch der Kontoauszug neu gestaltet. Meiner Forderung ist die Postbank dabei aber nur insoweit etwas entgegengekommen, als jetzt drei Ziffern der Kontonummer weggelassen werden. Ich halte das nur für einen ersten Schritt in die richtige Richtung und werde weiter auf ein völliges Weglassen der Kontonummer in der Anschrift drängen.

21 Telekommunikation

21.1 Regelung über Fangschaltung und Einsatz von Zählvergleichseinrichtungen in TDSV verfassungswidrig

In seiner Entscheidung vom 25. März 1992 (1 BvR 1430/88) hat das Bundesverfassungsgericht meine Zweifel an der Tragfähigkeit der Verordnungsermächtigung in § 30 Abs. 2 Postverfassungsgesetz für den Erlaß von Datenschutzverordnungen (vgl. zuletzt 11. TB Anlage 6 Nr. 4 S. 103) bestätigt.

Der Gegenstand der Entscheidung gab dem Bundesverfassungsgericht Anlaß, die in § 8 der TELEKOM-Datenschutzverordnung (TDSV) enthaltenen Regelungen über Fangschaltungen und Zählvergleichseinrichtungen einer verfassungsrechtlichen Prüfung zu unterziehen. Die wichtigste — und für den Datenschutz sehr positive — Aussage des Gerichts geht dahin, daß „*sämtliche* der Post zur Beförderung oder Übermittlung anvertrauten Kommunikationsvorgänge und -inhalte den Schutz des Artikel 10 Abs. 1 GG genießen." Demgegenüber waren die Post und ein Teil der Rechtsprechung bisher von „immanenten" oder „betriebsbedingten Schranken" des Grundrechts aus Artikel 10 GG ausgegangen, die sich aus den Erfordernissen eines störungsfreien und ordnungsgemäßen Betriebs ergeben und derartige Kontrollmaßnahmen abdecken sollten.

Mit der genannten Entscheidung steht fest, daß es gegenwärtig keine gesetzliche Grundlage für eine Beschränkung des Fernmeldegeheimnisses durch Fangschaltung oder Zählvergleichseinrichtung gibt. Das Bundesverfassungsgericht machte allerdings auch deutlich, daß diese fehlende gesetzliche Eingriffsermächtigung für eine Übergangszeit nicht zur Unzulässigkeit des Einsatzes dieser Mittel führt, wenn dies zum Schutz anderer grundrechtlich geschützter Belange von Fernsprechteilnehmern unerläßlich ist. Das hat das Bundesverfassungsgericht z. B. angenommen, wenn Fangschaltung oder Zählvergleichseinrichtung zur Abwehr bedrohender oder belästigender anonymer Anrufe eingesetzt werden. Durch solche Anrufe kann in das allgemeine Persönlichkeitsrecht (Artikel 2 Abs. 1 GG i. V. m. Artikel 1 Abs. 1 GG) und das Recht auf körperliche Unversehrtheit (Artikel 2 Abs. 2 GG) eingegriffen werden. Zur Abwehr derartiger Angriffe hält das Bundesverfassungsgericht Fangschaltungen und Zählvergleichseinrichtungen im Rahmen des Unerläßlichen in einer Übergangszeit für zulässig; der Gesetzgeber ist aber verpflichtet, „alsbald" einen verfassungsmäßigen Zustand herzustellen.

Die Entscheidung des Bundesverfassungsgerichtes bedeutet, daß auch andere Registrierungen von Telefondaten ohne Einwilligung der beteiligten Kommunikationspartner eine gesetzliche Regelung erfordern. Damit stellt sich zwangsläufig die Frage, welche

Eingriffe in der Übergangszeit ohne Vorhandensein einer Rechtsgrundlage als „unerläßlich" hingenommen werden können. Hierzu habe ich mich unmittelbar nach der Entscheidung mit dem Bundesminister für Post und Telekommunikation in Verbindung gesetzt. Dabei habe ich den weitgehenden Einsatz von Fangschaltungen und Zählvergleichseinrichtungen, wie die Telekom ihn bisher praktiziert hat, für nicht mehr zulässig erklärt. Auf die Darstellung unter 21.6 weise ich hin. Das BMPT hat zugesagt, den Entwurf eines Gesetzes, mit dem eine gesetzliche Grundlage für die notwendigen Eingriffe in das Grundrecht des Artikel 10 GG geschaffen werden soll, so rechtzeitig vorzulegen, daß er noch in dieser Legislaturperiode verabschiedet werden kann. Bei dessen Erarbeitung bin ich beteiligt.

21.2 Telekom konnte Datenschutzverordnungen nur teilweise in die Praxis umsetzen.

Das Poststrukturgesetz von 1989 hat die Grundlagen für die Neuregelung des Datenschutzes bei der Telekom geschaffen. Danach war die Bundesregierung verpflichtet, „Vorschriften zum Schutz personenbezogener Daten der am Fernmeldeverkehr Beteiligten" zu erlassen. Dies galt sowohl für das neue Unternehmen Deutsche Bundespost Telekom als auch für Privatunternehmen, die Telekommunikationsdienstleistungen erbringen, z. B. private Betreiber von Funktelefonnetzen. Dabei hat der Gesetzgeber durch wortgleiche Gestaltung der beiden Ermächtigungsvorschriften, nämlich § 30 Abs. 2 Postverfassungsgesetz und § 14 a Fernmeldeanlagengesetz, seinen Willen zum Ausdruck gebracht, daß in beiden Bereichen dem Kunden ein gleichwertiger Schutz seiner personenbezogenen Daten zu gewährleisten ist. Auf dieser Grundlage wurden die TDSV, die am 1. Juli 1991 in Kraft getreten ist, und die weitgehend wortgleiche Teledienstunternehmen-Datenschutzverordnung (UDSV) erlassen.

Die Verordnungen stellten einen vertretbaren Kompromiß zwischen dem Schutz der Betroffenen einerseits und den betrieblichen und kommerziellen Anliegen der Unternehmen andererseits dar. Aus verfassungsrechtlichen Gründen können allerdings zahlreiche Vorschriften derzeit nicht uneingeschränkt angewandt werden, nämlich diejenigen, die die Verarbeitung von Daten regeln, die dem Schutz des Fernmeldegeheimnisses unterliegen (s. o. 21.1).

21.2.1 Wahlrecht der Telekom-Kunden für die Verbindungsdatenspeicherung nicht realisiert

Einige der Regelungen der TDSV sollten erst dann in Kraft treten, wenn die zu ihrer Durchführung erforderlichen Datenverarbeitungsprogramme verfügbar sind, spätestens aber am 1. Juli 1992. Dies betrifft auch das Recht des Telefonkunden zu bestimmen, was mit den Daten geschieht, die über seine Telefonate gespeichert werden. Er hat danach das Recht zu wählen, ob diese Verbindungsdaten vollständig gelöscht oder unter Verkürzung der Zielrufnummer um die letzten drei Ziffern für weitere 80 Tage gespeichert werden sollen. Die Verordnung sieht eine Speicherung der vollständigen Verbindungsdaten über den Zeitpunkt der Rechnungsstellung hinaus nur vor, wenn der Kunde eine detaillierte Telefonrechnung („Einzelverbindungsnachweis") beantragt hat. Eine solche würde aber in das Fernmeldegeheimnis der Beteiligten eingreifen; sie ist daher derzeit in der von der Verordnung vorgesehenen Form nicht zulässig (s. u. 21.2.2).

Die Deutsche Bundespost Telekom war bisher nicht in der Lage, die in der TDSV vorgeschriebenen Wahlmöglichkeiten technisch zu realisieren. Zum Jahresende 1992 kündigte die Telekom an, zum Beginn des Jahres 1993 zunächst die Wahlmöglichkeit zwischen vollständiger Löschung und verkürzter Speicherung anzubieten. Hiergegen habe ich keine Bedenken.

Im übrigen ist zu betonen, daß Verbindungsdatenspeicherungen bislang ausschließlich bei ISDN- und Funktelefonanschlüssen sowie bei Benutzung der „Telekarte" erfolgen; der „normale" Telefonanschluß, den derzeit noch die meisten Telekom-Kunden haben („Analoganschluß"), ist somit nicht betroffen.

21.2.2 Probleme beim Einzelverbindungsnachweis und bei Anrufen z. B. bei der Telefonseelsorge

In vielen Eingaben beklagen sich Bürger auch bei mir über ihre Schwierigkeiten, wenn sie gegenüber der Deutschen Bundespost Telekom die Höhe ihrer Telefonrechnung beanstanden: Im Regelfall ist es weder der Telekom selbst noch dem Kunden möglich, die Entgelte der einzelnen Verbindungen im abgelaufenen Rechnungsmonat und somit die Gesamthöhe der Rechnung zu überprüfen. Dies scheitert vor allem an der alten Technik in den Vermittlungsstellen der Telekom, die allerdings sukzessive durch eine neuere ersetzt wird, die eine Erfassung der einzelnen Verbindungen grundsätzlich ermöglicht und damit auch zu einer Überprüfbarkeit der Telefonrechnung beitragen kann. Entsprechend beabsichtigt die DBP Telekom daher, ihren Kunden gegen ein zusätzliches Entgelt neben der „normalen", pauschalierten Telefonrechnung auch eine detaillierte Rechnung in Form eines „Einzelverbindungsnachweises" (EVN) anzubieten. Die entsprechenden Regelungen enthält § 6 Abs. 9 TDSV. Diese Vorschrift stellt aber Bedingungen für das Erteilen eines EVN; so müssen z. B. die Haushaltsangehörigen des Antragstellers damit einverstanden sein. § 6 Abs. 9 TDSV bestimmt auch den Inhalt des EVN: für jedes einzelne Gespräch werden die vollständigen Verbindungsdaten — Zeitpunkt, Dauer, Verbindungsentgelt und Rufnummer des angerufenen Anschlusses — angegeben.

Diese Verbindungsdaten unterliegen dem grundrechtlich geschützten Fernmeldegeheimnis aus Artikel 10 GG. Wie das Bundesverfassungsgericht in seiner „Fangschaltungsentscheidung" festgestellt hat, stellt die TDSV für die Verarbeitung dieser Daten keine verfassungsgemäße Grundlage dar (s. o. 21.1); der Gesetzgeber ist daher aufgefordert, auch hierfür eine gesetzliche Grundlage zu schaffen. In der Übergangszeit dürfen Daten zur Erstellung eines EVN nur

dann erhoben und verarbeitet werden, soweit dies „unerläßlich" ist. Angesichts der Tatsache, daß die Telefonkunden, deren Anschlüsse noch mit alter Technik ausgestattet sind, keinen EVN erhalten können, dürfte es schwer sein, für Kunden, die bereits über die neue Technik angeschlossen sind, einen EVN als „unerläßlich" anzusehen. Auch auf eine Einwilligung der Betroffenen kann die Datenverarbeitung im Ergebnis nicht gestützt werden. Zwar erscheint es möglich, eine Einwilligung des Anschlußinhabers und seiner Haushaltsangehörigen zu erreichen. Von der für einen EVN erforderlichen Datenverarbeitung sind aber auch die Personen betroffen, die angerufen wurden. Von diesen eine Einwilligung zur Datenverarbeitung rechtzeitig zu erlangen, dürfte praktisch unmöglich sein.

Ein weiteres Problem des EVN ergibt sich aus der Notwendigkeit, Menschen zu schützen, die sich in Notsituationen befinden und z. B. die Hilfe der Telefonseelsorge oder auch anderer Beratungsstellen, wie etwa einer Drogenberatung, in Anspruch nehmen. Erfahrungsgemäß möchte ein großer Teil dieser Menschen die jeweilige Beratung anonym durchgeführt wissen. Der Ausdruck der Telefonnummer einer angerufenen Beratungsstelle im EVN würde diese Anonymität zumindest gefährden und den Betroffenen u. U. Repressalien des Anschlußinhabers aussetzen.

Die TDSV sieht deshalb vor, daß „der Anruf bei Personen, Behörden und Organisationen, die selbst oder deren Mitarbeiter besonderen Verschwiegenheitsverpflichtungen unterliegen und die Beratungsaufgaben in sozialen oder kirchlichen Bereichen ganz oder überwiegend über Telefon abwickeln, . . . aus dem Nachweis nicht ersichtlich sein" darf (§ 6 Abs. 9 Satz 5 TDSV). Über diese Vorschrift bestand schon vor dem Erlaß der TDSV, nämlich seit Frühjahr 1991, Klarheit. Gleichwohl konnte die Telekom bis Ende 1992 kein Konzept vorlegen, das diese Vorschrift technisch-organisatorisch umsetzt. Dies ist nur schwer nachvollziehbar, weil bereits frühzeitig verschiedene Modelle diskutiert worden waren. Eine optimale Lösung wäre es, den durch die Vorschrift privilegierten Beratungsstellen eine sog. „Service 130" — Rufnummer zuzuteilen, bei der Anrufe für den Anrufenden kostenlos sind und die daher überhaupt nicht im EVN erscheinen. Als „zweitbeste" Lösung war von mir vorgeschlagen worden, die Anrufe bei den privilegierten Stellen mit solchen bei den Ansage- und Auskunftsdiensten der Telekom — Telefonauskunft, Wetterdienst, Zeitansage usw. — zusammenzufassen und gemeinsam lediglich mit Angabe der Entgeltsumme — etwa unter der Bezeichnung „Anrufe bei Auskunfts-, Ansage- und Beratungsstellen" — im EVN auszuweisen. Zwei Voraussetzungen müssen für eine solche Lösung jedoch gegeben sein: Zum einen muß eine ausreichende Anzahl „unverfänglicher" Ansage- und Auskunftsdienste ein „Verstecken" von Anrufen bei privilegierten Stellen auch wirklich ermöglichen. Zum anderen sollte die Telekom verstärkt die technischen Möglichkeiten nutzen, um noch mehr Telefonanschlüsse so zu schalten, daß Anrufe bei der Telefonseelsorge und ähnlichen Beratungsstellen „zeittaktfrei", also unabhängig von der Dauer des Gesprächs um den Preis einer Gebühreneinheit, erfolgen können; dies ist bislang nur aus den Ballungsräumen möglich.

Da die Telekom die Schutzvorschrift des § 6 Abs. 9 Satz 5 TDSV derzeit nicht umsetzen kann, bietet sie bisher folgerichtig auch keinen EVN an. Es muß also abgewartet werden, wann die Telekom in der Lage sein wird, den EVN zu realisieren, wie — angesichts des nicht geringen Entgeltes dafür — die Akzeptanz sein wird und welche Probleme durch den EVN bei Telekom-Kunden entstehen können.

21.3 Nicht nur die Telekom gibt Telefonbücher heraus

Der Infrastrukturrat der Deutschen Bundespost hat beschlossen, die Herausgabe von Telefonbüchern dem Wettbewerb zu öffnen, sie also nicht mehr ausschließlich durch die Deutsche Postreklame GmbH, eine Tochtergesellschaft der Telekom, vornehmen zu lassen.

Die Herausgabe von „öffentlichen Kundenverzeichnissen" ist für die Telekom in § 10 Abs. 1 TDSV geregelt. Danach darf „die Deutsche Bundespost Telekom öffentliche Verzeichnisse ihrer Kunden . . . herausgeben oder herausgeben lassen". Aus Sicht des Datenschutzes ist es daher im Ergebnis vertretbar, wenn die Telekom Namen, Anschrift und Rufnummer ihrer Kunden nicht nur an die Deutsche Postreklame GmbH, sondern auch an deren private Wettbewerber zum Erstellen von Teilnehmerverzeichnissen übermittelt, freilich unter der Voraussetzung, daß eine Verarbeitung und Nutzung durch den Empfänger nur für den Zweck „öffentliche Verzeichnisse von Telekom-Kunden" erfolgt. Dies bedeutet, daß die Daten nur zum Erstellen von öffentlichen Telefonverzeichnissen verwendet werden dürfen und das Widerspruchsrecht des Kunden (s. u.) beachtet werden muß. Die Zweckbindung der übermittelten Daten ist durch eine entsprechende vertragliche Regelung zwischen der Deutschen Bundespost Telekom und dem kommerziellen Nutzer zu gewährleisten. Die Deutsche Bundespost Telekom hat dies zugesagt und wird mich bei der Gestaltung eines solchen Mustervertrages beteiligen.

Möchte der Kunde nicht in solchen Telefonverzeichnissen geführt werden oder wünscht er nur einen bestimmten Eintrag, so muß auf entsprechenden Widerspruch oder Hinweis des Kunden die Eintragung ganz oder teilweise unterbleiben. Auf dieses Recht ist der Kunde von der Telekom hinzuweisen.

Der Widerspruch eines Kunden gegen die Eintragung gemäß § 10 Abs. 3 TDSV bewirkt ein generelles Verbot, seine Daten in irgend ein Teilnehmerverzeichnis aufzunehmen, unabhängig von dessen Art und vom Herausgeber. Ein „selektives Widerspruchsrecht" gegen die Eintragung in bestimmte — z. B. elektronische — Teilnehmerverzeichnisse bei Duldung der Eintragung in andere Verzeichnisse wird von der Verordnung leider nicht zwingend gefordert. Es könnte zwar als freiwillige kundenfreundliche Leistung von der Telekom angeboten werden, diese hat jedoch wiederholt dargelegt, daß ein selektiver

Widerspruch mit ganz erheblichem zusätzlichem organisatorischem Aufwand verbunden wäre, der nur durch eine Erhöhung der Entgelte abzufangen wäre. Daher habe sie nicht vor, ihn anzubieten. Im Ergebnis bedeutet dies, daß bei einem Widerspruch des Kunden gemäß § 10 Abs. 3 TDSV die Eintragung sowohl in den öffentlichen Kundenverzeichnissen der Telekom als auch in denen aller anderen Herausgeber unterbleibt.

21.4 Kundendaten der Telekom können zu Werbezwecken verwendet werden

Die Deutsche Bundespost Telekom darf die Bestandsdaten ihrer Kunden — Name, Anschrift, Angaben zum Vertragsinhalt (§ 4 Abs. 1 TDSV) — zur Werbung für eigene Produkte und Dienstleistungen verarbeiten und nutzen, soweit der Kunde dem nicht widersprochen hat. Auf dieses Widerspruchsrecht weist die Telekom ihre Kunden hin.

Nicht allen Telefonkunden ist bekannt, daß die Telekom — über ihre Tochtergesellschaft Deutsche Postreklame GmbH — die Anschriften ihrer Kunden auch an Dritte für deren eigene Werbezwecke verkauft, allerdings nur die Anschriften derjenigen, die einer Eintragung ins Telefonbuch (s. o. 21.3) nicht widersprochen haben. Die Telekom vertritt dabei die Auffassung, bei den Kundenanschriften, die in dieser Weise im Telefonbuch veröffentlicht sind, handele es sich um „Daten aus allgemein zugänglichen Quellen", deren Verarbeitung oder Nutzung nach Maßgabe des § 28 Abs. 1 Nr. 3 BDSG zulässig sei. Eine solche Auslegung der Vorschrift ist nicht abwegig; von großer Bedeutung ist es jedoch, daß der Telefonkunde hierüber in angemessener Weise informiert wird, damit er entscheiden kann, ob er damit einverstanden ist. Gemäß § 28 Absatz 3 BDSG hat er nämlich das Recht, der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung gegenüber der speichernden Stelle zu widersprechen. Adressat eines Widerspruches ist die speichernde Stelle, also die Deutsche Postreklame GmbH oder das jeweilige Unternehmen, das an den Kunden mit Werbung herantritt.

Es ist Aufgabe der Telekom, ihre Kunden auf diese Sachverhalte hinzuweisen und sie zu erläutern. Das zunächst hierfür angewandte Verfahren, bei dem den Telefonrechnungen ein Zettel mit dürftigen Informationen beigefügt worden war, war jedoch völlig ungenügend (s. u. 21.5).

In den daraufhin auf mein Drängen — und unter meiner Mitwirkung — formulierten „Hinweisen zum Datenschutz für unsere Telefonkunden" informiert die Telekom jetzt auch über die Verwendung der Kundendaten für Zwecke von Marktforschung und Werbung und weist auf das Widerspruchsrecht, aber auch auf die Möglichkeit der Eintragung in die sogenannte „Robinsonliste" hin (s. u. 21.5). Die Deutsche Postreklame GmbH berücksichtigt übrigens auch die „Robinsonliste"; Daten der dort Eingetragenen werden von ihr für Werbezwecke nicht weitergegeben.

21.5 Unzutreffende Information der Telekom-Kunden abgestellt

Die Deutsche Bundespost Telekom verarbeitet und nutzt personenbezogene Daten ihrer Kunden in vielfältiger, auch den einzelnen Dienststellen der Telekom selbst keineswegs vollständig bekannter und überschaubarer Weise. Dies gilt sowohl für die sog. Bestandsdaten — Name, Anschrift und Angaben über die vertraglich vereinbarten Dienstleistungen — als auch für Verbindungsdaten — Zeitpunkt, Dauer, Entgelt und angewählte Nummer einer Verbindung —; letztere unterliegen dem Schutz des grundgesetzlich garantierten Fernmeldegeheimnisses.

Auch und gerade im einem derartig komplexen technischen und organisatorischen System muß es dem Betroffenen möglich sein, sein Recht auf informationelle Selbstbestimmung wahrzunehmen, nämlich selbst zu bestimmen, welche Information er wem zu welchem Zweck gibt und an wen sie ggf. weitergegeben wird. Dies kann er aber nur, wenn ihm das gesamte Verfahren der Verarbeitung seiner personenbezogenen Daten hinreichend nachvollziehbar und transparent ist. Diese Transparenz benötigt der Telefonkunde außerdem, um ggf. von seinem Widerspruchsrecht Gebrauch machen zu können, z. B. gegenüber einer Verwendung seiner Daten für Werbezwecke (s. o. 21.4).

Die Bundesregierung hat bei der Ausarbeitung der TDSV die Bedeutung dieses Punktes gesehen und die Telekom verpflichtet, „die Beteiligten in angemessener Weise über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten" (§ 3 Abs. 4 TDSV). Dieser Verpflichtung versuchte die Telekom dadurch zu entsprechen, daß sie den monatlichen Rechnungen aller Telefonkunden einmalig einen Zettel beifügte, der zur Hälfte mit eigener Werbung bedruckt war, auf der Rückseite allerdings „Hinweise zum Datenschutz für unsere Telefonkunden" gab. Der Text, der mir erst durch eine Vielzahl von Eingaben aufgebrachter Bürger bekannt wurde, war nicht nur wegen seiner äußerst knappen Fassung ungeeignet, die Telekom-Kunden zutreffend und hinreichend zu informieren; er enthielt sogar unzutreffende Angaben.

Ich habe der Generaldirektion der Telekom daraufhin einen besseren Text vorgeschlagen, der inzwischen im wesentlichen übernommen wurde. Er wird künftig nicht nur den Neukunden im Zusammenhang mit dem Auftrag zur Einrichtung eines Telefonanschlusses ausgehändigt, sondern auch in das Amtliche Telefonbuch aufgenommen (s. Anlage 12).

21.6 Wer sich über die Telefonrechnung beschwerte, wurde heimlich mit einer Zählvergleichseinrichtungen kontrolliert

Im Rahmen der Kontrolle eines Fernmeldeamtes habe ich mich über die Praxis der Telekom beim Einsatz von Zählvergleichseinrichtungen (ZVE) und des befristeten Zählvergleichs (BZV) informiert. Mit ZVE- oder BZV-Schaltungen kann festgehalten werden, ob von einem bestimmten Telefonanschluß Telefonanrufe

abgegangen oder ob solche dort angekommen sind. Dabei werden Verbindungsdaten der erfaßten Anrufe gespeichert. Für abgehende Verbindungen werden — auch im Falle der Nichtannahme des Anrufs — Zeitpunkt und angewählte Nummer sowie gegebenenfalls Dauer und angefallene Gebühreneinheiten, bei ankommenden Verbindungen lediglich Zeitpunkt und Dauer registriert.

Solche Schaltungen können bei unerklärlich hoher Rechnung im Kundenauftrag zur Kontrolle der Telefonrechnung vorgenommen werden.

ZVE- und BZV-Schaltungen werden im Kundenauftrag auch vorgenommen, um zu überprüfen, ob belästigende oder bedrohende Anrufe von einem bestimmten Telefonanschluß, den der Telefonkunde angegeben hat, ausgehen.

Erhob ein Telefonkunde Einwendungen gegen seine Telefonrechnung, wurde für seinen Anschluß von der Telekom regelmäßig für den Zeitraum von zwei oder vier Wochen eine ZVE-Schaltung veranlaßt. Der Kunde wurde davon nicht informiert. Eine solche Maßnahme greift in das Fernmeldegeheimnis ein. Nach der Entscheidung des Bundesverfassungsgerichtes zu Fangschaltung und Zählvergleichseinrichtung (s. o. 21.1) gibt es dafür keine Rechtsgrundlage mehr: Deshalb mußte das Verfahren — zum Schutz der Persönlichkeitsrechte sowohl des Anschlußinhabers als auch der Angerufenen — geändert werden.

Nach anfänglichem Zögern der Telekom wurden auf mein Drängen im Januar 1993 unter Mitwirkung des BMPT mit der Telekom die Grundzüge eines neuen Verfahrens vereinbart. Danach soll eine ZVE- oder BZV-Schaltung bei Einwendungen gegen die Telefonrechnung nur dann erfolgen, wenn der Kunde in diesem Zusammenhang einen Auftrag zur Überprüfung der technischen Einrichtungen ausgefüllt und unterschrieben hat. Darin wird er auch auf die von der Telekom vorgesehene ZVE-/BZV-Schaltung hingewiesen, die ihm ausführlich erläutert wird.

Zum Schutz der Angerufenen, deren Rufnummern zunächst auf dem ZVE-Streifen ausgedruckt werden, soll sichergestellt werden, daß dieser unverzüglich ausgewertet — die Rufnummern sollen dabei zumindest um die letzten drei Stellen gekürzt werden — und sofort vernichtet wird.

Die Umsetzung dieser Absprache werde ich beobachten.

Auf Veranlassung des Forschungs- und Technologiezentrums (FTZ) — früher: Fernmeldetechnisches Zentralamt — der Telekom ließen die Oberpostdirektionen bei allen Fernmeldeämtern die Telefonanschlüsse einer bestimmten Anzahl von Kunden mittels ZVE-Schaltung überwachen, um das Kundenverhalten von verschiedenen Berufsgruppen zu ermitteln (sog. Verkehrssondermessungen). Die Erhebung, Verarbeitung und Nutzung von dem Fernmeldegeheimnis unterliegendem Verbindungsdaten für diese Zwecke war unter keinem rechtlichen Gesichtspunkt zulässig. Nachdem ich dieses Verfahren gem. § 25 BDSG beanstandet hatte, hat die Deutsche Bundespost Telekom das FTZ angewiesen, keine weiteren Sondermessungen zu veranlassen.

Bei der eingangs erwähnten Kontrolle habe ich auch festgestellt, daß die Systemsicherheit der eingesetzten Rechner in den Vermittlungsstellen nicht den Anforderungen der Anlage zu § 9 Satz 1 BDSG entsprach. So waren die zur Authentifikation verwendeten Paßwörter nicht individuell, sondern für Benutzergruppen vergeben worden.

Auch hatten nach meinen Feststellungen außer dem Fernmeldeamt selbst auch die Oberpostdirektion und die nicht zum Fernmeldeamt gehörige Dienststelle Zentrale Instandhaltung Zugriff auf die Rechner.

Diese in hohem Maß risikoträchtige Systemgestaltung habe ich beanstandet. Die Telekom hat diese Beanstandung aber nur hinsichtlich der Gruppenpaßwörter anerkannt und die Einführung individueller Paßwortgestaltung zugesagt.

Der Zugriff auf die Daten durch die Oberpostdirektion ist nach Darstellung der Telekom nicht möglich; den Zugriff durch die Dienststelle Zentrale Instandhaltung hält die Telekom für erforderlich; die Beseitigung von Störungen erfordere ein hohes Maß an an Expertenwissen, daß nur zentral bereitgestellt werden könne.

Ich werde sowohl die Realisierung der zugesagten Änderungen als auch die noch bestehenden Unklarheiten und Defizite im Rahmen einer weiteren Kontrolle überprüfen.

21.7 Risiko zu langer Überwachung des Fernmeldeverkehrs nach der Strafprozeßordnung

Bei Ermittlungen wegen besonders schwerwiegender Straftaten kann durch Gerichtsbeschluß die Überwachung und Aufzeichnung des Telefonverkehrs der Verdächtigten angeordnet werden (s. auch 24.6). Die Strafprozeßordnung (§§ 100 a, 100 b) benennt diese Straftaten abschließend und enthält auch Regelungen über das dabei zu beachtende Verfahren. Ist eine solche Anordnung ergangen, hat die Deutsche Bundespost Telekom wie auch jeder andere Betreiber einer für den öffentlichen Verkehr bestimmten Fernmeldeanlage — z. B. eines Funktelefonnetzes — den Berechtigten die Überwachung und Aufzeichnung des Telefonverkehrs zu ermöglichen.

Mitte 1992 habe ich bei einer Oberpostdirektion und einem ihr nachgeordneten Fernmeldeamt der Deutschen Bundespost Telekom die Einhaltung datenschutzrechtlicher Vorschriften bei der Durchführung von Maßnahmen zur Telefonüberwachung (TÜ), die nach den §§ 100 a und 100 b StPO angeordnet waren, kontrolliert. Da sich meine Kontrollkompetenz nur auf öffentliche Stellen des Bundes erstreckt (§ 24 Abs. 1 Satz 1 BDSG) und Bundesgerichte meiner Kontrolle nur insoweit unterliegen, wie sie in Verwaltungsangelegenheiten tätig werden (§ 24 Abs. 3 BDSG), bin ich von der Zulässigkeit der von der Deutschen Bundespost Telekom nach der Strafprozeßordnung durchgeführten Überwachungsmaßnahmen ausgegangen.

Meine Mitarbeiter haben nur geprüft, wie die Deutsche Bundespost Telekom die angeordneten Maßnahmen durchgeführt hat. Zu diesem Zweck wurden diese unter folgenden Gesichtspunkten geprüft:

— Sicherheit des bei der Telekom eingerichteten Verfahrens gegen unbefugte Veranlassung, d. h. ohne Vorliegen eines gerichtlichen Beschlusses;

— Korrektheit der Umsetzung des gerichtlichen Beschlusses durch die bei der Telekom veranlaßten Maßnahmen und

— Sicherung des Verfahrens gegen Kenntnisnahme durch Unbefugte.

Unter diesen Aspekten ist zu bemerken:

Die bestehenden dienstlichen Weisungen und die getroffenen Maßnahmen bieten einen sehr hohen Schutz gegen eine unbefugte Veranlassung von Maßnahmen der genannten Art sowohl durch Nichtberechtigte, als auch durch Bedienstete der Deutschen Bundespost Telekom.

Bei der praktischen Umsetzung eines gerichtlichen Beschlusses kommt es wesentlich darauf an, daß sich die Maßnahmen gegen den *richtigen* Telefonanschluß richten. Die bei der Telekom eingerichteten Verfahren bieten hohe Sicherheit gegen eine falsche Beschaltung durch Arbeitsfehler bei der Telekom.

Die Telefonüberwachung stellt eine zeitlich befristete Beschränkung eines Grundrechts dar. Die in der richterlichen Anordnung festgelegten Daten sind streng zu beachten. Probleme können auftreten, wenn die Anordnung den Beginn und das Ende der Maßnahme nicht exakt angibt (z. B. „vom 31. August 0.00 Uhr bis zum 30. September 24.00 Uhr"), sondern nur die Dauer festlegt (etwa: „für die Dauer von 4 Wochen"). Ich habe erhebliche Bedenken dagegen, daß in diesen Fällen nach einer internen Richtlinie für die Fristberechnung die Strafprozeßordnung (§§ 42, 43 StPO) herangezogen wird. Danach nämlich wird z. B. die Frist auf das Ende des nächsten Werktages verlängert, wenn sie an einem Feiertag endet. Was nach diesen allgemeinen strafverfahrensrechtlichen Fristenregelungen einen Vorteil für den Betroffenen bedeutet, darf ihm bei der Telefonüberwachung nicht zum Nachteil werden!

Ich habe zunächst das Bundesministerium der Justiz um Stellungnahme gebeten.

Das Problem kann dadurch ausgeräumt werden, daß die Gerichte bei Maßnahmen der Überwachung des Fernmeldeverkehrs exakte Zeitpunkte für Beginn und Ende der Frist angeben. Ich empfehle dringend, so zu verfahren.

21.8 Auch bei Textverarbeitung auf Personalcomputern muß Datenschutz gewährleistet sein

Die Generaldirektion der Deutschen Bundespost Telekom hat für ihren Geschäftsbereich die „Erhebung, Verarbeitung und Nutzung personenbezogener Daten auf PC-Einplatzsystemen" durch eine Verfügung neu geregelt.

Ich habe die Telekom hierbei beraten; meine „Empfehlungen für den Einsatz von Arbeitsplatzcomputern (APC)" (12. TB, Seite 114f.) sind überwiegend berücksichtigt worden. Unverständlich und bedenklich ist es jedoch, daß für die automatisierte *Textverarbeitung* eine Reihe von notwendigen Sicherheitsmaßnahmen nicht gelten sollen, wie z. B. die sichere Menüführung, die Protokollierung, die automatische Dunkelschaltung des Bildschirms bei längerer Abwesenheit des Benutzers, die kryptografische Verschlüsselung sensibler Texte und der Ausschluß einer freien Abfragesprache. Meinen Hinweis, daß Textverarbeitungsdateien im Regelfall in vollem Umfang den Bestimmungen des BDSG unterliegen und daß mit den verbleibenden Datensicherungsmaßnahmen jedenfalls für sensiblere Texte die Anforderungen des § 9 BDSG nicht zu erfüllen sind, hat die Telekom nicht beachtet.

Ich werde die Praxis des PC-Einsatzes nach der neuen Weisungslage kontrollieren. Eine Beanstandung etwaiger Mängel, die auf die beschriebenen Defizite in der Verfügung zurückzuführen sind, behalte ich mir vor.

21.9 Bekanntgabe von Telefonschulden an den Ehemann und die Großmutter der Schuldner

Daß Behörden nicht die Aufgabe haben, einen Bürger über Schulden seines Ehegatten oder eines nahen Verwandten „aufzuklären", ist bei der Telekom offenbar noch nicht überall bekannt. Ein Bürger teilte mir in einer Eingabe mit, sein Fernmeldeamt habe ihm mitgeteilt, seine Ehefrau habe Schulden gemacht, indem sie rückständige Fernmeldegebühren für ihren — inzwischen in Konkurs gegangenen — Geschäftsbetrieb bisher nicht beglichen habe. Zwei — offensichtlich vorgedruckte — Formulare wurden dem Bürger übersandt: Im ersten wurde er über die Tatsache, daß seine Ehefrau mit rückständigen Fernmeldegebühren belastet sei, informiert. Mit dem zweiten Formular wurde er um seine Einverständnis gebeten, daß die Rückstände von seinem Fernmeldekonto in Raten abgebucht werden dürfen; die Höhe der Telefonschulden wurde genau beziffert.

Nach Prüfung der Sach- und Rechtslage teilte ich der Generaldirektion der Deutschen Bundespost Telekom mit, daß es sich bei dem oben beschriebenen Vorgang um eine unzulässige Datenübermittlung gehandelt hat. Die Weitergabe von Kundendaten war zum Zeitpunkt des Vorgangs in § 454 Abs. 2 der Telekommunikationsordnung (TKO) eindeutig in dem Sinne geregelt, daß „. . . an Dritte . . . diese Daten nicht weitergegeben werden, es sei denn, die Weitergabe ist gesetzlich erlaubt oder der Teilnehmer hat der Weitergabe schriftlich zugestimmt". Die Telekom versuchte ihr Verhalten zu rechtfertigen und verwies u. a. auf § 1375 BGB, wonach Ehegatten für Verpflichtungen, die der jeweils andere bei Geschäften zur angemessenen Deckung des Lebensbedarfs eingeht, zu haften haben.

Ein kurzer Blick ins Gesetz zeigte die Unhaltbarkeit dieser Rechtsansicht. Die gesetzliche Haftung des Ehegatten erstreckt sich nämlich eindeutig nicht auf Verpflichtungen aus einer beruflichen oder gewerbli-

chen Tätigkeit des anderen Ehegatten. Ich habe daher eine förmliche Beanstandung ausgesprochen.

Nach einigem Widerstreben sagte die Telekom zu, künftig meiner Rechtsauffassung zu folgen.

Allerdings erreichte mich inzwischen eine weitere Eingabe zu demselben Thema, bei der Großmutter und Enkel beteiligt sind.

Ich sehe den Rechtsausführungen der Telekom mit Interesse entgegen.

21.10 Abhören von Funksendungen durch Unbefugte erleichtert

Rundfunkempfänger — die Stereoanlage oder der Fernseher zu Hause, der Radiorecorder ebenso wie das Autoradio — dürfen nur dann betrieben werden, wenn diese Geräte der „Allgemeingenehmigung für Ton- und Fernseh-Rundfunkempfänger" des Bundesministeriums für Post und Telekommunikation (BMPT) entsprechen. Erlaubt war danach bisher nur der Betrieb solcher Geräte, die — wie es technische Vorschriften des BMPT verlangten — Funksendungen nur in denjenigen Bereichen („Frequenzen") empfangen konnten, in denen üblicherweise *Rundfunksendungen* ausgestrahlt werden. Damit war es nicht zulässig, Rundfunkempfänger zu betreiben, mit denen etwa der Sprechfunkverkehr der Polizei mitgehört werden konnte. Solche Geräte waren in Deutschland allenfalls in Spezialläden und ausdrücklich „Nur für den Export" erhältlich.

Im April 1992 informierten mich Dritte über Pläne des BMPT, die dargestellte Beschränkung für den Betrieb von Rundfunkgeräten aufzuheben, d. h. auch den Betrieb von Allbandempfängern, „Scannern" und ähnlichen Geräten zuzulassen.

In einer Anhörung des BMPT zu der vorgesehenen Änderung der technischen Vorschriften, zu der ich übrigens nicht eingeladen war, brachte ich schwerwiegende Bedenken zum Ausdruck, die insbesondere vom BMI geteilt wurden. Meiner Bitte um Beteiligung wurde nicht entsprochen. Im August 1992 hob das BMPT die Begrenzung der Empfangsbereiche auf.

Von dieser Entscheidung sind neben den Benutzern schnurloser Telefone und der Polizei eine Vielzahl anderer Funkdienste betroffen, wie z. B. das B- und C-Funktelefonnetz der Telekom, die Funknetze von Rettungs- und Hilfsorganisationen und der Zugfunk der Bundesbahn. Sie führt zu gravierenden Risiken für die Vertraulichkeit der mit Hilfe von Funkanlagen übertragenen Informationen und hebt das Fernmeldegeheimnis in ganzen Bereichen, so etwa für die Benutzer schnurloser Telefone, die bereits stark verbreitet sind, faktisch weitgehend auf.

Ein wirksamer Schutz der Vertraulichkeit der auf den Funknetzen übertragenen Daten ist nach derzeitigem Stand der Technik nur durch eine kryptografische Verschlüsselung der auf dem Funkwege übermittelten Informationen möglich (s. u. Nr. 30.3). Entsprechende Techniken stehen zwar zur Verfügung; ihr praktischer Einsatz ist aber schon aus finanziellen und organisatorischen Gründen meist nicht kurzfristig realisierbar. Deshalb wäre vor der Entscheidung des BMPT zumindest eine angemessene Übergangsfrist erforderlich gewesen.

Ich habe die obersten Bundesbehörden in einem Rundschreiben auf die Problematik aufmerksam gemacht und das BMPT um Äußerung gebeten, insbesondere wie das Fernmeldegeheimnis der Betroffenen geschützt werden kann und soll. Das BMPT hat mir mitgeteilt, die Aufhebung sei erforderlich gewesen, weil die Empfangsbereichsbegrenzung ein nach europäischem Recht unzulässiges Wettbewerbshemmnis gewesen sei. Artikel 36 des EWG-Vertrages erlaubt Handelsbeschränkungen allerdings, wenn sie „aus Gründen der öffentlichen Sittlichkeit, Ordnung und Sicherheit . . . gerechtfertigt sind." Es ist unbefriedigend und nicht verständlich, daß das BMPT darauf überhaupt nicht eingegangen ist.

Auch die Ständige Konferenz der Innenminister und -senatoren der Länder hat ihre Besorgnisse über die Auswirkungen der Entscheidung des BMPT auf die Belange der öffentlichen Sicherheit vorgetragen und das BMPT nachdrücklich aufgefordert, die Empfangsbereiche für Rundfunkempfänger wieder zu beschränken. Auch im Ausschuß für Post und Telekommunikation des Deutschen Bundestages wurde die Vorgehensweise des BMPT kritisiert. Inzwischen hat das Bundesministerium für Post und Telekommunikation die Forderung der Innenministerkonferenz zurückgewiesen und die Auffassung vertreten, daß angesichts des seines Erachtens einzig gangbaren „Weges der Liberalisierung und Harmonisierung . . . die von den Sicherheitsbehörden geäußerten Bedenken zurücktreten" müssen.

21.11 Auch große behördeninterne Telekommunikationsanlagen erzeugen datenschutzrechtliche Risiken

Der Generationswechsel von konventionellen Telefonanlagen zu modernen, digitalisierten „Telekommunikationsanlagen" (TK-Anlagen) vollzieht sich in zunehmendem Maße auch bei Behörden und sonstigen öffentlichen Stellen des Bundes. Zu den damit verbundenen datenschutzrechtlichen Problemen der Telefondatenverarbeitung habe ich mich wiederholt geäußert (zuletzt im 13. TB S. 44, S. 84 i. V. m. Anlage 12). Im Berichtszeitraum hat sich auch die Datenschutzkonferenz mit dieser Frage befaßt (s. Anlage 7).

Um mich darüber zu informieren, welche Probleme beim Betrieb einer großen behördeninternen Telekommunikations-Anlage in der Praxis auftreten und wie sie gelöst werden, habe ich Anfang 1992 eine von drei Bundesministerien gemeinsam genutzte Anlage kontrolliert. Diese Anlage wurde im September/Oktober 1990 am Hauptstandort der Ministerien installiert und seit der Zeit betrieben; zum Zeitpunkt der Kontrolle stand sie kurz vor der formellen Übergabe durch die Lieferfirma an die Ministerien. Der installierte Telekommunikationskomplex besteht im wesentlichen aus fünf digitalen ISDN-Telekommunikationsanlagen, über die ca. 2 400 Nebenstellen auf insge-

samt 200 Amtsleitungen nachrichtentechnisch versorgt werden.

Alle drei Bundesministerien haben mit ihren Personalvertretungen Dienstvereinbarungen über die Verarbeitung von Telefondaten der Bediensteten abgeschlossen.

Die bei der Nutzung der TK-Anlage entstehenden Verbindungsdaten werden in einem — vom gemeinsamen Zentralen Technischen Dienst für alle drei Ministerien betriebenen — Vermittlungsrechner erfaßt. Nach Beendigung einer jeden Verbindung wird der betreffende Verbindungsdatensatz — der stets gleichartig aufgebaut ist — über eine Leitung an den sog. Erfassungsrechner des jeweiligen Ministeriums übertragen, der räumlich vom Vermittlungsrechner getrennt und vom jeweiligen Ministerium in eigener ausschließlicher Verantwortung betrieben wird.

Im Erfassungsrechner wird der Verbindungsdatensatz — nach den für das jeweilige Ministerium geltenden Regelungen — gekürzt und als Gesprächsdatensatz gespeichert. Die Gesprächsdatensätze eines Monats werden auf Disketten kopiert und so in den jeweiligen „Auswerterechner" — jedes Ministerium hat wiederum einen eigenen — übertragen, mit dessen Hilfe sie entsprechend den im Ministerium geltenden Regelungen ausgewertet werden.

Zur technisch-organisatorischen Ausgestaltung des geschilderten Verfahrens haben meine Mitarbeiter eine Reihe von Feststellungen getroffen, die zwar einerseits durch die Größe der Anlage und die Aufteilung der Kompetenzen an ihrem Standort bedingt waren, andererseits jedoch in modifizierter Form bei der Installation und dem Betrieb von TK-Anlagen überhaupt gelten und deshalb beachtet werden sollten:

a) Gestaltung und Einhaltung der Datensicherungsmaßnahmen lagen über ein Jahr nach Inbetriebnahme der Anlagen immer noch weitgehend in der Hand der Lieferfirma. Als besonders problematisch habe ich die *Gestaltung der Identifikations- und Authentifikationsverfahren* und den Zugang zu allen Teilen der TK-Anlage gewertet. Die Mitarbeiter der Lieferfirma hatten zum Teil dieselben, oftmals sogar weitergehende Zugriffsmöglichkeiten als die Betreiber, jedenfalls erheblich weitergehende Kenntnisse über die technischen Möglichkeiten der Anlage und hätten daher jederzeit ohne, ja sogar gegen den Auftrag der Betreiber Informationen zur Kenntnis nehmen und Änderungen an gespeicherten Daten vornehmen können. Ich habe darauf gedrungen, Maßnahmen einzuleiten, die sicherstellen, daß die technischen und organisatorischen Maßnahmen nach § 9 BDSG sowie der Anlage zu § 9 Satz 1 BDSG durch die Betreiber der TK-Anlage in eigener Verantwortung wahrgenommen und gleichzeitig die Zugangs- und Zugriffsrechte der Lieferfirma eingeschränkt werden.

b) Wie meinen Mitarbeitern mitgeteilt wurde, war zum Zeitpunkt der Kontrolle *für alle Servicefunktionen nur ein Paßwort* eingerichtet, das allen Mitarbeitern der Lieferfirma, die mit der TK-Anlage befaßt waren — möglicherweise sogar bundesweit — sowie weiteren drei Mitarbeitern des Zentralen Technischen Dienstes bekannt war. Dieses Verfahren entspricht nicht den Anforderungen des § 9 BDSG und der Anlage hierzu. Ich verweise zu diesem Problem auf mein Rundschreiben an die obersten Bundesbehörden vom 11. Dezember 1991, mit dem ich Empfehlungen zur Paßwortgestaltung und zum Sicherheitsmanagement gegeben habe (s. Anlage 13).

c) Wohl bedingt durch die Tatsache, daß die TK-Anlage noch nicht an die Nutzer übergeben war, existierten keine *speziellen schriftlichen Regelungen* über die Einrichtung von Anschlüssen, die Änderung von Leistungsmerkmalen und Berechtigungen usw., die zentral am Vermittlungsrechner durchgeführt werden. Ich habe empfohlen, das Verfahren unter Berücksichtigung der Verantwortlichkeiten sowie der Forderungen der Anlage zu § 9 Satz 1 BDSG revisionsfähig zu gestalten und schriftlich zu regeln.

d) Die meisten *Telefon-Endgeräte*, nämlich die Standardapparate, waren — anders als die mittels Chipkarte abschließbaren Komfortapparate — nur mit einfachen mechanischen Schloßschaltern gesichert. Bei solchen Schlössern werden erfahrungsgemäß eine begrenzte Zahl gruppengleicher Schlüssel vergeben. Dies bietet die Möglichkeit, Apparate unberechtigt aufzuschließen, zu benutzen und die im Apparat gespeicherten personenbezogenen Daten des Inhabers zur Kenntnis zu nehmen. So werden z. B. in der sog. „Anrufliste" die 16 letzten nicht entgegengenommenen Anrufe des betreffenden Apparates gespeichert und können auf dem Display angezeigt werden. Dabei werden für jeden Anruf Datum und Uhrzeit angezeigt, bei internen Anrufen zudem die Nummer und der Name — bei ISDN-Anrufen aus dem öffentlichen Netz nur die Rufnummer — des Anrufers. Auch die vom Anschlußinhaber gespeicherten individuellen Kurzwahlziele (häufig benutzte Rufnummern) können so abgerufen werden. Ich habe empfohlen, die Standardapparate besser, z. B. mittels eines individuellen, durch den Nebenstelleninhaber zu vergebenden und änderbaren Zahlencodes zu sichern. Dies wurde zwischenzeitlich zugesagt.

e) Die Auswerterechner sind mit einer sog. *Hardcopy-Funktion* ausgestattet: Durch deren Aktivierung wird der jeweils angezeigte Bildschirminhalt ausgedruckt, der vom Bediener beliebig und unkontrolliert gestaltet werden kann. Diese Funktion birgt erhebliche Risiken (vgl. ausführlich 11. TB Nr. 24.4). Sie macht die Verwendung der Gesprächsdaten praktisch unkontrollierbar und ermöglicht die Manipulation der Ausdrucke. Da es sich um die Verarbeitung von besonders schützenswerten Personaldaten handelt, habe ich empfohlen, den Einsatz der Hardcopy-Funktion zu verhindern.

f) Zur *Paßwortgestaltung* an den Erfassungs- und Auswerterechnern wurde festgestellt, daß die benutzten Paßwörter grundsätzlich alle durch die Lieferfirma eingerichtet worden waren und durch die Nutzer selbst nicht geändert werden konnten.

Sie waren unzureichend, d. h. leicht erratbar, gestaltet und wurden teilweise sogar auf dem Bildschirm angezeigt. Auf meine Anregung hin wird das Verfahren jetzt dahingehend geändert, daß die Paßworte der Erfassungs- und Auswerterechner durch die Betreiber selbst vergeben und jederzeit geändert werden können.

g) Während der Kontrolle haben meine Mitarbeiter darauf hingewiesen, daß nicht mehr benötigte *Gesprächsdaten umgehend zu löschen*, d. h. unkenntlich zu machen sind. Dies betraf insbesondere die auf Disketten gespeicherten Daten. Sie wurden lediglich im nächsten Einsatzzyklus der Disketten, d. h. mitunter erst nach Monaten, durch neue Daten überschrieben. Ich habe empfohlen, sich mit der Lieferfirma in Verbindung zu setzen, um eine erforderliche physische Löschung technisch zu realisieren.

h) Der Nachweis der bei der Telefondatenverarbeitung im Erfassungs- und Auswerterechner eingesetzten Disketten entsprach nicht den Erfordernissen der *Datenträgerkontrolle* (vgl. Anlage zu § 9 Satz 1 BDSG, Nr. 2). Ich habe ein geregeltes Ausgabeverfahren — zentrale Vergabe der Disketten gegen Quittung — sowie eine möglichst unveränderbare Kennzeichnung der einzelnen Disketten angeregt.

Die Reaktion der Ministerien auf meine Forderungen, Hinweise und Empfehlungen war konstruktiv. Sie bezog sich auf die vorstehend genannten Punkte zum Thema Datensicherheit, aber auch auf die von den drei Ressorts jeweils unterschiedlich organisierten und praktizierten Verfahren der Telefondatenverarbeitung (s. hierzu auch 9.5).

Schon während der Kontrolle wurden in der einen oder anderen Frage Veränderungen im Sinne der Datensicherheit und des Datenschutzes vorgenommen. Den Stellungnahmen zu meinem Kontrollbericht konnte ich entnehmen, daß auch die nicht sofort lösbaren Probleme aufgegriffen und zwischenzeitlich datenschutzgerechte Lösungen erzielt worden sind. Von einer Beanstandung konnte ich deshalb nach § 25 Abs. 2 BDSG absehen.

21.12 Telefonate wurden auf Antrag des Nachbarn registriert

„Es kann der Frömmste nicht in Frieden bleiben, wenn es dem bösen Nachbarn nicht gefällt"! Ein gelegentlich benutztes Mittel zur Austragung eines Nachbarschaftsstreites, ist es, sich gegenseitig belästigender Telefonanrufe zu beschuldigen und mit dieser Behauptung von der Telekom eine Registrierung der nachbarlichen Telefonate mittels einer ZVE (s. o. 21.1) zu verlangen.

Solange keine anderen technischen Mittel zur Verfügung stehen, sind unzweifelhaft Fangschaltungen und auch ZVE-Schaltungen zur Abwehr bedrohender oder belästigender anonymer Anrufe erlaubt. Wichtig ist hierbei jedoch eine wirksame Sicherung gegen Mißbrauch durch die Verfahrensgestaltung. Das von der Telekom derzeit praktizierte Verfahren weist in dieser Hinsicht erhebliche Mängel auf.

So registrierte die Telekom aufgrund eines nachbarschaftlichen „Auftrages zur Feststellung ankommender Telefonverbindungen im Telefondienst" die Verbindungsdaten eines Bürgers. Als er von der Registrierung seiner Telefonate erfuhr, bat er mich um eine datenschutzrechtliche Überprüfung. Im Rahmen meiner Untersuchungen mußte ich feststellen, daß das zuständige Fernmeldeamt die Gründe für die Entscheidung über die ZVE-Schaltung nicht dokumentiert hatte. Insbesondere war nicht festgehalten worden, wie der Antragsteller *glaubhaft gemacht* hatte, daß bei seinem Anschluß anonyme bedrohende oder belästigende Anrufe angekommen waren — was aber rechtlich geboten war. Dies war auch insoweit erstaunlich, als in dem dafür vorgesehenen Antragsformular durchaus Raum für eine „Begründung des Auftrags (bei Belästigung z. B. auch Angaben über die Häufigkeit und Uhrzeit der Anrufe sowie Schwere der Belästigung" vorgesehen ist. Gleichwohl wurde gerade diese Spalte nicht ausgefüllt. Desweiteren war der Bürger nicht gemäß der Vorschrift des § 8 Abs. 2 Satz 1 TDSV anschließend über die Registrierung seiner Telefonate informiert worden.

Meine dahingehende förmliche Beanstandung wurde von der Deutschen Bundespost Telekom zunächst zurückgewiesen. Nach Auffassung der Telekom „kann eine ausdrückliche Regelung, wonach die Gründe, die die Behauptung glaubhaft machen, schriftlich vorgetragen und manifestiert werden müssen", nicht aus den Rechtsvorschriften entnommen werden. Hinsichtlich des Informationsrechtes des Betroffenen wurde darauf hingewiesen, daß die Vorschrift des § 8 Abs. 2 TDSV in der Praxis nicht umsetzbar sei und darüber hinaus verfassungsrechtliche Bedenken bestünden.

In dieser Angelegenheit wandte ich mich daher an das Bundesministerium für Post und Telekommunikation. Hierbei regte ich an, auf die Deutsche Bundespost Telekom dahingehend einzuwirken, daß die Regelungen des § 8 TDSV ordnungsgemäß umgesetzt werden. Das Bundesministerium für Post und Telekommunikation hat mir nunmehr mitgeteilt, es werde der Telekom empfehlen, „die Fernmeldeämter anzuweisen, künftig in jedem Falle schriftlich festzuhalten, welche Tatsachen vom Antragsteller vorgebracht wurden und welche Tatsachen für die Entscheidung zur Registrierung der Verbindungsdaten maßgebend gewesen sind." Hinsichtlich des Informationsrechtes des Betroffenen nach § 8 Abs. 2 TDSV hat das Bundesministerium für Post und Telekommunikation zugesagt, die angesprochene Problematik zu prüfen. Jedenfalls teilt das Ministerium meine Auffassung, daß verfassungsrechtliche Bedenken im vorliegenden Fall nicht durchgreifen.

22 Wissenschaft und Forschung — Forschungsvorhaben „Anonymisierung" —

Die Ergebnisse des Forschungsvorhabens der Universität Mannheim, über das ich in meinem 13. Tätigkeitsbericht (S. 60f.) ausführlich berichtet habe,

wurde in der Schriftenreihe des Statistischen Bundesamtes veröffentlicht. Anläßlich der Vorstellung des Ergebnisbandes habe ich an einem Workshop in Mannheim teilgenommen. Der Verlauf und das Ergebnis dieses Workshops haben gezeigt, daß ein sachbezogenes und für beide Seiten fruchtbares Gespräch zwischen Datenschutz und Wissenschaft stattfinden kann.

Die Ergebnisse des Forschungsvorhabens wurden außerdem im Arbeitskreis Statistik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder durch den Leiter der Forschungsgruppe vorgestellt. Auch die Landesbeauftragten für den Datenschutz haben anläßlich dieser Besprechung deutlich gemacht, daß die in meinem 13. Tätigkeitsbericht (S. 61) wiedergegebenen Empfehlungen für Maßnahmen bei der Übermittlung von Einzelangaben aus dem Mikrozensus datenschutzrechtlich akzeptabel sind.

23 Statistik

23.1 Europäische Gemeinschaft aktiviert ihre Statistik

Statistiken, die das Statistische Amt der Europäischen Gemeinschaft (SAEG, auch EUROSTAT genannt) aus den von den Statistischen Ämtern der Mitgliedstaaten gelieferten Daten erstellt, gewinnen immer größere Bedeutung. Allerdings hat die datenschutzrechtliche Entwicklung bei der EG mit dem Aufbau der europäischen Statistik keineswegs Schritt gehalten. So fehlt es auf Gemeinschaftsebene immer noch an einer unabhängigen Datenschutzkontrolle (s. unten 33.5).

Die Europäische Statistik wird noch weitgehend aus den nach dem nationalen Recht der Mitgliedstaaten erhobenen Statistiken gespeist. Die Europäische Gemeinschaft (EG) hat aber eine eigene administrative und legislative Kompetenz im Bereich der Statistik. Letztere ergibt sich zwar nicht unmittelbar aus dem EWG-Vertrag, wird aber als logischer Annex der im EWG-Vertrag definierten Ziele und Aufgaben anerkannt. Von ihrer Rechtsetzungsbefugnis im Bereich der Statistik hat die EG bisher nur zurückhaltend Gebrauch gemacht. Sie gibt diese Zurückhaltung jetzt aber offenbar auf. So wird beispielsweise die „Entschließung des Rates über die Durchführung eines Plans für prioritäre Maßnahmen im Bereich der statistischen Informationen: Statistisches Programm der EG 1989 bis 1992" durch einen „Beschluß des Rates über das EG-Rahmenprogramm für prioritäre Maßnahmen im Bereich der statistischen Information (1993 bis 1997)" abgelöst. Das Statistikprogramm soll durch einen Rahmenbeschluß des Rates gestützt werden, der dann durch Statistikverordnungen der EG für einzelne Bereiche ausgefüllt werden soll.

Die wesentliche rechtliche Grundlage für die EG-Statistik werden zwei Verordnungen über das Gemeinschaftliche Statistische System bilden. Die erste, eine Verordnung des EG-Rates, wird die Aufgaben und Grundprinzipien der Gemeinschaftsstatistik, die Organisation des gemeinschaftlichen statistischen Systems sowie die Rolle und Durchführung des gemeinschaftlichen statistischen Programms regeln. Mit der zweiten Verordnung wird die EG-Kommission die Aufgaben, Stellung und Organisation von EUROSTAT festlegen. Diese EG-Verordnungen sollen die technische, inhaltliche und methodische Ebene des europäischen Statistiksystems beschreiben. Darüber hinaus will die EG-Kommission erreichen, daß die nationalen statistischen Systeme auf den gleichen Grundprinzipien beruhen. Nach den Vorstellungen der EG-Kommission sollen die Verordnungen die nationalen Statistikgesetze ergänzen, soweit es um Gemeinschaftsstatistiken geht. Außerdem soll die Rolle von EUROSTAT definiert werden, insbesondere dessen Rechte und Pflichten gegenüber den Gemeinschaftsbehörden und die Beziehungen zu den nationalen Behörden sowie zu anderen Gemeinschaftsinstitutionen, wie dem Europäischen Währungsinstitut (künftig: Europäische Zentralbank), dem auch der Maastrichter Vertrag Kompetenzen und Unabhängigkeit im Statistischen Bereich zuspricht.

In diesem Zusammenhang begrüße ich ausdrücklich, daß sich sowohl die Bundesregierung als auch das Statistische Bundesamt bei der EG für die strikte Anwendung des Subsidiaritätsprinzips einsetzen. Ebenso unterstütze ich die Forderung, EUROSTAT unter dem Gesichtspunkt der Objektivität und Neutralität organisatorisch aus der Kommission herauszulösen und dieser Behörde den gleichen unabhängigen Status zu verleihen, wie er für die Europäische Umweltagentur und die Europäische Zentralbank vorgesehen ist, auch wenn dafür der EWG-Vertrag geändert werden muß. EUROSTAT selbst sieht es aus Budgetgründen zur Zeit leider als vorteilhafter an, Teil der EG-Kommission zu sein.

23.1.1 Statistikgeheimnis durch Entwurf einer EG-Unternehmensregisterverordnung gefährdet

Datenschutzrechtlich nicht akzeptabel ist der „Vorschlag für eine Verordnung (EWG) des Rates über die innergemeinschaftliche Koordinierung des Aufbaus von Unternehmensregistern für statistische Verwendungszwecke" (EG-Unternehmensregisterverordnung). Mit der Verordnung bezweckt die EG-Kommission, daß in allen Mitgliedstaaten nationale, aber mit den in den anderen Mitgliedstaaten zu errichtenden Unternehmensregistern kompatible Register geschaffen werden, um damit die Erstellung von konsistenten Gemeinschaftsstatistiken zu ermöglichen. Darüber hinaus sollen die Unternehmensregister auch der Kontrolle der von den Unternehmen zu liefernden Daten dienen. Aus diesem Grund sieht der Verordnungsvorschlag die Übermittlung statistischer Informationen, auch soweit sie von den nationalen Behörden als vertraulich eingestuft wurden, „an die Kommission" vor. In der EG-Übermittlungsverordnung von 1990 war demgegenüber noch EUROSTAT als Empfänger der vertraulichen statistischen Daten genannt. Die Begründung zu dem Verordnungsvorschlag, nach der die Verknüpfung der für statistische Zwecke erhobenen Daten mit anderen Daten des Verwaltungsvollzugs, u. a. mit Zolldateien, vorgesehen ist, läßt befürchten, daß für eine Statistik erhobene Daten von anderen Teilen der EG-Kommission für Zwecke der Wirtschaftsüberwachung genutzt werden

sollen. Dies wäre mit deutschem Recht nicht vereinbar. Abgesehen davon, daß das Statistikgeheimnis nicht mehr gewahrt wäre, würde hier gegen den vom Bundesverfassungsgericht hervorgehobenen Grundsatz der Trennung von Statistik und Verwaltung verstoßen. Die Bundesregierung teilt diese Bedenken.

Das federführende Bundesministerium für Wirtschaft habe ich gebeten, sich bei den Beratungen mit der EG-Kommission auch gegen die vorgesehene Erfassung aller Unternehmen zu verwenden, da die Erforderlichkeit dieser Totalerfassung weder dargelegt wurde noch ersichtlich ist. Nach dem Verordnungsvorschlag müßten alle Einzelkaufleute erfaßt werden, was bei der Adreßdatei im Rahmen der Statistik im Produzierenden Gewerbe nach § 13 Bundestatistikgesetz (BStatG) nicht der Fall ist (vgl. schon 9. TB S. 44).

Der Verordnungsvorschlag sieht ferner vor, eine Kopie des EG-Unternehmensregisters „zehn Jahre zu Analysezwecken" aufzubewahren. Es ist aber nicht ersichtlich, welcher Art diese Analysen sein sollen. Um das Recht des einzelnen auf informationelle Selbstbestimmung nicht zu verletzen, ist es erforderlich, daß Klarheit darüber besteht, zu welchem Zweck Angaben verlangt werden und welche Verknüpfungs- und Verwendungsregelungen bestehen. Dies gilt vor allem deshalb, weil die Daten des vorgesehenen Unternehmensregisters — anders als statistische Daten nach deutschem Recht — nicht anonymisiert werden.

Den Statistischen Ämtern soll auch erlaubt werden, auf alle in den Mitgliedstaaten bestehenden administrativen und gerichtlichten Dateien zuzugreifen, die für die Erstellung des Unternehmensregisters nützlich sind. Hiergegen habe ich erhebliche datenschutzrechtliche Bedenken geltend gemacht. Nach ausführlicher Diskussion hat bei der Anpassung des Bundesstatistikgesetzes an die verfassungsrechtlichen Vorgaben des Volkszählungsurteils der Gesetzgeber zwar in § 5 Abs. 5 BStatG festgelegt, daß für eine Bundesstatistik ohne eine weitere rechtliche Grundlage Daten aus allgemein zugänglichen Quellen (Bundesanzeiger, Geschäftsberichte, öffentliche Register wie z. B. das Handelsregister) entnommen werden können. Die vorgesehene Regelung soll darüber hinaus aber erlauben, für statistische Zwecke Daten auch aus nicht allgemein zugänglichen Quellen zu erheben. Ich vermag weder das erforderliche Allgemeininteresse noch einen aktuellen Bedarf für eine so weitreichende Durchbrechung des Grundsatzes von der gesetzlichen Anordnung einer Statistik zu erkennen. Deshalb habe ich die Bundesregierung aufgefordert, sich für die Streichung dieser Regelung einzusetzen.

23.2 Rechtslücke geschlossen — Schutz von Statistikdaten auch bei EG

Die Verordnung des Rates der EG vom 11. Juni 1990 über die Übermittlung von unter die Geheimhaltungspflicht fallenden Informationen an das Statistische Amt der Europäischen Gemeinschaft (EG-Übermittlungsverordnung) ließ für die Anwendung des jeweiligen nationalen Strafrechts auf Verletzungen des Statistikgeheimnisses durch das Personal der EG eine Lücke (13. TB S. 60). Sie wurde für Deutschland mittlerweile durch das SAEG-Übermittlungsschutzgesetz geschlossen. Danach stehen die Beamten und sonstigen Bediensteten von EUROSTAT bei der Anwendung von Vorschriften des Strafgesetzbuches den Amtsträgern nach § 11 Abs. 1 Nr. 2 StGB gleich. In einigen EG-Mitgliedstaaten wurde der bestehende Strafrechtsschutz als ausreichend angesehen. In anderen EG-Mitgliedstaaten wurden mittlerweile ebenfalls Strafvorschriften geschaffen oder sind in Vorbereitung.

23.3 Zwangsweise Erhebung von Geburtsgewicht und Körperlänge der Neugeborenen — Zum Bevölkerungsstatistikgesetz —

Die aus einer Volkszählung gewonnenen regionalen Einzelergebnisse, z. B. für Gemeinden, veralten ziemlich schnell. Sie werden deshalb mit Hilfe der beim Verwaltungsvollzug der Standesämter und Meldebehörden anfallenden Daten über Geburten, Umzüge, Todesfälle und Eheschließungen fortgeschrieben. Im Rahmen dieser Erhebungen wird aber nicht nur die Anzahl der Fälle festgestellt, man erfaßt vielmehr auch einige weitere Daten, wie z. B. bei Sterbefällen die Todesursache und bestimmte Krankenheiten, wenn sie bei der Untersuchung der Todesursache festgestellt worden sind. Es werden allerdings auch Angaben erhoben, die beim normalen Verwaltungsvollzug nicht anfallen. Hierzu gehören etwa die Daten über das Gewicht und die Länge der Neugeborenen bei der Geburtenstatistik.

Die Datenerhebung erfolgt z. Z. auf der Grundlage eines Gesetzes, das auch nach Ansicht des BMI nicht den verfassungsrechtlichen Anforderungen Rechnung trägt, die das Bundesverfassungsgericht im Volkszählungsurteil vom 15. Dezember 1983 aufgestellt hat. Wenn diese Statistiken weitergeführt werden sollen, muß schnell eine tragfähige Rechtsgrundlage geschaffen werden. Nachdem die früheren Entwürfe eines Bevölkerungsstatistikgesetzes, gegen die ich Bedenken geäußert habe (11. TB S. 47 und 12. TB S. 98), in der letzten Legislaturperiode nicht Gesetz werden konnten, hat das BMI einen neuen Referentenentwurf vorgelegt. Aber auch dieser Entwurf weist noch Mängel auf:

— *Erhebung von Geburtsgewicht und Körperlänge der Neugeborenen*

Datenschutzrechtlich bedenklich finde ich, daß der Entwurf Erhebungsmerkmale vorsieht, die bei den Verwaltungsstellen nur zum Zweck der Statistik erhoben werden. Hierzu gehören etwa bei der Geburtenstatistik die Angaben über das Körpergewicht und die Körperlänge des Neugeborenen. Gegenüber dem BMI habe ich zudem kritisiert, daß diese Angaben zur Zeit lediglich aufgrund einer Dienstanweisung von den Standesbeamten erhoben werden, obwohl sie für Verwaltungszwecke des Standesamtes nicht erforderlich sind und lediglich der Bevölkerungsstatistik dienen. Diese Praxis verstößt gegen das im Volkszäh-

lungsurteil ausdrücklich betonte Prinzip der Trennung von Statistik und Verwaltung.

In diesem Zusammenhang habe ich besonders bedauert, daß sich das BMI der im Volkszählungsurteil vom Bundesverfassungsgericht geforderten Methodendiskussion noch nicht mit der erforderlichen Intensität gestellt hat. Dies gilt z. B. für die Frage, ob nicht bei einigen Erhebungsmerkmalen statt auf Auskunftspflicht auf „Freiwilligkeit" der Angaben abgestellt werden sollte. So habe ich vorgeschlagen, daß die Angaben, die lediglich für Statistikzwecke benötigt werden, von den Betroffenen freiwillig zu erheben sind. Unter Hinweis darauf, daß diese Angaben unverzichtbar seien und nur bei Auskunftspflicht brauchbare Ergebnisse erzielt werden könnten, hat es das BMI allerdings abgelehnt, bestimmte Erhebungsmerkmale lediglich auf Freiwilligkeitsbasis erheben zu lassen.

— *Weiterleitung nicht ausreichend aggregierter Daten an Religionsgesellschaften*

Bedenken habe ich gegen die Regelung erhoben, wonach öffentlich-rechtliche Religionsgesellschaften tabellarisch zusammengefaßte Daten auch erhalten sollen, soweit einzelne Felder nur einen einzigen Fall enthalten. Eine solche Regelung durchbricht das Statistikgeheimnis, ohne daß ein überzeugender Grund dafür erkennbar ist. Der vom BMI vorgetragene Grund, die Religionsgesellschaften sollten in die Lage versetzt werden, ihre Mitgliederzahlen fortzuschreiben, überzeugt mich nicht. Auf örtlicher Ebene können die Kirchen ihren Mitgliederbestand mit Hilfe der Datenübermittlung durch die Meldebehörden fortschreiben. Auf überörtlicher Ebene spielen Tabelleneinsen erfahrungsgemäß keine Rolle.

23.4 Haushaltsmitglieder müssen monatliches Nettoeinkommen angeben — Zum Wohnungsstatistikgesetz —

Nachdem in der 11. Legislaturperiode der Entwurf eines Gebäude- und Wohnungsstichprobengesetzes (s. dazu 12. TB S. 55f.), nicht Gesetz wurde, hat der Deutsche Bundestag am 15. Januar 1993 das Gesetz über gebäude- und wohnungsstatistische Erhebungen (Wohnungsstatistikgesetz) verabschiedet. Das Bundesministerium für Raumordnung, Bauwesen und Städtebau hat mich bei der Vorbereitung frühzeitig beteiligt. Das Gesetz erlaubt eine flächendeckende Gebäude- und Wohnungszählung im Beitrittsgebiet sowie eine Stichprobenerhebung im gesamten Bundesgebiet mit einem Auswahlsatz von einem Prozent der Wohnungen.

Der Gesetzentwurf der Bundesregierung war aus meiner Sicht datenschutzrechtlich ausgewogen. Auf Forderung des Bundesrats wurde das Erhebungsmerkmal „Höhe des monatlichen Nettoeinkommens" aber nicht mehr nur für die Haushalte, sondern „für jedes Haushaltsmitglied" vorgesehen. Nach allen Erfahrungen ist für statistische Zwecke das Einkommen des eine Wohnung nutzenden Haushalts erforderlich, wobei unerheblich ist, wie sich das Einkommen auf die Haushaltsmitglieder verteilt. Es ist sogar methodisch zweifelhaft, das Einkommen einzelner Mitglieder dann in die Relation Haushaltseinkommen-Wohnungsmiete einzubeziehen, wenn es dem Haushalt zur Deckung der Ausgaben nicht zur Verfügung steht. Für den seltenen Fall, daß einzelne Mitglieder eines Haushaltes die genaue Höhe ihres Einkommens innerhalb des Haushalts nicht nennen möchten, bestand auch nach dem ursprünglichen Gesetzentwurf der Bundesregierung die Möglichkeit zur diskreten Erklärung gegenüber der erhebenden Stelle. Es mag sein, daß der Text des Gesetzentwurfs der Bundesregierung diese — aus Gründen der informationellen Selbstbestimmung eingeräumte — Wahlmöglichkeit nicht so deutlich machte, wie sie in der Begründung beschrieben wurde. Das andere Extrem, nämlich die Verankerung eines gesetzlichen Zwanges für alle Haushalte, die Höhe des monatlichen Nettoeinkommens für jedes Haushaltsmitglied anzugeben, ist aber die schlechtere Lösung. Denn in vielen Fällen ist die Angabe des Gesamteinkommens des Haushalts — und damit des aussagefähigeren Wertes — problemlos möglich.

Erfolgreich habe ich mich gegen Versuche der kommunalen Spitzenverbände gewandt, in das Wohnungsstatistikgesetz eine Regelung aufzunehmen, die die permanente Speicherung der Hilfsmerkmale „Straße und Hausnummer" in den statistischen Ämtern der Kommunen ermöglicht hätte. Eine Gebäude- und Adressendatei, die ständig aktualisiert wird, hätte dem Bundesstatistikgesetz (BStatG) widersprochen, das verlangt, Hilfsmerkmale sobald wie möglich zu löschen. Der Verwendungszweck dieser Daten wäre auch reichlich unklar gewesen. Zur Bildung kleinräumiger Gliederungen und entsprechender Auswertungen können die Gemeinden nach § 16 Abs. 5 BStatG im übrigen Einzelangaben erhalten, zu denen auch diese Hilfsmerkmale gehören. Jede Erweiterung in Richtung auf eine dauerhafte Einzeldatenspeicherung und -nutzung käme einer Verwendung für Verwaltungszwecke bedenklich nahe. Damit würde aber die vom Bundesverfassungsgericht im Volkszählungsurteil ausdrücklich geforderte Trennung von Statistik und Verwaltung aufgehoben.

23.5 Umweltstatistik wird geregelt

Das Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU) hat einen neuen Entwurf eines Gesetzes über Umweltstatistiken vorgelegt (zu den Vorentwürfen vgl. 11. TB S. 43 und 12. TB S. 98).

Er trägt dem Datenschutz insgesamt besser Rechnung. Der mir ursprünglich zugeleitete Entwurf enthielt jedoch wiederum eine Ermächtigung zur Weitergabe von Einzelangaben in Tabellen für Planungszwecke an das Umweltbundesamt. Dies wäre eine verfassungsrechtlich bedenkliche Durchbrechung des Grundsatzes der Trennung von Statistik und Verwaltung gewesen und hätte auch nicht mit § 16 Abs. 4 Bundesstatistikgesetz (BStatG) in Einklang gestanden. Wegen dieses Einwandes hat das BMU schließlich auf diese Regelung verzichtet.

Bedenken habe ich auch gegen eine Regelung geäußert, die es erlaubt hätte, mittels der Hilfsmerkmale die Angaben aus bestimmten Umweltstatistiken zu verknüpfen, ohne daß dies aus dem Wortlaut ohne weiteres erkennbar war. Das BMU hat auf meinen Hinweis zunächst lediglich die Begründung zum Gesetzesentwurf ergänzt und dort präzisiert, daß man an die Möglichkeit gedacht hat, solche nach § 13 a BStatG unter bestimmten Umständen erlaubte Verknüpfungen vorzunehmen (s. hierzu 12. TB S. 53 f.). Weil auch das BMJ hierfür eine normenklare bereichsspezifische Regelung in diesem Gesetz verlangte, will das BMU als Ergebnis der intensiven Diskussion nun einen entsprechenden Vorschlag für eine gesetzliche Klarstellung vorlegen.

23.6 Strafverfolgungsstatistik noch immer ohne Rechtsgrundlage

Über die Gestaltung der Personenstatistik in der Strafrechtspflege hat ein Expertengespräch im Bundesministerium der Justiz stattgefunden, an dem ich teilgenommen habe. Gegenstand dieses Expertengespräches war unter anderem die Möglichkeit der Verknüpfung der unterschiedlichen Statistiken auf dem Gebiet der Strafrechtspflege miteinander, angefangen von der Kriminalstatistik über die Statistiken, die im gerichtlichen Verfahren geführt werden, bis hin zur Strafverfolgungs- und zur Bewährungshilfestatistik. Zu meinem großen Bedauern wurde der Entwurf eines Strafverfolgungsstatistikgesetzes, über den ich in meinem 12. (S. 56f.) und meinem 13. (S. 59f.) Tätigkeitsbericht berichtet hatte, nicht mehr weiter verfolgt. Obwohl ich anläßlich dieses Expertengespräches erneut meine Bedenken dagegen erläutert habe, daß die Strafrechtspflegestatistiken weiterhin ohne die hierfür nach § 5 Bundesstatistikgesetz erforderliche gesetzliche Grundlage erhoben werden sollen, hat das Bundesministerium der Justiz bis heute keinen neuen Entwurf eines Strafverfolgungsstatistikgesetzes vorgelegt.

23.7 Einsatz von Laptops und fernmündliche Datenerhebungen bei der Durchführung von Statistiken

Das Statistische Bundesamt und die Statistischen Ämter der Länder beabsichtigen, künftig bei statistischen Erhebungen verstärkt computerunterstützte Befragungsmethoden anzuwenden. Es handelt sich zum einen um die Möglichkeit einer telefonischen Befragung durch die Statistischen Landesämter, bei der die telefonisch eingeholten Antworten bei den Statistischen Ämtern direkt in den Computer eingegeben werden, und zum anderen um den Einsatz von tragbaren Personalcomputern (Laptops).

Mit der Mehrzahl der Landesbeauftragten für den Datenschutz vertrete ich die Auffassung, daß eine telefonischen Befragung durch die Statistischen Landesämter datenschutzrechtlich nicht zu beanstanden ist, wenn die Initiative vom Bürger ausgeht. In einem solchen Fall kann von einer Einwilligung des betroffenen Bürgers in diese Befragungsmethode ausgegangen werden. Demgegenüber habe ich erhebliche Bedenken, wenn Statistische Ämter unaufgefordert Bürger anrufen, weil sich dann auch Unbefugte als Statistisches Amt ausgeben könnten. Auch halte ich eine fernmündliche Unterrichtung über die Auskunftspflicht und die Rechtsgrundlage der Erhebung in einem solchen Fall für nicht ausreichend, weil der Angerufene überrascht wird und deshalb zu Angaben verleitet werden kann, die er bei ruhiger Überlegung vielleicht so nicht machen würde. Ich unterstütze daher die Forderung von Landesbeauftragten für den Datenschutz, den Bürger im Vorfeld einer Befragung schriftlich darauf hinzuweisen, daß er sich auf diese Erhebungsmethode nicht einzulassen braucht.

Gegen den Einsatz von Laptops bei statistischen Erhebungen habe ich grundsätzlich keine datenschutzrechtlichen Bedenken. Allerdings bedarf es vor dem Einsatz dieser Erhebungsmethode einer Ergänzung des Bundesstatistikgesetzes. Die Statistikgesetze sehen nämlich als Intrumentarium zur Erhebung von Statistiken nur das eigenhändige Ausfüllen von Erhebungsvordrucken und die mündliche Beantwortung von Fragen eines Erhebungsbeauftragten (Interviewer, Zähler, Preisermittler) vor, der die Antworten anschließend in den Erhebungsbogen einträgt. Zu diesem gesetzlichen Instrumentarium gehören computerunterstützte Befragungsmethoden nicht. Ich habe deshalb dem Bundesministerium des Innern vorgeschlagen, bei der nächsten Novellierung eines Statistikgesetzes eine entsprechende Ergänzung des Bundesstatistikgesetzes vorzusehen, wenn diese Erhebungsmethode zukünftig genutzt werden soll.

24 Bundeskriminalamt

24.1 Gesetzgebungsstand

24.1.1 Neues BKA-Gesetz fehlt immer noch

Im Oktober 1992 ist mir eine überarbeitete Fassung des Referentenentwurfs zu einem Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKA-Gesetz) zugeleitet worden. Der Entwurf berücksichtigt nur zum Teil meine Vorschläge zu den beiden früheren Entwürfen (vgl. 11. TB S. 61 f., 13. TB S. 70). In den Ressortbesprechungen wurde noch nicht in allen Punkten Einvernehmen erzielt:

- Dies gilt u. a. für Art und Umfang der Verarbeitung und Nutzung personenbezogener Daten, die beim BKA im Rahmen seiner Zentralstellenfunktion zur Vorsorge für die Verfolgung künftiger Straftaten vorgehalten werden, insbesondere soweit es sich um die Daten Nicht-Beschuldigter und Nicht-Tatverdächtiger handelt.
- Ferner muß die datenschutzrechtliche Verantwortung der eingebenden Stelle für die im polizeilichen Informationssystem INPOL gespeicherten Daten im Entwurf eindeutig geregelt werden.

Es läßt sich derzeit leider noch nicht absehen, wann die Datenerhebung und Datenverarbeitung beim

Bundeskriminalamt eine gesetzliche Grundlage erhält, die den Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts aus dem Jahre 1983 entspricht. Sie ist dringend erforderlich.

24.1.2 Das Schengener Durchführungsübereinkommen bedarf der Ergänzung durch nationale Regelungen

Nach der Unterzeichnung des Übereinkommens vom 13. Juni 1990 betreffend den schrittweisen Abbau der Kontrolle an den gemeinsamen Grenzen (Schengener Durchführungsübereinkommen) durch Frankreich, die Beneluxstaaten und die Bundesrepublik Deutschland sind im Berichtszeitraum auch Italien, Portugal, Spanien und Griechenland dem Vertrag beigetreten (zu dessen Grundzügen vgl. 12. TB S. 95f.). Die entsprechenden Vertragsgesetze stehen kurz vor der Verabschiedung im Parlament.

Zu dem Gesetzentwurf der Bundesregierung mit dem das Schengener Durchführungsübereinkommen ratifiziert werden soll, habe ich mehrfach Stellung genommen und darauf hingewiesen, daß es für die Bereiche von

— Ausländerzentralregister

— Bundeskriminalamt

— Strafverfahren und

— Bundesgrenzschutz

bisher keine ausreichenden bereichsspezifischen Datenschutzregelungen gibt. Ich habe deshalb angeregt, bei der Beratung des Ratifizierungsgesetzes die Bundesregierung aufzufordern, alles zu unternehmen, damit möglichst bis zum Inkrafttreten des Durchführungsübereinkommens zumindest das Gesetzgebungsverfahren in den genannten Bereichen eingeleitet ist. Der gute Datenschutzstandard nach dem Schengener Durchführungsübereinkommen kann nur dann gewährleistet werden, wenn er im inländischen Recht seine Ergänzung findet. Entsprechende Beschlüsse der Bundesregierung liegen bisher leider nicht vor.

Aus Gründen der Transparenz habe ich ferner vorgeschlagen, die durch das Übereinkommen entstehenden neuen Aufgaben und Befugnisse des BKA nicht nur im Vertragsgesetz selbst — das lediglich im wenig verbreiteten Bundesgesetzblatt Teil II abgedruckt wird —, sondern im BKA-Gesetz niederzulegen. Auch halte ich eine gesetzliche Klarstellung für erforderlich, wonach der Zeitpunkt, zu dem die Datenübermittlung an ausländische Stellen zulässig ist, von der Bundesregierung im Bundesgesetzblatt bekanntzugeben ist.

Die im Schengener Durchführungsübereinkommen vorgesehene Einrichtung des Schengener Informationssystems (SIS), eines gemeinsamen automatisierten Fahndungssystems der Vertragsparteien, wird bereits praktisch vorbereitet. Um schon in der Vorbereitungsphase des SIS einen hohen Datenschutzstandard zu gewährleisten, haben die Vertragsstaaten am 19. Juni 1992 die Einsetzung einer vorläufigen gemeinsamen Datenschutz-Kontrollinstanz im Vorgriff auf die entsprechende Regelung des Durchführungsübereinkommens (Artikel 115) beschlossen, in der die unabhängigen Datenschutzbeauftragten der Vertragsstaaten vertreten sind. In seiner ersten Sitzung am 29. Juni 1992 hat dieses Gremium den Vorschlag abgelehnt, bereits in der Vorbereitungsphase, also noch vor Inkrafttreten der Datenschutzbestimmungen des Übereinkommens und ehe alle Vertragsparteien über den erforderlichen Datenschutzstandard verfügen, das automatisierte Schengener Informationssystem mit echten Daten aus nationalen Fahndungsbeständen zu testen. Die verantwortlichen Stellen wurden aufgefordert, erforderliche Tests mit fiktiven Daten durchzuführen. Dieser von der vorläufigen gemeinsamen Datenschutz-Kontrollinstanz einstimmig gefaßte Beschluß entsprach voll meinem zuvor schon gegenüber der Bundesregierung geäußerten Votum.

Der Datenschutzstandard des Schengener Durchführungsübereinkommens ist inzwischen schon zur Meßlatte für andere internationale Informationssysteme geworden. Um so wichtiger ist es, daß bis zum Inkrafttreten des Übereinkommens alle Vertragsparteien auch in ihrem nationalen Recht die nach dem Vertrag erforderlichen Vorkehrungen zum Schutz des Persönlichkeitsrechts getroffen haben.

24.2 Polizeiliche Datenverarbeitung in Europa

24.2.1 Europäisches Informationssystem — EIS —

In Ergänzung zum Schengener Informationssystem (SIS) (vgl. 24.1.2) soll ein Europäisches Informationssystem — EIS — errichtet werden, dem auch Dänemark, Irland sowie das Vereinigte Königreich, die dem Schengener Übereinkommen nicht beigetreten sind, angehören. Das EIS soll als einheitliches Informationssystem auf der Grundlage des Schengener Durchführungsübereinkommens errichtet werden. Nach derzeitigem Verhandlungsstand ist jedoch nicht an ein umfassendes Fahndungssystem wie bei Schengen gedacht. Vielmehr stellen die Mitgliedstaaten zunächst nur Daten von zur Einreiseverweigerung ausgeschriebenen Drittausländern für ein zentrales automatisiertes Verfahren zur Verfügung. Rechtsgrundlage für eine solche Sammlung sind Artikel 10 und 13 des noch nicht ratifizierten Übereinkommens über das Überschreiten der Außengrenzen. Die Überlegungen über die Konzeption dieses Informationssystems und das bei seinem Einsatz zu praktizierende Verfahren sind jedoch noch nicht abgeschlossen.

Mein vorrangiges Ziel ist, daß der Schengener Datenschutzstandard im Rahmen des EIS nicht unterschritten wird. Dies gilt insbesondere für Regelungen über die Rechte der Betroffenen sowie eine effektive und unabhängige Datenschutzkontrolle.

24.2.2 Polizeiliche Datenspeicherung europaweit; — EUROPOL, das Zentrale Europäische Kriminalpolizeiamt, kommt

Angesichts der drängenden Probleme, die sich aus dem internationalen illegalen Drogenhandel und der Organisierten Kriminalität ergeben, haben die

zuständigen Minister dem Europäischen Rat Vorschläge für die Einrichtung eines Zentralen Europäischen Kriminalpolizeiamtes (EUROPOL) unterbreitet; der Europäische Rat hat schließlich im Dezember 1991 in Maastricht die Schaffung von EUROPOL beschlossen. Im Vollausbau soll EUROPOL ein gemeinschaftsweites Informationssystem zur Bekämpfung des Terrorismus, des illegalen Drogenhandels und anderer schwerwiegender Formen der grenzüberschreitenden Kriminalität auf der Basis einer Konvention betreiben. Dabei geht es nicht nur um ein Fahndungssystem wie bei Schengen, sondern um ein aktives Recherchesystem, auf das die Strafverfolgungsbehörden der Mitgliedsstaaten im Rahmen der Verbrechensbekämpfung Zugriff haben sollen.

Ungeachtet der im einzelnen noch nicht festgelegten Zielsetzung von EUROPOL habe ich von Anfang an den Datenschutzstandard des Schengener Durchführungsübereinkommens als datenschutzrechtliche Leitlinie für EUROPOL gefordert. Dieser Maßstab ist auch geboten, weil EUROPOL im Endstadium eigenständige Datenverarbeitung — auch mit personenbezogenen Daten — betreiben wird. Alle Mitgliedstaaten müssen sich deshalb zur Einhaltung eines datenschutzrechtlichen Mindeststandards verpflichten. Da EUROPOL auch eigenständige Ermittlungsbefugnisse erhalten soll, sind auch klare Vorgaben über die Zulässigkeit der Datenverarbeitung und die Rechte des Betroffenen, vor allem das Recht auf Auskunft, erforderlich. Eine unabhängige internationale Datenschutz-Kontrollinstanz muß die Einhaltung des Datenschutzes bei EUROPOL kontrollieren können.

Obwohl die für EUROPOL erforderliche Konvention noch nicht vorliegt, sollte EUROPOL als Europäische Drogeneinheit (EDU) bereits am 1. Januar 1993 seine Aktivitäten zunächst bei der Bekämpfung des Drogenhandels vorläufig aufnehmen. Dazu ist es mangels Einigung über den Sitz der Einrichtung nicht gekommen. In der zunächst vorgesehenen vorläufigen Ausbauphase sollten die Vertragsstaaten nationale Verbindungsbeamte an EUROPOL entsenden, um dort auf der Basis des jeweiligen nationalen Rechts Informationsaustausch mit ihren Kollegen aus den anderen Staaten zu betreiben. Diese Verbindungsbeamten sollten Zugriff auf den Datenbestand ihrer entsendenden Behörde, nicht jedoch Direktzugang zu fremden Datenbeständen besitzen.

Auch wenn der Informationsaustausch unter den entsandten Beamten konventionell erfolgen soll, geht es auch in dieser ersten Phase von EUROPOL um mehr als nur eine Intensivierung der bisherigen grenzüberschreitenden polizeilichen Zusammenarbeit. Ich habe angeregt, daß die Rauschgift-Verbindungsbeamten nur Zugriff auf die rauschgiftrelevanten nationalen Datenbestände haben und daß die jeweiligen Datenterminals in der EDU-Zentrale nur den Verbindungsbeamten des jeweiligen Staates zugänglich sind. Schließlich müssen die von deutscher Seite entsandten Beamten bei der Verarbeitung personenbezogener Daten im Rahmen ihrer Aufgaben meiner uneingeschränkten Kontrollkompetenz unterliegen, auch wenn die EDU-Zentrale außerhalb des Geltungsbereichs des Grundgesetzes untergebracht sein sollte.

Ich konnte feststellen, daß meine Anregungen im Entwurf eines Regierungsübereinkommens zur vorläufigen Errichtung von EUROPOL weitgehend berücksichtigt worden sind. Bei der in Vorbereitung befindlichen Konvention über den Status von EUROPOL kommt es darauf an, den im Regierungsübereinkommen festgelegten Datenschutzstandard im Hinblick auf die eigenständige Datenverarbeitung bei dieser Zentrale angemessen fortzuentwickeln.

24.2.3 Polizeiliche Zusammenarbeit mit Staaten in Osteuropa

Die Grenzen zum früheren Ostblock sind auch für kriminelle Organisationen durchlässiger geworden. Die Bundesregierung hat deshalb mit einzelnen mittel- und osteuropäischen Regierungen Verwaltungsabkommen über die Zusammenarbeit bei der Bekämpfung der Organisierten Kriminalität geschlossen, die im wesentlichen standardisiert sind und spezielle datenschutzrechtliche Vorschriften enthalten. Am Entwurf des ersten derartigen Abkommens — mit der Regierung der ehemaligen Sowjetunion — war ich beteiligt, zu hieran orientierten Abkommen mit Ungarn, Polen und der damaligen Tschechoslowakei habe ich Stellung genommen.

Aufgrund meiner Anregungen wurde der in den Abkommen enthaltene spezielle Datenschutzartikel um Bestimmungen zu Erforderlichkeit und Verhältnismäßigkeit von Datenübermittlungen, zu Löschungsfristen und zur Datensicherung ergänzt. Weitergehende Anregungen, die von Datenübermittlungen betroffenen Personen zu konkretisieren, den Zusammenarbeitsbereich klarer zu bezeichnen und klare Übermittlungsschranken für mit besonderen Methoden oder Mitteln erhobene Daten aufzunehmen, sind nicht aufgegriffen worden. Da es sich insoweit jedoch um Sachprobleme handelt, die — anders als die Sicherung eines datenschutzrechtlichen Mindeststandards beim Empfänger — im eigenen, nationalen Bereich zu lösen sind, war es auch nicht zwingend, Regelungen hierüber in die Abkommen selbst aufzunehmen. Die Datenübermittlung durch deutsche Stellen bleibt an die einschlägigen gesetzlichen Regelungen gebunden. Ich empfehle, in Durchführungsbestimmungen auf die sich daraus ergebenden Schranken hinzuweisen. Die Durchführung der Abkommen auf deutscher Seite werde ich auch unter diesem Gesichtspunkt im Auge behalten.

Zum Jahresende 1992 hat das Bundesministerium des Innern mir einen Muster-Entwurf für künftige Regierungsabkommen „über die Zusammenarbeit bei der Bekämpfung der Organisierten Kriminalität sowie des Terrorismus und anderer schwerer Straftaten" zugeleitet, der aus den vorausgegangenen Abkommen entwickelt worden ist und für den deshalb die oben getroffenen Anmerkungen entsprechend gelten. Unter Würdigung dieser Erwägungen habe ich gegen den „Muster-Entwurf" keine datenschutzrechtlichen Bedenken geltend gemacht und lediglich angeregt, noch ergänzend zu berücksichtigen, daß es nach deutschem Recht der ersuchenden ausländischen Stelle obliegt, die Berechtigung ihres Informationsinteresses darzulegen.

24.3 Viel leistungsfähigeres Fingerabdruck-Identifizierungssystem AFIS eingerichtet

Seit etwa fünfzehn Jahren arbeiten Bund und Länder im Bereich der Daktyloskopie mit einem computergestützten Recherchiersystem zur Identifizierung von Fingerabdrücken. Es handelt sich um ein halbautomatisch betriebenes Bund-Länder-System. Hierbei werden die Fingerabdrücke von Asylbewerbern und von Straftätern, die Delikte von geringerer Bedeutung begangen haben oder begangen haben sollen, lediglich zum Zwecke der Identifizierung der Person automatisch in einem sogenannten Kurzsatz verformelt. Fingerabdrücke von anderen Straftätern werden von Daktyloskopen manuell zum Zwecke der Verwendung für eine etwaige Spurenrecherche am Tatort in einem sogenannten Langsatz verformelt, was einen Arbeitsaufwand von 60 bis 90 Minuten je Datensatz bedeutet. Aufgrund der Änderung des Asylverfahrensgesetzes, wonach jeder Asylbewerber erkennungsdienstlich zu behandeln ist, (1992 etwa 438 000 Asylbewerber) und des hohen Zeitaufwandes bei der Klassifizierung des Langsatzes hat das BKA am 3. Dezember 1992 die erste Ausbaustufe des neuen Systems AFIS (Automatisiertes Fingerabdruck-Identifizierungssystem) in Betrieb genommen. Es ermöglicht die automatisierte Verformelung *aller* Fingerabdrücke einer Person mit der Qualität des bisherigen Langsatzes in ca. 2 bis 3 Minuten. Die auf diese Art und Weise verformelten Fingerabdrücke können — wie der frühere Langsatz- auch zur Spurenrecherche verwendet werden. Das System AFIS wird auch in anderen europäischen Staaten verwendet. Derzeit werden beim Bundeskriminalamt die ab Dezember 1992 eingesandten Fingerabdruckblätter von Asylbewerbern in das neue System eingegeben. Gleichzeitig läuft das bisherige Verfahren für die Verformelung der Fingerabdrücke von Straftätern weiter; auch sie werden noch im Verlauf dieses Jahres für das neue System erfaßt. Der volle Wirkbetrieb von AFIS ist für Herbst 1993 vorgesehen.

Die nach dem alten Verfahren (Bund-Länder-System) verformelten Fingerabdrücke werden derzeit retrograd (rückwirkend) in den USA von einer Firma für die Speicherung in AFIS neu verformelt (ca. 1,6 Millionen Datensätze). Aus datenschutzrechtlicher Sicht handelt es sich hierbei um eine Auftragsdatenverarbeitung. Die Versendung der Fingerabdruckblätter an den Systemanbieter in den Vereinigten Staaten stellt eine Datenübermittlung an nicht-öffentliche Stellen außerhalb des Geltungsbereichs des Bundesdatenschutzgesetzes dar (§ 17 BDSG). Ich habe gegenüber dem Bundesministerium des Innern darauf hingewiesen, daß die Übermittlung der Fingerabdruckblätter an den Auftraggeber in den USA nur dann möglich ist, wenn dem § 11 BDSG entsprechende, das Persönlichkeitsrecht der Betroffenen sichernde Maßnahmen durch vertragliche Vereinbarung und organisatorische Vorkehrungen getroffen werden. Insoweit galt es insbesondere, datenschutzgerechte Regelungen für den Transport, die Aufbewahrung, die Zugriffsberechtigung, die Verarbeitung und die Nutzung der an den Auftragnehmer übermittelten Daten zu finden. Meine Vorstellungen wurden vom BMI weitgehend berücksichtigt, insbesondere wurde sichergestellt, daß die Vorschriften über das Datengeheimnis angewendet werden, daß ich die Datenverarbeitung vor Ort kontrollieren kann und daß bei Vertragsverletzung Vertragsstrafen fällig werden. So erfolgte z. B. der Transport in besonders gesicherten Behältnissen unter Einsatz von Sicherheitsunternehmen in beiden beteiligten Staaten. Verstöße gegen datenschutzrechtliche Bestimmungen habe ich bisher nicht festgestellt.

Ein Anschluß der Landeskriminalämter an AFIS soll im Laufe der Jahre 1993 und 1994 erfolgen.

24.4 INPOL-Sachfahndung — Übermittlung von Kfz-Sachfahndungsdaten an den HUK-Verband und an Kfz-Hersteller grundsätzlich zulässig —

In den vergangenen Jahren ist die Zahl der Diebstähle von Kraftfahrzeugen mit anschließender Verschiebung ins Ausland sprunghaft angestiegen. Zur effizienteren Bekämpfung dieser Delikte, die zum Teil Formen Organisierter Kriminalität angenommen haben, ist es aus Sicht des Bundeskriminalamts erforderlich, technische Daten über entwendete Fahrzeuge aus dem Kfz-Sachfahndungsbestand des INPOL-Systems beim BKA einigen Fahrzeugherstellern sowie dem HUK-Verband möglichst schnell zur Verfügung zu stellen. Die schon bisher mittels der Übersendung von Listen erfolgende Übermittlung der Daten soll zur Beschleunigung auf den Austausch automatisierter Datenträger umgestellt werden. Damit soll das Wiederauffinden gestohlener Fahrzeuge bei Kfz-Händlern und Vertragswerkstätten sowie im Ausland erleichtert werden. Die Daten über entwendete Fahrzeuge stammen überwiegend von den Strafverfolgungsbehörden der Länder und werden von diesen für den INPOL-Sachfahndungsbestand erfaßt.

Da über die betreffenden Kfz-Daten auch der Halter eines Fahrzeugs festgestellt werden kann, hat mich das Bundeskriminalamt um datenschutzrechtliche Beurteilung des Verfahrens gebeten.

Ungeachtet der nicht ganz eindeutig geklärten Frage, ob das Bundeskriminalamt oder Landespolizeibehörden für die Datenweitergabe zuständig sind, habe ich keine Bedenken gegen das geplante Verfahren erhoben. Maßgebend dafür war auch, daß die Länder ganz überwiegend mit der Datenweitergabe durch das BKA einverstanden waren. Es handelt sich um eine Datenübermittlung an nicht-öffentliche Stellen, wobei davon auszugehen ist, daß schutzwürdige Interessen der Betroffenen nicht entgegenstehen. Die Eigentümer haben mit ihrer Anzeige bei der Polizeibehörde oder der Verlustmeldung gegenüber ihrer Versicherung zum Ausdruck gebracht, daß sie mit den Maßnahmen zur Wiederbeschaffung des Fahrzeugs einverstanden sind. Ich habe jedoch darauf gedrungen, daß die nicht-öffentlichen Datenempfänger sich schriftlich zu einer strikt zweckgebundenen Nutzung der übermittelten Daten verpflichten. Schließlich ist dafür Sorge zu tragen, daß die übermittelten Daten aktuell gehalten werden. Auch aus Datenschutzsicht wäre es freilich noch wichtiger, den Diebstahl von

Kraftfahrzeugen — vor allem technisch — zu erschweren.

24.5 Neue Dateien — Geplante Datei „Gewalttäter Sport" (Hooligandatei)

Aufgrund einschlägiger Vorfälle beauftragte die Innenministerkonferenz (IMK) den AK II zu prüfen, ob und in welcher Form von den Polizeien des Bundes und der Länder Informationen über Personen, die wegen Gewalttägigkeiten im Zusammenhang mit sportlichen Veranstaltungen aufgefallen sind, zur Gefahrenabwehr und zur Verfolgung von Straftaten vorgehalten und übermittelt werden können. Im Jahre 1991 hat die Innenministerkonferenz dann auf Grund entsprechender Vorschläge des AK II beschlossen, eine Datei „Gewalttäter Sport" einzurichten. Nach dem Beschluß soll die sogenannte Hooligandatei als Verbunddatei beim Bundeskriminalamt geführt werden. Sie soll laut IMK einen erzieherischen und abschreckenden Effekt auf potentielle „Hooligans" haben. Zu diesem Zweck ist eine Speicherung personenbezogener Daten in der Datei vorgesehen bei Ermittlungsverfahren und Bußgeldbescheiden im Zusammenhang mit Krawallen, Stadionverboten, Ingewahrsamnahmen zur Gefahrenabwehr und im Falle des Mitführens von Waffen bei Sportveranstaltungen.

In Übereinstimmung mit den meisten Landesbeauftragten für den Datenschutz habe ich darauf hingewiesen, daß bei der Entscheidung über die Einrichtung einer solchen Datei und bei deren Ausgestaltung der Persönlichkeitsschutz berücksichtigt werden muß. Ich verkenne nicht, daß Gewalttätigkeiten im Zusammenhang mit Sportveranstaltungen ein großes Problem für die öffentliche Sicherheit und Ordnung darstellen. Allerdings muß eine neue Datei, die der Bewältigung dieses Problems dienen soll, dafür auch geeignet sein. Ich habe den Eindruck, daß bei den zuständigen Stellen bis heute kein klares Konzept für eine Bekämpfungsstrategie und über die Rolle, die eine neue Datei darin spielen soll, besteht. Das ist aber Voraussetzung für ein abschließendes Urteil, das zur Zeit noch nicht möglich ist.

24.6 Der Umgang mit Daten aus der Überwachung des Fernmeldeverkehrs muß präziser geregelt werden

Nachdem ein früherer Hessischer Innenminister Informationen öffentlich bekanntgegeben hatte, die das Bundeskriminalamt aufgrund einer gerichtlich angeordneten Maßnahme zur Überwachung des Fernmeldeverkehrs gewonnen hatte (s. 13. TB S. 70 f.) habe ich präzisere datenschutzrechtliche Regelungen gefordert. Es sollte sichergestellt werden, daß das Bundeskriminalamt mit Informationen, die durch Eingriffe in das Fernmeldegeheimnis erlangt worden waren, nach Sinn und Zweck der gesetzlichen Vorschriften umging. Das BMI hat mir im Berichtszeitraum einen entsprechenden Richtlinien-Entwurf zugeleitet. In den Beratungen habe ich erreicht, daß personenbezogene Daten aus Überwachungsmaßnahmen nach § 100 a StPO an Stellen außerhalb des BKA nur mit Zustimmung der zuständigen Staatsanwaltschaft weitergegeben werden dürfen. Nur wenn die zuständige Staatsanwaltschaft nicht erreichbar und die Übermittlung der Daten zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist, darf die Übermittlung auch ohne vorherige Zustimmung der Staatsanwaltschaft erfolgen. Die Staatsanwaltschaft ist aber unverzüglich hiervon zu unterrichten.

Leider sind diese Richtlinien noch nicht in Kraft getreten, da über die Verwertung von Zufallsfunden und auch zu einigen anderen Punkten noch kein Einvernehmen erzielt werden konnte. Die in § 100 a StPO vorgesehene Überwachung des Fernmeldeverkehrs stellt eine nach Artikel 10 Abs. 2 Satz 1 GG zulässige gesetzliche Beschränkung des Grundrechts der Unverletzlichkeit des Fernmeldegeheimnisses und des in Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG gewährleisteten allgemeinen Persönlichkeitsrechts dar. Es entspricht dem Wertgehalt dieses Grundrechts, daß sowohl die Überwachung des Fernmeldeverkehrs als auch die Verwertung angefallener Erkenntnisse nur bei besonders schwerwiegenden Straftaten zulässig sein dürfen. Nach § 100 b Abs. 5 StPO dürfen deshalb Zufallserkenntnisse zu Beweiszwecken nur für die Verfolgung von Katalogtaten im Sinne des § 100 a StPO, nicht aber für die Verfolgung anderer Taten verwertet werden. Streitig ist, ob eine mittelbare Verwertung dieser Zufallserkenntnisse in der Weise zulässig ist, daß aufgrund der erlangten Erkenntnisse Ermittlungen zu anderen Straftaten geführt und neue Beweismittel gewonnen werden dürfen.

Das BKA nimmt eine solche Befugnis in Anspruch und stützt sich dabei auf die Rechtsprechung des BGH aus der Zeit vor dem Erlaß des Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG).

Ich habe dies — in Übereinstimmung mit der überwiegenden Literatur — verneint, da eine Weiterverwendung der Daten zu Ermittlungszwecken das Persönlichkeitsrecht ebenso in gesetzlich nicht vorgesehener Weise beeinträchtigt wie eine Verwendung zu Beweiszwecken.

24.7 Aussonderungsprüffristen und Löschung gespeicherter Daten

In jüngster Zeit ist immer wieder der Vorwurf erhoben worden, die Aussonderungsprüffristen, wie sie in den einschlägigen Rechts- und Verwaltungsvorschriften für die Polizeien vorgesehen sind, behinderten die Aufklärung von Straftaten. Dies wurde jedoch — jedenfalls für den Bereich des Bundes — bisher nicht mit konkreten Fakten belegt. Ich glaube auch nicht, daß diese Attacken überhaupt begründet werden können: Die einschlägigen Vorschriften sehen nämlich keineswegs einen Löschungs-Automatismus vor; vielmehr bleibt die Speicherung über die vorgesehenen Regelfristen — im Grundfall ohnehin bereits 10 Jahre! — hinaus zulässig, wenn Tatsachen die Annahme recht-

fertigen, daß wegen Art und Ausführung der Tat, die der Betroffene begangen hat oder derer er verdächtigt war, die Gefahr der Wiederholung besteht oder die Speicherung der Daten aus anderen schwerwiegenden Gründen zur Aufgabenerfüllung weiterhin erforderlich ist. Die einschlägigen Fristen wurden unter Berücksichtigung polizeifachlicher Erfahrungen festgelegt: Liegen nach zehn Jahren immer noch keine neuen Erkenntnisse vor, würde die weitere Speicherung in der Regel unnütz Ressourcen zur Speicherung und Auswertung binden, weil so alte Spurenansätze regelmäßig keinen praktischen Aussagegehalt mehr besitzen, wenn sie zwischenzeitlich nicht in irgendeiner Weise aktualisiert oder konkretisiert werden konnten.

Im übrigen war und bin ich stets bereit, auch über die Richtigkeit von Aussonderungsprüffristen zu sprechen, wenn mir konkret dargelegt werden kann, daß und warum sie eine effektive Strafverfolgung behindern. So habe ich z. B. im Berichtszeitraum einer Fristverlängerung bei der Speicherung von Daten im Bereich von Delikten der organisierten und terroristischen Kriminalität (§§ 129, 129 a StGB) zugestimmt (s. 24.8.2).

Bei dieser Sachlage frage ich mich, was mit den fachlich nicht näher begründeten Attacken auf Prüf- und Speicherfristen, die dann noch mit einem generellen Angriff auf den Datenschutz im Polizeibereich verbunden werden, erreicht werden soll. Bisher konnte jedenfalls noch niemand belegen, daß Regelungen des Datenschutzes die Ursache sind, wenn den hohen Erwartungen unserer Bevölkerung an die polizeiliche Tätigkeit in Wahrheit aus anderen Gründen nicht genügt wird und oftmals aus schlicht faktischen — nicht rechtlichen — Umständen auch nicht genügt werden kann.

24.8 Zur Speicherungspraxis des Bundeskriminalamtes —

24.8.1 Das Bundeskriminalamt prüft die Löschungsmöglichkeit von Datenspeicherungen zu spät — Kontrolle beim Referat TB 22 des Bundeskriminalamtes —

Das Referat TB 22 ist im Bundeskriminalamt für die Datenerfassung und die Datenpflege des Aktennachweises zuständig. Wie ich bereits früher (12. TB S.74) dargelegt habe, wurde mit der Kontrolle des Referats im Jahre 1989 begonnen, die aber wegen personeller Engpässe erst im Berichtszeitraum mit Übersendung des Kontrollberichts an das BMI abgeschlossen werden konnte.

Die Kontrolle diente auch dem Zweck festzustellen, ob die datenschutzrechtlichen Mängel abgestellt waren, die bei vorangegangenen Kontrollen in den Jahren 1985 und 1987/88 festgestellt worden waren.

Im wesentlichen wurden die Dateien KAN (Kriminalaktennachweis), BKA-AN (BKA-Aktennachweis) und BKA-VNP (BKA-Vorgangsnachweis Personen) kontrolliert:

1. Die *Datei KAN* ist eine Verbunddatei, die Nachweise über die beim BKA und den Polizeien der Länder geführten Kriminalakten mit überregionaler Bedeutung enthält. Meine Kontrolle hat ergeben, daß die Rechtmäßigkeit der Speicherung in dieser Datei nicht immer lückenlos anhand der Akten nachvollzogen werden kann. Ohne hinreichenden Aktenrückhalt wird jedoch ein wesentlicher Zweck der Datei KAN, nämlich zu den Akten hinzuführen, nicht mehr ermöglicht. Zum Schutz des Persönlichkeitsrechts von Betroffenen muß daher stets auf einen hinreichenden Aktenrückhalt geachtet werden. Das BMI hat sich meiner Auffassung angeschlossen.

2. Die *Datei BKA-AN* führt das Bundeskriminalamt als Zentraldatei. Sie weist Kriminalakten nach, die beim BKA aufgrund des kriminalpolizeilichen Meldedienstes oder des Schriftverkehrs im Zusammenhang mit Ermittlungsverfahren, erkennungsdienstlichen Unterlagen und sonstigem polizeilich relevanten Schriftverkehr angelegt werden. Anderen Polizeibehörden wird aus der Datei nur auf konventionellem Wege Auskunft gegeben.

   Ich bemängelte an der Führung der Datei insbesondere die Festsetzung der Prüffristen für die Aussonderung der Akten, die auch für die Dauer der Speicherung in der Datei maßgeblich sind:

   — Bei der Eingabe der vorgesehenen Daten in das System wird per Programm ein Datum für die Prüfung der Aussonderung festgesetzt, das grundsätzlich dem Tag der ersten Einspeicherung plus 10 Jahre entspricht. Ich vertrete dagegen die Auffassung, daß für die Festlegung des Datums der Tag des die Speicherung veranlassenden Ereignisses (i. d. R. der Tat) maßgebend ist, wie es auch die Dateienrichtlinien des Bundeskriminalamtes vorsehen. Das BMI hat meiner Rechtsauffassung zugestimmt. Danach ist nun für den Beginn der Frist der Zeitpunkt der Tat maßgebend, soweit dieser nicht bekannt ist, der Tag der ed (erkennungsdienstlichen)-Behandlung oder der Tag der Absendung der Information über das Ereignis.

   — Die Datei BKA-AN weist vorwiegend Kriminalakten nach, die beim BKA aufgrund erkennungsdienstlicher Maßnahmen angelegt wurden. Die Polizeidienststellen der Länder übersenden Unterlagen über solche Maßnahmen dem BKA. Die Prüfung der Zulässigkeit der ed-Behandlung fällt damit in den Zuständigkeitsbereich der Länder. Es war aber nicht zu übersehen, daß es sich bei einer Vielzahl der aufgrund erkennungsdienstlicher Behandlung gespeicherten Fälle um Straftaten von geringer Bedeutung, z. B. Ladendiebstahl, handelte. Auch in diesen Fällen war stets die 10jährige Aussonderungsprüffrist gespeichert. Ich habe daher das BMI aufgefordert, die Regelspeicherfristen von drei Jahren, die die „Ergänzenden Regelungen für das BKA" (ergänzend zu den Richtlinien für die Führung kriminalpolizeili-

cher personenbezogener Sammlungen) bei Straftaten von geringer Bedeutung vorsehen, konsequent anzuwenden.

Damit die Aussonderungsprüffristen richtig festgesetzt werden können, muß aus den übersandten ed-Unterlagen allerdings ersichtlich sein, ob es sich um einen Fall von geringer Bedeutung handelt, was leider meist nicht der Fall ist. Um so bedauerlicher ist, daß es das BMI nicht für geboten hält, die Polizeibehörden der Länder zu bitten, entsprechende Angaben in die mit den Fingerabdruckblättern übersandten Personenbeschreibungsbögen aufzunehmen oder nachzumelden. Nach meinen Feststellungen enthält die Akte zumeist lediglich den Personenbeschreibungsbogen, so daß abzusehen ist, daß hier auch künftig die 10-Jahres-Frist undifferenziert zum Zuge kommen wird.

— Ein weiteres Problem betraf die Speicherung von personenbezogenen Daten im BKA-AN aufgrund von Erkenntnisanfragen in- und ausländischer Polizeibehörden. Es handelt sich hierbei um Anfragen, ob beim Bundeskriminalamt über eine bestimmte Person Unterlagen vorhanden sind. Ich habe festgestellt, daß über solche Anfragen auch ohne erkennbaren polizeilich relevanten Hintergrund Daten im BKA-AN gespeichert wurden, wie etwa die Anfrage einer ausländischen Polizeibehörde wegen der Vergabe einer Gaststättenlizenz an einen Deutschen. Solche Anfragen dürfen jedoch allenfalls in der Datei VNP (Vorgangsnachweis Personen) gespeichert werden. Das BMI macht dagegen geltend, *alle* Erkenntnisanfragen hätten einen polizeilichen Hintergrund, auch wenn keinerlei Angaben zum Hintergrund vorliegen. Daher sei die Erfassung der Erkenntnisanfragen im BKA-AN und nicht im VNP sachgerecht. Dies führt jedoch nach meinen Feststellungen zur Anlegung von Kriminalakten allein aufgrund von Erkenntnisanfragen, die dann für Zwecke der vorbeugenden Straftatenbekämpfung 10 Jahre vorgehalten werden.

  Erfreulicherweise hat das BKA inzwischen das Verfahren in eigener Verantwortung doch dahin geändert, daß derartige Erkenntnisanfragen nur noch im VNP, und zwar mit einer Laufzeit von maximal einem Jahr erfaßt werden. Sofern in diesem Zeitraum kein polizeilicher Hintergrund festgestellt werden kann, der eine Speicherung im BKA-AN rechtfertigt, werden die Daten gelöscht.

  Meiner Anregung, die festgestellten Mängel, insbesondere was Aussonderungsprüffristen betrifft, auch im vorhandenen Datenbestand zu beseitigen, will das BMI nicht nachkommen. Dies sei im Hinblick auf den Gesamtbestand von ca. 2 Mio. Datensätzen arbeitsorganisatorisch nicht durchführbar.

3. Die *Datei VNP* (Vorgangsnachweis Personen) ist eine Amtsdatei zum Nachweis von Vorgängen administrativer Art beim BKA. Darunter werden Vorgänge ohne polizei- oder strafrechtlichen Bezug verstanden. Darüber hinaus werden in der Datei der Schriftverkehr im Zusammenhang mit Unbedenklichkeitsbescheinigungen für gewerbsmäßige Veranstaltungen sowie bestimmte Spiele mit Gewinnmöglichkeiten und der Schriftverkehr im Zusammenhang mit Zulassungen von Ausnahmen nach § 37 Abs. 3 Waffengesetz nachgewiesen.

   Bei der Kontrolle habe ich festgestellt, daß in einigen Fällen in der Datei VNP Informationen gespeichert waren, die für die Aufgabenerfüllung des Bundeskriminalamtes nicht erforderlich waren. Beispielhaft seien erwähnt:

   — Eine Person war mit einer Aussonderungsprüffrist von drei Jahren gespeichert, weil die amerikanische Polizei das BKA um Erkenntnismitteilung gebeten hatte. Der Betroffene hatte einen Waffenschein in den USA beantragt. Das BKA hat der anfragenden Behörde mitgeteilt, es lägen keine Erkenntnisse vor.

   — Eine Person war für drei Jahre gespeichert, weil eine ausländische Polizeibehörde über sie angefragt hatte. Die Betroffene hatte sich für eine Tätigkeit zur Betreuung, Fürsorge oder Beaufsichtigung von Jugendlichen beworben. Das BKA hat auch hier mitgeteilt, es habe keine Erkenntnisse.

   Diese Informationen wurden inzwischen gelöscht.

   Die technische Ausgestaltung der Datei VNP ermöglicht eine Nutzung auch für Zwecke der Gefahrenabwehr und der vorbeugenden Verbrechensbekämpfung. Die Errichtungsanordnung sieht deshalb — datenschutzrechtlich korrekt — ausdrücklich eine Nutzung nur für rein administrative Zwecke vor. Diese Nutzungsbeschränkung sollte freilich auch durch geeignete Maßnahmen technisch und organisatorisch so abgesichert werden, daß unzuständige Organisationseinheiten nicht auf diese Datei zugreifen können. Die Auffassung des BMI, eine solche Abschottung sei rechtlich nicht geboten und aus praktischen Gründen nicht akzeptabel, entspricht aus meiner Sicht nicht den Anforderungen des § 9 BDSG und sollte nochmals überprüft werden.

24.8.2 Speicherungen in APIS besser — aber noch nicht problemlos

Die Arbeitsdatei PIOS Innere Sicherheit ist eine beim BKA geführte Verbunddatei, die Erkenntnisse über Staatsschutzdelikte und andere Straftaten — soweit sie politisch motiviert sind — enthält. Im August 1991 habe ich erneut (s. 12. TB S. 73, 11. TB S. 63) die Datenverarbeitung des BKA in dem System APIS unter folgenden Schwerpunkten kontrolliert:

Speicherung „anderer Straftaten"

Unter „anderen Straftaten" sind nach der Errichtungsanordnung zu APIS nicht die Staatsschutzdelikte im

eigentlichen Sinne zu verstehen, sondern andere Straftaten mit extremistischem Hintergrund. Bereits 1987 (s. 11. TB S. 63) hatte ich festgestellt, daß im Datenfeld „andere Straftaten" häufig auch Angaben zu Straftaten gespeichert wurden, die keine verfassungsfeindliche Zielsetzung hatten. Dieser Fehler war 1991 erfreulicherweise ausgeräumt. Anscheinend liegt dies aber in erster Linie daran, daß das BKA von sich aus in APIS nur noch solche Fälle speichert, in denen es selbst ermittelt. Ich habe allerdings den Eindruck, daß die Speicherpraxis der Länder in APIS nach wie vor an Mängeln leidet, wie ich sie früher beim Bundeskriminalamt festgestellt habe. Die Kontrolle der materiellen Zulässigkeit einer Speicherung durch ein Land liegt bei dem jeweils zuständigen Landesbeauftragten für den Datenschutz.

Speicherung „anderer Personen"

Nach der Errichtungsanordnung dürfen Daten „anderer Personen" in APIS gespeichert werden, wenn sie in Verbindung mit Beschuldigten oder verdächtigen Personen oder Organisationen stehen und zureichende tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß die Erfassung zur Aufklärung oder vorbeugenden Bekämpfung der in § 138 StGB genannten Straftaten (z. B. Mord, Totschlag, Landesverrat) oder einer Straftat nach § 129 StGB (Bildung einer kriminellen Vereinigung) erforderlich ist. Nach meinen Feststellungen handelt es sich bei den meisten gespeicherten „anderen Personen" um sog. Kontaktpersonen eines zur polizeilichen Beobachtung Ausgeschriebenen.

Zwei Fälle habe ich nach § 25 BDSG beanstandet, weil aus den mir zur Verfügung gestellten Unterlagen keine konkreten Hinweise auf eine Verbindung mit Beschuldigten oder verdächtigen Personen zu erkennen waren. Das BMI hat diese Beanstandungen zunächst zurückgewiesen, da nach weiteren Recherchen beim BKA tatsächliche Anhaltspunkte für eine solche Verbindung festgestellt worden seien. Nach einer nochmaligen Kontrolle dieser Vorgänge beim BKA habe ich erreicht, daß die Daten der beiden Betroffenen gelöscht wurden. Auch das BKA hielt nun die weitere Speicherung der Daten für nicht mehr erforderlich.

Nach wie vor halte ich den Begriff der „anderen Personen" in Nr. 4.3 der Errichtungsanordnung zu APIS für zu unbestimmt. Er trägt nach meiner Überzeugung dazu bei, daß zumindest zweifelhafte Fälle gespeichert werden. Ich habe vorgeschlagen, in Zukunft folgende Grundsätze zu beachten:

— Die Speicherung von Daten einer „anderen Person" ist zulässig, soweit dies zur Ermittlung gegen den Beschuldigten oder Verdächtigen erforderlich ist. Sie muß also stets im Zusammenhang mit einem Verfahren gegen einen Dritten stehen.

— Allein eine Verbindung der „anderen Person" zum Beschuldigten oder Verdächtigen reicht nicht aus. Zusätzlich sind tatsächliche Anhaltspunkte zu fordern, die die Annahme rechtfertigen, daß die Erfassung der Daten der „anderen Person" zur Aufklärung oder vorbeugenden Bekämpfung der in 138 StGB genannten Straftaten oder einer Straftat nach § 129 StGB erforderlich ist. Dies bringt die Regelung in Nr. 4.3 der Errichtungsanordnung auch zum Ausdruck; die Vorschrift wird aber nicht immer beachtet.

Ich habe auch die Frage problematisiert, ob der Begriff „andere Person" auch auf Anzeigeerstatter, Hinweisgeber und Zeugen angewandt wurde, denn gem. Nr. 4.2.10 der Dateienrichtlinien für das BKA dürfen Daten dieser Personen nur in zeitlich befristet geführten Spurendokumentationssystemen gespeichert werden. Auf meine Empfehlung, solche Fehlspeicherungen in der Errichtungsanordnung zu APIS klarer als bisher auszuschließen, ist das BMI leider nicht eingegangen.

Generell hält das BMI meine zuvor erwähnte Rechtsauffassung zur Zulässigkeit der Speicherung von Daten „anderer Personen" für zu eng. Ich bin mir darüber im Klaren, daß die Anwendung eines so allgemeinen Merkmals wie der „tatsächlichen Anhaltspunkte" in der Praxis nicht einfach ist. Trotzdem darf nicht davon abgesehen werden, es als Voraussetzung für eine Speicherung zu fordern. Eine zu großzügige Handhabung gerade dieses Merkmals führt mit hoher Wahrscheinlichkeit zur Speicherung Unverdächtiger.

Feststellung der Speicherfristen

In mehreren Fällen habe ich das Versäumnis beanstandet, die Erforderlichkeit der weiteren Speicherung über „andere Personen" zu prüfen, und das BMI aufgefordert sicherzustellen, daß nach Nr. 10.3 Satz 3 der Errichtungsanordnung nach jeweils einem Jahr seit der letzten Erfassung geprüft wird, ob die Daten weiter gespeichert bleiben müssen.

Die Festlegung der Aussonderungsprüffrist bezüglich Betroffener, die als Kontaktpersonen zu einer zur polizeilichen Beobachtung ausgeschriebenen Person gespeichert sind, wird uneinheitlich gehandhabt, ohne daß hierfür ein sachlicher Grund ersichtlich ist. Sie richtet sich in manchen Fällen danach, wie lange die polizeiliche Beobachtung noch läuft. In anderen Fällen wird eine Laufzeit von einem Jahr ab dem Datum, an dem ein Betroffener zusammen mit der ausgeschriebenen Person beobachtet wurde, festgelegt. Ich habe angeregt, eine gleichmäßige Handhabung sicherzustellen.

Das BMI hat dies bisher nicht aufgegriffen. Die Angelegenheit wird weiter mit dem Ziel einer gleichmäßigen Anwendung erörtert.

Da die Polizeibehörden des Bundes und der Länder der Auffassung sind, daß die bisher längste Speicherfrist von drei Jahren für Daten „anderer Personen" im Bereich der Delikte von §§ 129, 129a StGB nicht ausreicht, wurde diese auf 5 Jahre verlängert. Hiergegen habe ich keine Bedenken geltend gemacht, wenn — auch in diesen Fällen — die Speicherung jährlich überprüft wird.

Warnmeldungen

Das BKA gibt sog. Warnmeldungen über mögliche terroristische Anschläge heraus und speichert Daten potentieller Gefährder als „Beschuldigte/Gefährder" regelmäßig für drei Jahre in APIS. Die meisten Warnmeldungen stammen von den Nachrichtendiensten, einige von Fluggesellschaften. Die Meldungen sind zumeist sehr vage. Problematisch hierbei sind die Zulässigkeit der Speicherung, ihre Dauer und die Übermittlung der Gefährdungsmeldung an verschiedene Empfänger. Die Erfassung der potentiellen Gefährder unter dem Katalogbegriff „Beschuldigter" ist unzulässig, weil es regelmäßig an der Einleitung eines Ermittlungsverfahrens mangelt. Meiner Empfehlung, die Katalogbegriffe zur Kennzeichnung der potentiellen Gefährder durch treffendere Bezeichnungen zu ersetzen, wird das BMI nachkommen.

Auf meine Anregung hin wird das BMI auch prüfen, ob für Gefährder besondere Speicher- oder Prüffristen festgelegt werden können.

24.8.3 Speicherung von „Palästinenserdaten" in APIS

Aufgrund von Hinweisen auf eine bundesweite gezielte Überprüfung von Palästinensern während des Golfkrieges habe ich die Datenverarbeitung bei der Abteilung Staatsschutz des Bundeskriminalamtes kontrolliert. Ich habe festgestellt, daß das BKA die Daten von ca. 300 Personen als mögliche Gefährder in die Arbeitsdatei APIS eingestellt hatte.

Hintergrund der Überprüfung dieses Personenkreises und seiner Erfassung in APIS war die Drohung von irakischer Seite, europäische Staaten, insbesondere die Bundesrepublik Deutschland, wegen der Unterstützung der Alliierten im Golfkrieg mit Terrorakten zu überziehen. Bei den zu überprüfenden Personen hatten die Sicherheitsbehörden Anhaltspunkte für eine Zusammenarbeit mit irakischen Stellen oder pro-irakischen extremistischen Gruppierungen. Sie sollten deshalb zu möglichen Kontakten mit irakischen Stellen befragt werden.

Die Speicherung war zum damaligen Zeitpunkt gerechtfertigt. Eine fortdauernde Speicherung habe ich jedoch wegen Wegfalls der besonderen Gefährdungslage in Frage gestellt. Das BKA hat mir daraufhin mitgeteilt, daß es die Daten zum April 1992 gelöscht und die erstellten Unterlagen vernichtet hat, da es bezüglich des erfaßten Personenkreises keine tatsächlichen Anhaltspunkte für weitere Gefährdungen gebe.

24.9 Unschuldiger aufgrund fehlerhafter Datenspeicherung des BKA bei der Grenzkontrolle „auseinandergenommen"

Im Jahre 1991 hat sich ein Bürger erbost ein zweites Mal an mich gewandt, weil er bei der Rückreise von einer Dienstreise in die damalige CSFR im Zuge der grenzpolizeilichen Personenkontrolle erneut umfassend überprüft worden war. Wie der Petent erfahren hatte, war Anlaß für das genaue „Filzen", daß sich die Daten des Petenten als Alias-Personalie eines im INPOL-System ausgeschriebenen Straftäters im Grenzfahndungsbestand befanden. Erst nach langwierigen, sehr belastenden Untersuchungen hatte der Grenzbeamte festgestellt, daß der Petent mit dem Straftäter nicht identisch war.

Der Petent war besonders verärgert, weil sich ein ähnlicher Vorfall bereits 1980 bei einer Ausreise aus Berlin ereignet hatte. Nachdem der Petent sich seinerzeit an mich gewandt hatte, hatte ich festgestellt, daß dessen Daten deshalb im INPOL-System erfaßt waren, weil der gesuchte Straftäter vom Petenten als verloren gemeldete Ausweisdokumente benutzt hatte. Das BKA hatte seinerzeit die Daten des Petenten im INPOL-Personenfahndungsbestand gelöscht.

Wie kam es dann aber zur erneuten unrichtigen Speicherung der Daten des Petenten? Auf meine erneute Anfrage an das BKA stellte dieses fest, daß anläßlich einer erkennungsdienstlichen Behandlung des Straftäters dessen Kriminalakte durchgesehen wurde. Dabei wurden die in dieser Akte gespeicherten Daten des Petenten festgestellt und erneut als Alias-Daten des Straftäters im INPOL-System ausgeschrieben, was dazu führte, daß der Petent bei der grenzpolizeilichen Personenkontrolle, die Anlaß zu der Eingabe war, so richtig „auseinandergenommen" wurde. Um dem Petenten ähnliches in Zukunft zu ersparen, hat das BKA auf meine Anregung nicht nur den Alias-Datensatz des Petenten in INPOL, sondern auch die entsprechenden Daten in der Kriminalakte des Straftäters gelöscht.

Offen bleibt die Frage, ob sich ein ähnlicher Vorgang nicht bei anderen Bürgern, bei denen die Verhältnisse ähnlich liegen, erneut ereignen kann. Es müssen Vorkehrungen getroffen werden, um dies soweit irgend möglich zu vermeiden.

25 Bundesgrenzschutz

25.1 Dienstanweisung Amtshilfe/Grenze

Über die Probleme, die sich bei der Zusammenarbeit von Polizeibehörden, insbesondere auch des Bundesgrenzschutzes, mit den Nachrichtendiensten ergaben, habe ich bereits in meinem Ersten Tätigkeitsbericht (Seite 71) berichtet. Von zentraler Bedeutung sind hierbei das Gebot zur strikten organisatorischen Trennung von Polizei und Nachrichtendiensten (§ 2 Abs. 1 Satz 3 BVerfSchG) und der Grundsatz, daß den Nachrichtendiensten polizeiliche Befugnisse nicht zustehen (§ 8 Abs. 3 BVerfSchG). Daher ist die in den Gesetzen über die Nachrichtendienste getroffene Klarstellung so wichtig, daß diese die Polizei nicht im Wege der Amtshilfe um Maßnahmen ersuchen dürfen, zu denen sie selbst nicht befugt sind. Von ganz entscheidender Bedeutung für die Zusammenarbeit zwischen den Diensten und dem Bundesgrenzschutz ist auch der allgemeine, für jede Amtshilfe geltende Grundsatz, daß die ersuchte Behörde nicht Hilfe leisten darf, wenn sie dazu aus rechtlichen Gründen nicht in der Lage ist (§ 5 Abs. 2 Nr. 1 VwVerfG). Das heißt im Ergebnis, daß Aufgaben und Befugnisse einer

ersuchten Behörde durch ein Amtshilfeersuchen nicht erweitert werden.

Vor diesem Hintergrund durfte eigentlich erwartet werden, daß nach Inkrafttreten der Gesetze über die Nachrichtendienste keine grundsätzlichen Probleme im Bereich der Zusammenarbeit des Grenzschutzes mit Nachrichtendiensten mehr auftreten würden. Das ist leider nicht der Fall. In der im Berichtszeitraum erlassenen Dienstanweisung nach § 17 Abs. 2 Satz 2 des Bundesverfassungsschutzgesetzes, in der die Zulässigkeit besonderer Ersuchen der Nachrichtendienste an den Bundesgrenzschutz geregelt ist, heißt es an einer Stelle:

„Mit dem Ersuchen können folgende Informationen angefordert werden, die bei der Wahrnehmung grenzpolizeilicher Aufgaben bekannt werden *oder infolge des Ersuchens erhoben werden dürfen:*"

Damit wird den die Dienstanweisung ausführenden Bediensteten der Nachrichtendienste suggeriert, es dürfe auch um die Übermittlung erst noch zu erhebender personenbezogener Daten ersucht werden, die nicht bei der Wahrnehmung grenzpolizeilicher Aufgaben bekannt werden. Und bei den Beamten des BGS wird der Eindruck erweckt, sie dürften personenbezogene Daten ohne Rücksicht auf das für sie geltende Recht nur deshalb erheben, weil ein Nachrichtendienst um deren Übermittlung ersucht hat. Die Gesetze über die Nachrichtendienste sowie die Grundsätze für die Amtshilfe stehen dem aber klar und eindeutig entgegen.

Das Bundesministerium des Innern, dem ich diese Auffassung mitgeteilt habe, hat erwidert, die Dienstanweisung könne nicht gegen das Gesetz — über dessen Auslegung offenbar Einvernehmen mit mir bestehe — ausgelegt werden. Ob dieses Einvernehmen wirklich besteht, scheint zweifelhaft, denn in dem mir kurz vor Redaktionsschluß zugegangenen Entwurf eines BGS-Gesetzes soll jetzt offenbar die bisher noch fehlende Rechtsgrundlage für die Erhebung von personenbezogenen Daten allein auf Grund von Amtshilfeersuchen geschaffen werden. Einer solchen Regelung widerspreche ich, weil der BGS damit zu einem Anhängsel der Nachrichtendienste würde. Ich halte es außerdem für erforderlich, die zumindest höchst mißverständliche (nach ihrem Wortlaut rechtswidrige) oben zitierte Regelung in der Dienstanweisung nach § 17 Abs. 2 BVerfSchG so schnell wie möglich mit der Rechtslage in Einklang zu bringen. Das hat mir das BMI bisher leider nicht zugesichert.

25.2 Arbeitnehmer verliert Arbeitsplatz durch zweifelhafte Sicherheitsüberprüfung

Durch eine Eingabe erfuhr ich, daß der Bundesgrenzschutz einem Arbeitnehmer, der für einen Handwerksbetrieb Arbeiten in einer Liegenschaft des BGS durchführen sollte, den Zugang zu diesen Liegenschaften wegen angeblicher Eintragungen im Bundeszentralregister versagt hatte. Daraufhin hatte der Arbeitgeber das Arbeitsverhältnis des Petenten gekündigt.

Das Bundesministerium des Innern hat auf meine Nachfragen angegeben, die über den Petenten beim Bundeszentralregister eingeholte Auskunft habe zehn bis zwölf Verurteilungen des Betroffenen ausgewiesen, die nach Art und Schwere den Einsatz in der BGS-Unterkunft aus allgemeinen Sicherheitsgründen nicht vertretbar erscheinen ließen. Da der Petent eine solche Zahl von Verurteilungen mit Entschiedenheit bestritt, habe ich mich selbst mit dem Bundeszentralregister in Verbindung gesetzt. Dabei ergab sich, daß lediglich eine Verurteilung des Petenten im Bundeszentralregister eingetragen war. Gleichwohl blieb das Bundesministerium des Innern bei seiner Darstellung. Obwohl diese aufgrund meiner Feststellungen beim Bundeszentralregister recht unwahrscheinlich ist, konnte ich mit den mir zur Verfügung stehenden Mitteln leider nicht mehr ohne jeden Zweifel feststellen, ob wirklich eine Auskunft des vom Bundesministerium des Innern behaupteten Inhalts gegeben worden war. Der Bundesgrenzschutz vernichtet nämlich in der Regel unmittelbar nach Abschluß der Bearbeitung die Auskünfte aus dem Bundeszentralregister. Dies soll auch im vorliegenden Fall geschehen sein. Deshalb konnte ich dem Petenten im Ergebnis leider nicht helfen.

Ich habe den Fall zum Anlaß genommen, die Art und Weise des vom Bundesgrenzschutz durchgeführten Sicherheitsüberprüfungsverfahrens zu problematisieren. Insbesondere habe ich kritisiert, daß das Bundesministerium des Innern für die nachgeordneten Dienststellen des Bundesgrenzschutzes die nur ihm gestattete unbeschränkte Auskunft nach § 41 BZRG aus dem Bundeszentralregister einholt. Darin kann eine Umgehung des Bundeszentralregistergesetzes gesehen werden, das ganz bewußt die Einholung einer unbeschränkten Auskunft nur den obersten Bundesbehörden für die Erfüllung ihrer Aufgaben gestattet.

Das Bundesministerium des Innern wird in Zukunft in vergleichbaren Fällen unbeschränkte Auskünfte aus dem Bundeszentralregister nicht mehr einholen. Solche sind auch nicht erforderlich, weil ein polizeiliches Führungszeugnis, u. U. ergänzt durch eine Polizeiauskunft, für den verfolgten Zweck ausreicht.

25.3 Kommen automatisierte Personenkontrollen an den Grenzen?

Wenn demnächst das Schengener-Durchführungs-Übereinkommen (s. o. 24.1.2) in Kraft tritt, wird sich ein EG-Bürger bei der Einreise aus Drittstaaten einer genauen Kontrolle zumindest seiner Identität zu unterziehen haben. Das Bundesministerium des Innern ist nämlich der Ansicht, Artikel 6 des vorgenannten Vertrages schreibe eine erheblich intensivere Personenkontrolle an den Außengrenzen vor als sie bisher üblich war. Es befürchtet deshalb, daß infolge dieser Einreisekontrollen — besonders auf Flughäfen — lange Wartezeiten für die Betroffenen entstehen. Um dem entgegenzuwirken, plant das Bundesministerium des Innern den Aufbau einer teilweise automatisierten Grenzkontrolle. Nach den bisher entwickelten Vorstellungen kann an diesem

Verfahren teilnehmen, wer zuvor — auf freiwilliger Basis — die in seinem Grenzdokument enthaltenen Personenangaben sowie bestimmte biometrische Daten (Fingerabdrücke oder Meßdaten über die Hände, wie z. B. Länge der Hände und der Finger) erfassen und speichern ließ. Sobald dies geschehen ist, soll der Betroffene berechtigt sein, besondere zur Personenkontrolle (z. B. auf Flughäfen) aufgestellte automatisierte Vorrichtungen zu passieren um damit etwaige Warteschlangen bei der Abfertigung zu vermeiden.

Das Verfahren soll nach Vorstellung des BMI im einzelnen wie folgt durchgeführt werden:

Zunächst muß der Reisende beim Bundesgrenzschutz, z. B. auf einem Flughafen, einen schriftlichen Antrag auf Teilnahme an diesem Verfahren stellen. Hierfür hat er sich mit einem maschinenlesbaren Personalausweis oder Reisepaß auszuweisen und die genannten biometrischen Daten zur Verfügung zu stellen. Seine Identifikationsdaten aus dem Personalausweis oder Paß (z. B. Name, Vorname, Geburtsdatum, Geburtsort, Wohnort, Paßnummer/Personalausweisnummer) und seine biometrischen Daten werden dann in einer speziellen Datei gespeichert.

Bei der Grenzkontrolle werden zunächst die personenbezogenen Daten aus dem Reisedokument maschinell gelesen und mit den aus dem Antragsverfahren gespeicherten Informationen abgeglichen. Dabei erfolgt gleichzeitig immer eine fahndungsmäßige Überprüfung. Danach wird die eigentliche Identität des Betroffenen durch Vergleich seiner aktuellen biometrischen Daten mit den für diese Person im Antragsverfahren zur Verfügung gestellten Daten geprüft. Stimmen die Daten überein und ist der Betroffene nicht fahndungsmäßig ausgeschrieben, kann er ohne weiteres die Grenzkontrolle passieren.

Das Verfahren soll demnächst auf dem Frankfurter Flughafen in einem Großversuch getestet werden, wobei zwei unterschiedliche biometrische Identifikationsverfahren eingesetzt werden, nämlich Identifizierung mit Hilfe der Handgeometrie und mit Hilfe von Fingerabdrücken.

Ich werde den Umgang mit personenbezogenen Daten bei Durchführung dieses Versuchs kontrollieren und besonderen Wert darauf legen, daß die Rechte der Teilnehmer unter datenschutzrechtlichen Aspekten gewahrt werden. Insbesondere muß sichergestellt sein, daß die während des Feldversuchs anfallenden personenbezogenen Daten nur für die Personenkontrolle genutzt und nach Beendigung des Versuchs — auf Wunsch des Betroffenen auch früher — gelöscht werden. Auch muß geprüft werden, ob die Freiwilligkeit der Teilnahme an den Verfahren wirklich echt ist und sich nicht aus der „Drohung" mit der Einweisung in lange Warteschlangen vor der Personenkontrolle ein faktischer Zwang zur Teilnahme an dem „freiwilligen" Verfahren ergibt. Nach Durchführung des Versuchs werde ich ihn abschließend bewerten.

Ich habe angeregt, die parlamentarischen Gremien über den geplanten Feldversuch zu unterrichten, weil dieser den zumindest teilweisen Einstieg in eine völlig neue Kontrollpaxis zum Ziel hat.

26 Zoll- und Außenwirtschaftskontrolle

26.1 Telefonüberwachung bei Außenwirtschaftskontrolle eingeführt

Durch das Gesetz zur Änderung des Außenwirtschaftsgesetzes, des Strafgesetzbuches und anderer Gesetze vom 28. Februar 1992 hat das Zollkriminalamt (ZKA) Befugnisse zur Überwachung des Brief-, Post- und Fernmeldeverkehrs erhalten. Über diese zur Kontrolle des Außenwirtschaftsverkehrs vorgesehene Beschränkung des Grundrechts aus Artikel 10 des Grundgesetzes habe ich bereits berichtet (13. TB S. 71f). Der damalige Dissens zwischen Bundestag und Bundesrat hat die Bundesregierung veranlaßt, den Gesetzentwurf in einer so veränderten Form erneut einzubringen, daß er der Zustimmung des Bundesrats nicht mehr bedurfte.

Bei einer so tief in das Persönlichkeitsrecht eingreifenden Form der Datenerhebung, wie sie die Überwachung des Brief-, Post- und Fernmeldeverkehrs darstellt, ist eine strenge Zweckbindung der dabei erlangten Informationen von besonderer Bedeutung; für andere Zwecke als die mit der Datenerhebung verfolgten dürfen die Erkenntnisse nur in sehr engen und klar definierten Grenzen verwendet werden. Im ursprünglichen Gesetzentwurf war dementsprechend auch eine umfassend zu beachtende enge Zweckbindung vorgesehen. Der neue Regierungsentwurf sah demgegenüber, weil er eine Zustimmungsbedürftigkeit des Gesetzes durch den Bundesrat unter allen Umständen vermeiden wollte, eine Zweckbindung nur noch für die Verwendung der Daten beim Zollkriminalamt vor. Aufgrund meiner Bemühungen ist im Gesetz wenigstens die Verwendung der Daten bei sämtlichen Stellen des Bundes der Zweckbindung unterworfen worden. Dies bleibt jedoch unzulänglich.

Die Bundesregierung vertritt die Auffassung, der Bund sei von Verfassungs wegen nicht gehalten, zum Schutze des Persönlichkeitsrechts auch für die Verwendung der Daten im Landesbereich angemessene Zweckbindungen zu treffen; dies könne den Ländern überlassen werden. Ich teile diese Auffassung deshalb nicht, weil Stellen der Länder hier erst infolge der Übermittlung einer Bundesstelle, des ZKA, Kenntnis von den bei der Brief- und Telefonüberwachung erlangten Informationen erhalten. Wenn es aber der Bund ist, der durch die Weitergabe besonders schützenswerter Daten Gefahren für das Persönlichkeitsrecht schafft, dann trifft ihn aufgrund des Schutzauftrags des Grundgesetzes auch die Pflicht, die notwendigen, ihm möglichen Schutzvorkehrungen zu treffen. In diesem Sinne hat auch das Bundesverfassungsgericht entschieden, daß Grundrechtseingriffe nur zulässig sind, wenn der Gesetzgeber zugleich organisatorische und verfahrensmäßige Vorkehrungen trifft, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken (BVerfGE 65, 1 Leitsatz 2).

Die durch die Änderung des Außenwirtschaftsgesetzes eingeführten Möglichkeiten zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses gelten entsprechend meiner Anregung nur befristet; sie

treten Ende 1994 außer Kraft. Dann wird zu prüfen sein, ob ein überwiegendes Interesse der Allgemeinheit an den weitgehenden Grundrechtsbeschränkungen noch besteht und ob damit tatsächlich belegbare Aufklärungserfolge erreicht werden können. Die Sachverständigenanhörung während des Gesetzgebungsverfahrens hat meine insoweit bestehende Skepsis eher verstärkt.

26.2 Zollkriminalamt als Bundesoberbehörde geschaffen — aber ohne bereichsspezifischen Datenschutz

Auf Gesetzgebungsvorhaben zur Regelung des Umgangs mit personenbezogenen Daten beim früheren Zollkriminalinstitut (ZKI) habe ich bereits hingewiesen (13. TB S. 71). Zwischenzeitlich ist das Finanzverwaltungsgesetz — FVG — geändert worden (BGBl.1992 I S. 1222), um dem früheren Zollkriminalinstitut den Status einer Bundesoberbehörde — unter der Bezeichnung Zollkriminalamt (ZKA) — zu verleihen. Die bisherigen Regelungen zum ZKI sind dabei im wesentlichen übernommen worden. Die Absicht, bereits im Rahmen dieses Änderungsgesetzes auch den Datenschutz zu regeln, ist im Laufe des Gesetzgebungsverfahrens aufgegeben worden. Zwar wurde seinerzeit anerkannt, daß die gesetzlichen Regelungen der neuen Funktion der Behörde als Zentralstelle und ihren sprunghaft gewachsenen Aufgaben nicht mehr gerecht werden, insoweit also dringender Regelungsbedarf besteht. Andererseits wurde eingewandt, wegen der notwendigen und sicher zeitaufwendigen Abstimmung mit teilweise sich überschneidenden Regelungen in anderen Gesetzgebungsvorhaben, insbesondere im Strafverfahrensänderungsgesetz und im Entwurf eines neuen BKA-Gesetzes, sei ein Vorhaben, das auch den Datenschutz beim ZKA bereichsspezifisch regelt, nicht kurzfristig zur Gesetzesreife zu bringen. Die Datenschutzregelungen wurden deshalb zu meinem Bedauern vertagt.

Im Finanzverwaltungsgesetz sind dann einige von mir vorgebrachte Anregungen berücksichtigt worden, wie etwa die Bindung des Empfängers an den Übermittlungszweck. Vorrangig ist aber jetzt die Aufgabe, umfassende bereichsspezifische Datenschutzregelungen für das ZKA zu treffen. Noch so berechtigte Hinweise auf andere Gesetzgebungsverfahren dürfen im Ergebnis nicht zur Dauerblockade eines als notwendig erkannten Gesetzes führen. Im Entwurf des FVG-Änderungsgesetzes hatte die Bundesregierung noch angekündigt, die bereichsspezifischen Datenschutzregelungen „voraussichtlich bis zum Ende des Jahres 1991 einzubringen". Dies ist bis heute aber nicht geschehen. Ich fordere nachdrücklich, die vom Bundesverfassungsgericht zum Schutz des Persönlichkeitsrechts aufgestellten Grundsätze ernst zu nehmen. Seit dem Volkszählungsurteil sind bald zehn Jahre vergangen. Da ist es kaum verständlich, wenn eine intensive Datenverarbeitungspraxis trotz klarer rechtsstaatlicher Mängel nur unter Berufung auf einen „Übergangsbonus" aufrechterhalten werden kann, ja sogar noch ausgebaut wird. Dies gilt besonders im Bereich von Behörden, die an Strafverfahren mitwirken und für Ämter mit Zentralstellenfunktion — wie das ZKA —, bei denen empfindliche personenbezogene Informationen in großem Umfang gesammelt, ausgewertet und weitergegeben werden. Erschwerend kommen beim ZKA die tief in Bürgerrechte eingreifende Ausdehnung der Überwachung im Post- und Fernmeldeverkehr, die enge Einbindung dieses Amtes in das normale Verwaltungsverfahren der Außenwirtschaftskontrolle (12. TB S. 83) und die Vorfeldüberwachung hinzu.

Der vom BMF inzwischen übersandte Arbeitsentwurf für ein Gesetz über das Zollkriminalamt trägt dem Schutz des Persönlichkeitsrechts in wesentlichen Fragen noch nicht hinreichend Rechnung. Die Eingriffsbefugnisse des ZKA sollten nach dessen verschiedenen Aufgaben sachgerecht abgestuft werden. Zudem sind technische und organisatorische Sicherungsmaßnahmen vorzusehen. Auch über die Voraussetzungen zur Einrichtung von automatisierten Abrufverfahren und die Berechtigung zur Teilnahme am Zollinformationssystem bedarf es klarerer Regelungen, auch mit Blick auf die gebotene organisatorische Trennung von Polizeibehörden und Nachrichtendiensten, wie z. B. den BND. Bei der Führung zollkriminalpolizeilicher personenbezogener Sammlungen ist deutlich nach verschiedenen Personenkreisen (Beschuldigte/Zeugen/Minderjährige usw.) zu differenzieren. Schließlich ist — ebenso wie im Strafverfahrensrecht und im neuen BKA-Gesetz — die Speicherung von Daten zur Vorsorge für die künftige Strafverfolgung angemessen zu regeln.

Gerade wegen der noch bestehenden deutlichen Mängel des Arbeitsentwurfs ist es notwendig, die Arbeit am Gesetzentwurf zu intensivieren.

26.3 Gemeinsames Zollinformationssystem der EG-Mitgliedstaaten — CIS (Customs Information System) — kommt

Zur Verwirklichung des Europäischen Binnenmarktes sind am 1. Januar 1993 die Zollkontrollen an den Binnengrenzen der Mitgliedstaaten weggefallen. Der Europäische Rat hat bereits 1989 auf Rhodos beschlossen, daß Ausgleichsmaßnahmen erarbeitet werden müssen, um den Wegfall der Kontrollen an den Binnengrenzen zu kompensieren. Jeder Mitgliedstaat hat deshalb einen Koordinator bestellt, der für die Erarbeitung und Umsetzung der Ausgleichsmaßnahmen auf nationaler Ebene zuständig ist. Betroffen davon sind insbesondere die Bereiche Zoll und Polizei.

Rechtsgrundlage für die Zusammenarbeit der europäischen Zollverwaltungen ist bisher das *Neapeler Übereinkommen* vom 7. September 1967. Das Übereinkommen regelt — anders als die EG-Verordnung über die gegenseitige Unterstützung der Zollverwaltungen (s. 6.7) — die Zollbereiche, die nicht aufgrund des EWG-Vertrags in die Zuständigkeit der Europäischen Gemeinschaften fallen (Ein- und Ausfuhrverbote oder Beschränkungen zum Schutz der öffentlichen Sittlichkeit, Ordnung und Sicherheit). Da eine Verankerung der Ausgleichsmaßnahmen zum Abbau der Grenzkontrollen im Neapeler Übereinkommen selbst nicht erreichbar erschien, einigten sich die

Mitgliedstaaten darauf, zunächst nur den automatisierten Datenaustausch zwischen ihnen in einem gemeinsamen Zollinformationssystem (Customs Information System — CIS —) zu regeln. Rechtsgrundlage für die Errichtung von CIS soll eine eigene Konvention werden, die die Zollverwaltungen der EG-Mitgliedstaaten unter dem Vorsitz von Großbritannien erarbeiten. Ziel des Übereinkommens ist die Unterstützung der Zollverwaltungen bei der Verhinderung, Ermittlung und Verfolgung schwerwiegender Zuwiderhandlungen gegen nationale Zollbestimmungen, die dem Schutz der öffentlichen Sicherheit oder der Bekämpfung der Geldwäsche dienen. CIS ist als Verbunddatei geplant, deren zentraler Bestand in Brüssel geführt werden und dem direkten Zugriff der einzelnen Mitgliedstaaten unterliegen soll. In CIS sollen z. B. folgende personenbezogenen Daten erfaßt werden:

— Name, Geburtsname, Vornamen und angenommene Namen

— Geburtsdatum u. Geburtsort

— Staatsangehörigkeit

— Angaben über Waren, Transportmittel etc.

Das Bundesministerium der Finanzen hat mich von Anfang an bei den Verhandlungen beteiligt. Mein Ziel war es, in CIS den guten Datenschutzstandard des Schengener Durchführungsübereinkommens zu erreichen. Obwohl dies nicht in allen Punkten voll gelang, konnte im Entwurf des Übereinkommens zu CIS ein im großen und ganzen zufriedenstellendes datenschutzrechtliches Niveau erreicht werden. Das gilt insbesondere für die Sicherung der Rechte der Betroffenen und die Datenschutzkontrolle. Bedauerlich ist allerdings, daß der Abschluß einer Regelung über den konventionellen Datenaustausch zwischen den Zollbehörden auf unbestimmte Zeit verschoben wurde. Ich habe das BMF darauf aufmerksam gemacht, daß ich auch diesen Bereich für dringend regelungsbedürftig halte.

Die Verhandlungen sind im wesentlichen abgeschlossen. Die zunächst für Ende 1992 vorgesehene Unterzeichnung des Entwurfs des Übereinkommens wurde wegen einiger noch offener Fragen verschoben. Sollte es zu weiteren Verhandlungen kommen, bleibe ich beteiligt. Ferner werde ich nach Inkrafttreten des Vertrags in der gemeinsamen Aufsichtsbehörde für den Datenschutz mitwirken.

26.4 Übermittlungsersuchen von Nachrichtendiensten an das Zollkriminalamt nicht präzise genug

Im Juli 1992 habe ich die Übermittlung personenbezogener Daten zwischen dem Zollkriminalamt (ZKA) einerseits und dem Bundesnachrichtendienst (BND) sowie dem Bundesamt für Verfassungsschutz (BfV) andererseits kontrolliert. Bei der Übermittlung von Daten insbesondere zur Bekämpfung von Verstößen gegen das Außenwirtschaftsgesetz und das Kriegswaffenkontrollgesetz von diesen Nachrichtendiensten an das Zollkriminalamt habe ich keine datenschutzrechtlichen Defizite festgestellt. Die Ersuchen auf Übermittlung von Daten seitens der Nachrichtendienste an das ZKA enthalten jedoch nicht immer ausreichend geeignete Angaben, damit das ZKA prüfen kann, ob eine Übermittlung von Daten nach dem BND- oder Bundesverfassungsschutzgesetz zulässig ist. Auch war der Umfang der gewünschten Informationen in einigen Fällen im Ersuchen nicht hinreichend präzisiert. Ich habe dies den zuständigen Fachaufsichtsbehörden mitgeteilt und Vorschläge gemacht, welche Anforderungen an ein zulässiges Übermittlungsersuchen der Nachrichtendienste an das Zollkriminalamt zu stellen sind. Die Diskussion über diese Frage ist noch nicht abgeschlossen.

27 Verfassungsschutz

27.1 Die Sicherheitsüberprüfung ist gesetzlich zu regeln

Kürzlich hat das Bundesamt für Verfassungsschutz öffentlich bekanntgegeben, daß in der zentralen Verbunddatei der Verfassungsschutzbehörden die Daten von rd. 600 000 Personen aus Anlaß einer Sicherheitsüberprüfung erfaßt sind. Diese Größenordnung unterstreicht eindrucksvoll den gesetzlichen Regelungsbedarf im Bereich der Sicherheitsüberprüfungen (so schon der 2. TB S. 44, ausführlich 9. TB S. 56, zuletzt 12. TB S. 77). Im Zusammenhang mit der Verabschiedung der Gesetze über die Nachrichtendienste (13. TB S. 72) haben Bundestag und Bundesrat meine Hinweise aufgegriffen und die Bundesregierung zur Vorlage eines Gesetzentwurfs aufgefordert. Dies hat den entscheidenden Anstoß gegeben, zuvor ergebnislos gebliebene Vorbereitungen für ein Geheimschutzgesetz (10. TB S. 74) wieder aufzunehmen und den Entwurf eines Sicherheitsüberprüfungsgesetzes vorzulegen.

Anliegen dieses Entwurfs ist allein die Sicherheitsüberprüfung von Personen, denen im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse (Verschlußsachen) anvertraut werden, also der sogenannte „personelle Geheimschutz" (vgl. § 3 Abs. 2 Satz 1 Nr. 1 des Bundesverfassungsschutzgesetzes — BVerfSchG —). Nicht erfaßt ist der „personelle Sabotageschutz" (§ 3 Abs. 2 Satz 1 Nr. 2 BVerfSchG), der Personen betrifft, die an sicherheitsempfindlichen Stellen von lebens- und verteidigungswichtigen Einrichtungen beschäftigt sind oder beschäftigt werden sollen. Wenn an der Notwendigkeit einer Sicherheitsüberprüfung auch für diesen Bereich festgehalten werden soll, besteht — entgegen der Auffassung des Bundesministeriums des Innern — auch insoweit Regelungsbedarf (so bereits 8. TB, Anlage 3), der allerdings auch außerhalb des Sicherheitsüberprüfungsgesetzes aufgegriffen werden kann. Dies ist aber erst für einzelne Bereiche im Ansatz geschehen (vgl. § 12 b Atomgesetz/12. TB S. 77, § 29 d Luftverkehrsgesetz/13. TB S. 57, s. o. 18.10.1).

Das vorgesehene Verfahren zum personellen Geheimschutz greift Grundzüge der bisherigen Verfahrensweise auf, wie sie derzeit in Verwaltungsvor-

schriften, insbesondere den Sicherheitsrichtlinien des Bundes (s. u. 34.9), enthalten sind.

Die deutsche Einheit und der Demokratisierungsprozeß in Osteuropa haben einen angemessenen Geheimschutz nicht überflüssig gemacht, weshalb es auch künftig erforderlich bleiben wird, Personen zu überprüfen, die Zugang zu Verschlußsachen haben oder ihn sich verschaffen können, um z. B. festzustellen, ob es Umstände in ihren Lebensverhältnissen gibt, die sie erpreßbar machen. Allerdings meine ich auch, daß die veränderte Bedrohungslage bei der Gewichtung des öffentlichen Interesses am Geheimschutz und damit auch bei der Verhältnismäßigkeitsabwägung gegenüber Eingriffen in das Persönlichkeitsrecht berücksichtigt werden muß. Es wäre deshalb verfehlt, die bestehenden Verwaltungsvorschriften, die in den Grundzügen aus dem Jahr 1987 stammen, schlicht auf den Rang eines formellen Gesetzes zu heben. Vielmehr ist unter Bewertung der neuen Bedrohungslage eine sachgerechte Lösung für die jetzt erkennbaren Risiken geboten.

Ich habe dazu konkrete Vorschläge gemacht. Der Regierungsentwurf eines Sicherheitsüberprüfungsgesetzes (ESÜG, BR-Drucksache 97/93) enthält deutliche Verbesserungen und hat von mir unterbreitete Anregungen aufgegriffen.

Wesentliche Verbesserungen im Regierungsentwurf gegenüber den bisherigen Sicherheitsrichtlinien sind:

— *Bereichsspezifische Auskunftsregelung*

Im Gegensatz zu der — wenig bürgerfreundlichen — Auskunftsregelung des Bundesverfassungsschutzgesetzes (s. u. 27.3) wird das Auskunftsrecht der Betroffenen über die im Zusammenhang mit ihrer Sicherheitsüberprüfung gespeicherten Daten nicht an irgendwelche zusätzlichen Voraussetzungen geknüpft (§ 23 ESÜG). Eine Auskunft darf damit nur dann abgelehnt werden, wenn Gründe vorliegen, die weitgehend § 19 Abs. 4 BDSG entsprechen. Das sind z. B. die Gefährdung der Aufgabenerfüllung der speichernden Stelle oder der öffentlichen Sicherheit. Auch ist nunmehr ein — von mir mit besonderem Nachdruck geforderter — Anspruch auf Einsicht in die Sicherheitsakte vorgesehen (§ 23 Abs. 6 ESÜG).

— *Engere Zweckbindung*

Die Verwendung für andere Zwecke als den der Sicherheitsüberprüfung soll in § 21 ESÜG klarer und überwiegend einschränkend geregelt werden. Vorgesehen ist z. B. eine Eingrenzung der Verwendung für Zwecke der Strafverfolgung auf Straftaten von erheblicher Bedeutung, ferner eine — wohl eher klarstellende — Beschränkung der Verwendung für arbeits- und dienstrechtliche Maßnahmen, einschließlich disziplinarrechtlicher, auf das zur Gewährleistung des Verschlußsachenschutzes Erforderliche. Besonders wichtig ist die meinen Kompromißvorschlag aufgreifende Begrenzung innerhalb der Aufgaben des Verfassungsschutzes auf die Spionageabwehr, die Terrorismusbekämpfung und im Bereich des nicht gewaltgeneigten Extremismus auf die Aufklärung sonstiger Bestrebungen von erheblicher Bedeutung.

— *Trennung von der Personalverwaltung*

Die Einhaltung der notwendigen Zweckbindung und spezialgesetzlicher Verwendungsbeschränkungen (z. B. nach dem Bundeszentralregistergesetz) sind nur dann gewährleistet, wenn die für die Sicherheitsüberprüfung zuständige Stelle eine von der Personalverwaltung getrennte Organisationseinheit ist (vgl. 12. TB S. 77). Diese organisatorische Trennung soll ausdrücklich gesetzlich festgeschrieben werden (§ 3 Abs. 1 Satz 3 ESÜG).

— *Personalakteneinsicht*

Die mitwirkende Behörde (BfV, MAD) darf nur dann eine Einsicht in die Personalakte des Betroffenen erhalten, wenn dies zur Klärung oder Beurteilung sicherheitserheblicher Erkenntnisse unerläßlich ist, und auch dann nur mit Zustimmung des Betroffenen und der zuständigen Stelle (§ 13 Abs. 6 Satz 5 ESÜG).

— *Geheimschutz in der Wirtschaft*

Entgegen ursprünglichen Vorstellungen ist nun doch beabsichtigt, durch Sonderregelungen (§§ 24 bis 31 ESÜG) den Besonderheiten Rechnung zu tragen, die sich ergeben, wenn eine Person zur Ausübung einer sicherheitsempfindlichen Tätigkeit bei einer nichtöffentlichen Stelle ermächtigt werden soll. Der Gesetzentwurf schließt z. B. aus, daß der nicht-öffentlichen Stelle, also dem Arbeitgeber, Erkenntnisse mitgeteilt werden, die eine Ablehnung der Ermächtigung zur sicherheitsempfindlichen Tätigkeit betreffen (§ 27 Satz 2 ESÜG). Zur Gewährleistung des Verschlußsachenschutzes können sicherheitserhebliche Erkenntnisse selbstverständlich übermittelt werden (§ 27 Satz 3 ESÜG).

Der Entwurf ist eine gute Grundlage für die Beratungen in den gesetzgebenden Körperschaften. aus meiner Sicht bedürfen nur noch wenige Fragen einer nochmaligen vertieften Erörterung. Dabei habe ich insbesondere Fragen der Erhebungstransparenz und der Zweckbindung im Auge:

— Bei der Erhebung von Daten für Zwecke der Sicherheitsüberprüfung durch Befragung von Referenz- und Auskunftspersonen sollten diese grundsätzlich auf den Zweck der Erhebung und die Freiwilligkeit der Angaben hingewiesen werden. Es besteht kein Grund, allgemein von § 13 Abs. 4 BDSG abzuweichen.

— Der oben dargestellte Kompromiß zu den zulässigen Verwendungszwecken ist tragfähig. Allerdings sollte die Zweckbindung im Falle einer Übermittlung der im Sicherheitsüberprüfungsverfahren erhobenen personenbezogenen Daten ausdrücklich auch für den Empfänger gelten, wie dies sowohl im allgemeinen Datenschutzrecht (§ 15 Abs. 3, § 16 Abs. 4 BDSG) als auch speziell im Bundesverfassungsschutzgesetz (§ 19) der Fall ist.

  Der spezielle Vorbehalt für Verwendungsschranken nach dem Stasi-Unterlagen-Gesetz (§ 21 Abs. 1 Satz 4 ESÜG) sollte — schon zur Vermeidung von Umkehrschlüssen — verallgemeinert werden; damit wäre beispielsweise auch klarge-

stellt, daß die Zweckbindung unbeschränkter Auskünfte aus dem Bundeszentralregister (§ 41 Abs. 4 Satz 2 letzter Halbsatz BZRG) unberührt bleibt. In diesem Zusammenhang ist darauf hinzuweisen, daß z. B. § 23 Nr. 3 BVerfSchG besonderen gesetzlichen Übermittlungsregelungen generell den Vorrang vor denen des Bundesverfassungsschutzgesetzes einräumt.

Inzwischen ist mir bekannt geworden, daß in Baden-Württemberg seit 1991 eine Regelung über die Zweckbindung bei der Mitwirkung des Landesamtes für Verfassungsschutz an der Sicherheitsüberprüfung besteht, die offenbar bisher in der Praxis zu keinen Schwierigkeiten geführt hat. Sie sieht im Ergebnis eine Verwendung der aus der Sicherheitsüberprüfung gewonnenen Erkenntnisse für die Aufklärung des Extremismus nur insoweit vor, als es sich um gewalttätigen Extremismus handelt (§ 7 Abs. 3 LVSG). Wenn diese Regelung im Land Baden-Württemberg nicht zu Sicherheitsdefiziten geführt hat, liegt der Schluß nahe, daß sie auch für das Sicherheitsüberprüfungsgesetz des Bundes ohne schädliche Auswirkungen übernommen werden kann.

Der Bundesrat hat in seiner Stellungnahme zum Regierungsentwurf empfohlen, die Zweckbindung der im Rahmen der Sicherheitsüberprüfung gewonnenen personenbezogenen Daten in dieser Weise zu regeln.

27.2 Das Bundesamt für Verfassungsschutz offenbarte Privatpersonen Erkenntnisse über Dritte

Bei der Anwendung des im Dezember 1990 in Kraft getretenen novellierten Bundesverfassungsschutzgesetzes haben sich insbesondere in bezug auf die Datenübermittlung an andere (nicht-öffentliche) Stellen (§ 19 Abs. 4) Schwierigkeiten ergeben. Diese Regelung untersagt grundsätzlich die Datenübermittlung durch das Bundesamt für Verfassungsschutz an (nicht-öffentliche) Stellen, es sei denn, daß dies zum Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes oder der Sicherheit des Bundes oder eines Landes erforderlich ist und das Bundesministerium des Innern seine Zustimmung erteilt hat. In den nachfolgenden Fällen haben sich Betroffene hilfesuchend an mich gewandt:

— Das Bundesamt für Verfassungsschutz hatte in Erfahrung gebracht, daß eine in einer hessischen Stadt wohnhafte Angestellte eines Industrieunternehmens möglicherweise privaten Umgang mit Personen aus dem RAF-Umfeld hatte, und erhoffte sich von ihr nähere Informationen. Für die Kontaktaufnahme wählte das Bundesamt den Weg über ihren Arbeitgeber und informierte deshalb ihren Personalchef — zumindest andeutungsweise — über Hintergrund und Zweck des geplanten Gesprächs. Dieses fand dann sogar in den Räumen der Firma statt, war aber nur von kurzer Dauer, weil die Betroffene es ablehnte, sich unter diesen Umständen gegenüber einem Vertreter des Bundesamtes für Verfassungsschutz über ihren privaten Umgang zu äußern. Das Bundesamt für Verfassungsschutz informierte den Arbeitgeber vom Scheitern des Gespräches. Darauf kam es umgehend zur Aufhebung des Arbeitsverhältnisses, weil die Angestellte nun als Sicherheitsrisiko erschien.

— Nach Erkenntnissen des Bundesamtes für Verfassungsschutz hatte eine Hamburgerin Kontakt zu einer Person, die im Verdacht stand, für einen ausländischen Nachrichtendienst zu arbeiten. Ein Mitarbeiter des Bundesamtes für Verfassungsschutz erhielt den Auftrag, sie in ihrer Wohnung aufzusuchen und sie entsprechend zu sensibilisieren. Als er sie selbst dort nicht antraf, informierte er kurzerhand einen ihrer Mitbewohner.

— Das Bundesamt für Verfassungsschutz hatte von ihm erhobene und gespeicherte personenbezogene Daten eines Bewerbes um ein öffentliches Amt einem Mitglied des brandenburgischen Landtages übermittelt, darunter auch eine Mitteilung über strafrechtliche Verurteilungen.

Alle diese Datenübermittlungen an private Stellen habe ich wegen Verstoßes gegen § 19 Abs. 4 BVerfSchG beanstandet.

In den beiden erstgenannten Fällen hatte das Bundesministerium des Innern meine Beanstandung zunächst zurückgewiesen. Es vertrat die Auffassung, die Datenweitergabe sei durch § 8 Bundesverfassungsschutzgesetz als notwendiger Teil der Datenerhebung gedeckt gewesen.

Es bestehen schon Bedenken, ob überhaupt im Rahmen von Datenerhebungen Datenübermittlungen ohne Rücksicht auf § 19 BVerfSchG erfolgen dürfen. Selbst wenn man das für zulässig hält, wären in den beiden Fällen die Datenübermittlungen nicht gerechtfertigt gewesen, denn sie erfolgten nicht im Rahmen von Datenerhebungen über die jeweils Betroffenen. Der Innenausschuß des Deutschen Bundestages, dem ich über die Problematik berichtet habe, hat meine Auffassung geteilt, daß die Datenübermittlung in den genannten Fällen nicht den datenschutzrechtlichen Anforderungen entsprach. Gleichwohl beharrt das Bundesamt für Verfassungsschutz in gerichtlichen Verfahren, die in beiden Fällen anhängig sind, weiter auf seinem gegenteiligen Standpunkt, den ich für überwunden hielt.

Mit dem Bundesministerium des Innern, das die Fachaufsicht über das Bundesamt führt, besteht nämlich Einigkeit, daß Datenübermittlungen im Zusammenhang mit der Erhebung von Daten für die Erfüllung der Aufgaben des Verfassungsschutzes, z. B. bei der Befragung von Privatpersonen, nur in dem Umfang zulässig sind, wie dies zur Erreichung des Befragungszwecks unerläßlich ist. Sollen personenbezogene Daten außerhalb einer Datenerhebung oder über das zur Erreichung des Befragungszwecks unerläßliche Maß hinaus an Privatpersonen weitergegeben werden, so ist dies nur unter den Voraussetzungen des § 19 Abs. 4 BVerfSchG erlaubt. Diese Gesetzesauslegung erlaubt dem Bundesamt für Verfassungsschutz eine sachgerechte Aufgabenerfüllung. Aus Gründen der Normenklarheit sollte jedoch bei

einer künftigen Novellierung des Gesetzes eine gesetzliche Klarstellung erfolgen.

In dem dritten der eingangs erwähnten Fälle hat das Bundesministerium des Innern meine Beanstandung zwar nicht ausdrücklich zurückgewiesen, jedoch geltend gemacht, daß die Datenübermittlung im Rahmen des § 19 Abs. 1 Bundesverfassungsschutzgesetz zulässig gewesen sei. Nach dieser Regelung dürfen personenbezogene Daten an inländische Behörden übermittelt werden, wenn dies zur Erfüllung der Aufgaben des Bundesamtes für Verfassungsschutz erforderlich ist oder der Empfänger die Daten zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für Zwecke der öffentlichen Sicherheit benötigt. Diese Regelung ist aber hier nicht einschlägig, weil die Übermittlung nicht an die Behörde Landtag, sondern an ein einzelnes Mitglied erfolgte, das im übrigen selbst bestätigt hat, es habe die ihm überlassenen Unterlagen für sich behalten, insbesondere nicht an den Ausschuß weitergeleitet, dessen stellvertretendes Mitglied es war. Der Innenausschuß des Deutschen Bundestages hat auch in diesem Falle meine Rechtsauffassung bestätigt.

27.3 Auskünfte an den Betroffenen zu restriktiv

Bei der Erarbeitung des neuen Verfassungsschutzgesetzes war es ein Anliegen des Gesetzgebers, die Rechte der betroffenen Bürger zu stärken. Zu diesem Zweck wurde in § 15 des Gesetzes das Recht auf Auskunft bereichsspezifisch normiert. Die Praxis der vergangenen zwei Jahre zeigt, daß eine ganze Reihe von Bürgern Auskunft über möglicherweise beim Verfassungsschutz über sie gespeicherte Daten erhalten wollen. Das Bundesverfassungsschutzgesetz sieht in § 15 Abs. 1 grundsätzlich vor, daß dem Betroffenen über zu seiner Person gespeicherte Daten auf Antrag unentgeltlich Auskunft zu erteilen ist, soweit er hierzu auf einen konkreten Sachverhalt hinweist und ein besonderes Interesse an einer Auskunft darlegt.

Bis vor kurzem hat das Bundesamt für Verfassungsschutz die Anwendung des § 15 Abs. 1 BVerfSchG in der Weise praktiziert, daß es regelmäßig die Auskunft ablehnte, wenn auch nur ein Teil der in § 15 Abs. 1 BVerfSchG genannten Voraussetzungen fehlte. Das Bundesamt für Verfassungsschutz teilte dem Bürger lediglich mit, es könne wegen der fehlenden Anspruchsvoraussetzungen keine Auskunft erteilen. Die Frage, ob in solchen Fällen, selbst wenn ein Rechtsanspruch auf Auskunft nach dem Gesetz nicht gegeben war, nicht doch eine Auskunft erteilt werden konnte, ohne die Aufgabenerfüllung des Bundesamtes für Verfassungsschutz zu gefährden, wurde gar nicht erst gestellt. Die Vorschrift wurde also so angewandt, als enthalte sie ein Verbot für eine Auskunft in Fällen, bei denen die Voraussetzungen des § 15 BVerfSchG nicht vorliegen.

Ein derartiges Verbot vermag ich § 15 Abs. 1 BVerfSchG nicht zu entnehmen. Die Vorschrift besagt lediglich, daß der Betroffene, wenn er auf einen konkreten Sachverhalt hinweist und ein besonderes Interesse an der Auskunft darlegt, einen Rechtsanspruch auf Auskunft hat, sofern nicht die Ausschlußgründe des Absatzes 2 vorliegen. Die Vorschrift verbietet aber keineswegs, dem Betroffenen im Rahmen der Ausübung pflichtgemäßen Ermessens auch in anderen Fällen Auskunft zu geben.

Das Bundesamt wandte die Vorschrift im übrigen auch insofern einschränkend an, als es Auskunft nur zu dem Sachverhaltskomplex erteilte, auf den sich die besonderen Darlegungen des Betroffenen jeweils bezogen. Es teilte dem Betroffenen z. B. mit, Daten über ihn seien wegen des vorgetragenen Sachverhalts nicht gespeichert. Über andere Speicherungen schwieg es sich aus, auch wenn der Betroffene — wie üblich — ganz allgemein angefragt hatte, welche Daten über ihn gespeichert seien. Es wurde nicht geprüft, ob dem Betroffenen auch zu anderen Sachverhalten eine weitere Auskunft gegeben werden konnte. Der Bürger erhielt in solchen Fällen auch keinen — allenfalls einen sehr versteckten — Hinweis darauf, daß es sich bei der Auskunft nur um eine Teilauskunft handelte.

Auf Grund einiger Eingaben habe ich auch festgestellt, daß das Bundesamt für Verfassungsschutz an den Hinweis auf einen konkreten Sachverhalt zu hohe Anforderungen gestellt hat. Auch dann, wenn Bürger Sachverhalte vortrugen, die von vornherein nicht zu einem Tätigwerden des Bundesamtes für Verfassungsschutz geführt haben konnten, wurde äußerst restriktiv verfahren.

Gerade in solchen Fällen könnte es zur Beruhigung der Bürger beitragen, wenn das Bundesamt für Verfassungsschutz die Auskunft erteilte, daß es keine Daten gespeichert hat, insbesondere dann, wenn nicht zu befürchten ist, daß die Aufgabenerfüllung des Bundesamtes für Verfassungsschutz durch eine Auskunftserteilung gefährdet wird.

Bei der bisherigen Auskunftspraxis des Bundesamtes für Verfassungsschutz verwundert es nicht, daß die beschriebene Haltung der Verfassungsschutzbehörde zu wenig befriedigenden Auskünften führte.

Wegen der Schwierigkeiten bei der Anwendung des § 15 BVerfSchG habe ich mich sowohl an das Bundesministerium des Innern als auch an den Innenausschuß des Deutschen Bundestages gewandt.

Der Deutsche Bundestag hat auf Vorschlag des Innenausschusses die Angelegenheit aufgegriffen und der Bundesregierung empfohlen (s. BT-Drucksache 12/4094), „bei der Anwendung des § 15 BVerfSchG

aa) davon auszugehen, daß die Vorschrift in Fällen, in denen die Voraussetzungen dieser Vorschrift nicht vorliegen — vorbehaltlich des Absatzes 2 — eine Auskunftserteilung zuläßt,

bb) deshalb auch der Umfang der Auskunft nicht zwingend auf Speicherungen zu dem Sachverhalt beschränkt ist, der konkret vorgetragen wurde,

cc) an die Darlegungen eines konkreten Sachverhalts und eines besonderen Interesses an der Auskunft keine zu strengen Anforderungen zu stellen."

Ich gehe davon aus, daß das Bundesamt für Verfassungsschutz nunmehr zu dieser Auskunftspraxis

übergeht. Damit wäre eine Annäherung an die bürgerfreundlichen Regelungen in den Verfassungsschutzgesetzen der Länder Hessen, Schleswig-Holstein und Sachsen gefunden, die den Auskunftsanspruch des Bürgers nicht vom Vortrag eines konkreten Sachverhalts und der Darlegung eines besonderen Interesses abhängig machen. Wie mir u. a. der Landesbeauftragte für den Datenschutz von Schleswig-Holstein mitgeteilt hat, führen diese Bestimmungen in der Praxis zu keinerlei Schwierigkeiten bei der Aufgabenerfüllung der dortigen Verfassungsschutzbehörden.

Bei der Notwendigkeit, einen konkreten Sachverhalt zu benennen, und sei es auch in der „gemilderten" Form der genannten Empfehlung des Innenausschusses des Deutschen Bundestages, bleibt das Problem einer möglichen Selbstbezichtigung. Hierzu hat mir das Bundesamt für Verfassungsschutz allerdings zugesagt, solche vom Bürger selbst im Rahmen eines Auskunftsersuchens vorgetragenen Sachverhalte in seinen Fachabteilungen nicht zu nutzen und zu speichern.

Die Durchführung des vom Bundestag empfohlenen Verfahrens werde ich beobachten.

27.4 Das Bundesamt für die Anerkennung ausländischer Flüchtlinge darf nicht alle Daten aus Asylverfahren an Nachrichtendienste übermitteln

Um mir ein Bild darüber zu verschaffen, inwieweit Informationen aus Asylverfahren an das Bundesamt für Verfassungsschutz und an andere Nachrichtendienste übermittelt werden und ob diese Praxis der durch das neue Bundesverfassungsschutzgesetz veränderten Rechtslage angepaßt wurde, habe ich 1992 das Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) besucht.

Im Gebäude des Bundesamtes in Zirndorf waren zum Zeitpunkt des Besuchs Außenstellen des Bundesamtes für Verfassungsschutz und des Bundesnachrichtendienstes untergebracht. Den Asylbewerbern wurde nach der Anhörung durch einen Bediensteten des Bundesamtes für die Anerkennung ausländischer Flüchtlinge ein Handzettel des Bundesamtes ausgehändigt, auf dem lediglich die Büroräume aufgeführt waren, die sie aufsuchen sollten. Die Räumlichkeiten waren nicht als Dienststellen der Nachrichtendienste gekennzeichnet. Asylbewerber, die sich dorthin begaben, konnten deshalb annehmen, daß sie auch dort für ihr Asylgesuch Relevantes zu erledigen hätten. Ihnen wurde auf diese Weise suggeriert, daß sie notwendigerweise die im Handzettel aufgeführten Stationen im Rahmen ihres Anerkennungsverfahrens zu durchlaufen hätten, um ihrem Antragsbegehren Geltung zu verschaffen. In den Räumen der Dienste wurden die Asylbewerber auf die Freiwilligkeit von Angaben hingewiesen, aber eben erst, wenn sie sich schon dort befanden. In den Befragungen durch die Nachrichtendienste wurden Informationen von den Asylbewerbern erhoben und anschließend beim Bundesamt für Verfassungsschutz sowie beim Bundesnachrichtendienst verarbeitet.

Darüber hinaus hat das Bundesamt für die Anerkennung ausländischer Flüchtlinge ganz allgemein Daten über Asylbewerber den Nachrichtendiensten zugänglich gemacht. Eine gesetzliche Grundlage für die darin liegenden Übermittlungen personenbezogener Daten fehlte weitgehend. Nach § 18 Abs. 1 BVerfSchG haben Bundesbehörden das BfV von sich aus nur über Tatsachen zu unterrichten, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht oder Bestrebungen im Bundesgebiet erkennen lassen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Abs. 1 Nr. 1 und 3 genannten Schutzgüter gerichtet sind. Auch auf Ersuchen des BfV dürfen Bundesbehörden nur solche personenbezogene Informationen übermitteln, die zur Erfüllung der Aufgaben des BfV erforderlich sind und nicht aus allgemein zugänglichen Quellen oder nur mit übermäßigem Aufwand oder nur durch eine den Betroffenen stärker belastende Maßnahme erhoben werden können (§ 18 Abs. 3 BVerfSchG). Eine wahllose Übermittlung fast aller im Asylverfahren anfallenden Informationen an Verfassungsschutzbehörden ist daher nicht zulässig.

Für die Übermittlung von Informationen an den BND gelten nach § 8 BNDG die gleichen Grundsätze.

Ich habe die Bundesregierung aufgefordert, das Verfahren der Datenübermittlung so zu regeln, daß es den gesetzlichen Vorgaben entspricht. Dem will die Bundesregierung folgen.

27.5 Bundesamt für Verfassungsschutz behindert datenschutzrechtliche Kontrollen

Wie alle öffentlichen Stellen des Bundes ist auch das BfV nach § 24 Abs. 4 BDSG grundsätzlich verpflichtet, mich bei der Erfüllung meiner Aufgaben zu unterstützen, mir insbesondere Auskunft zu meinen Fragen zu erteilen. Zu Beginn des Berichtszeitraums hatten sich die Fälle gehäuft, in denen das BfV dieser Pflicht nicht in der gebotenen Weise nachgekommen war. Ich habe dies am 20. August 1991 gegenüber dem Bundesministerium des Innern beanstandet. Dem lagen folgende Fälle zugrunde:

— Das mit Schreiben vom 22. März 1991 erstmals mit einer Eingabe befaßte BfV war von mir mit Schreiben vom 19. Juni 1991 zur kurzfristigen Stellungnahme aufgefordert worden. Trotz dreimaliger Erinnerung, zuletzt am 16. August 1991, war keine Reaktion des BfV erfolgt.

— In einem anderen Fall hatte ich das BfV — erstmals am 8. November 1990 — um Stellungnahme gebeten. Nach einer beiläufigen mündlichen Erörterung gelegentlich eines Kontrollbesuchs am 28. Januar 1991, in der die Bitte um schriftliche Stellungnahme bekräftigt worden war, erfolgte — nach weiteren zwei Mahnungen — am 29. Mai 1991 eine erste, inhaltlich aber unzureichende schriftliche Antwort. Trotz weiterer drei Mahnungen war die ausstehende ergänzende Stellungnahme nicht erfolgt.

— Bei datenschutzrechtlichen Kontrollen am 19. November 1990 und 28. Januar 1991 hatte ich einige Mängel festgestellt, die zu beseitigen mir zugesagt worden war. Trotz viermaliger Erinnerung war die zugesagte Stellungnahme in der Angelegenheit nicht erfolgt.

Leider habe ich nicht feststellen können, daß sich infolge der Beanstandung die Bereitschaft des BfV, mich bei meiner Aufgabenerfüllung zu unterstützen, grundlegend verbessert hätte.

Hierzu nur ein neueres Beispiel:

Aufgrund von Presseveröffentlichungen im Sommer vergangenen Jahres war bekannt geworden, daß dem Bundesamt für Verfassungsschutz Erkenntnisse über eine mutmaßliche Stasi-Mitarbeit eines Mitgliedes der Landesregierung in einem neuen Bundesland vorlagen. Die Erkenntnisse beruhten auf Aussagen eines Überläufers gegenüber einem Landesamt für Verfassungsschutz, die dem BfV zugegangen waren. Sie wurden auf verschiedenen Wegen Stellen des betreffenden Bundeslandes, unter anderem dem Ministerpräsidenten, übermittelt. Dabei war auch die — zwischenzeitlich aufgelöste — Außenstelle des BfV in dem neuen Bundesland tätig gewesen.

Wegen möglicher Verletzungen schutzwürdiger Interessen des Betroffenen und weiterer Personen habe ich beim BfV eine Kontrolle begonnen. Diese konnte jedoch bislang nicht abgeschlossen werden, u. a. weil nach Angaben des BfV die Unterlagen der ehemaligen Außenstelle vernichtet worden seien. Soweit einzelne Vermerke der Außenstelle — die im übrigen auszugsweise in der Presse veröffentlicht waren — noch vorhanden waren, wurden sie mir nur unvollständig zur Kenntnis gegeben. Auch die Überlassung einer Kopie derjenigen Unterlagen, die, wie eingangs erwähnt, von einem Landesamt dem BfV übermittelt worden waren, wurde mir verweigert.

Nachdem ich mich an das Bundesministerium des Innern gewandt hatte, konnte ich in die Unterlagen Einsicht nehmen.

27.6 Gesperrte NADIS-PZD-Daten dürfen nicht rechtswidrig genutzt werden

Das neue Bundesverfassungsschutzgesetz (BVerfSchG) sieht in § 12 Abs. 2 erstmals vor, daß personenbezogene Daten, die in Dateien des Bundesamtes für Verfassungsschutz nur deshalb weiter gespeichert bleiben, weil ihre Löschung schutzwürdige Belange des Betroffenen beeinträchtigen würde, zu sperren sind. Die gesperrten Daten dürfen nur noch mit Einwilligung des Betroffenen übermittelt werden. Das Bundesamt für Verfassungsschutz hat mir im August 1992 auf wiederholtes Drängen eine Verfahrensbeschreibung für die Sperrung von Datensätzen in der Datei NADIS-PZD (Personenzentraldatei) zugesandt und mitgeteilt, diese Regelung werde voraussichtlich Mitte September 1992 in die Praxis umgesetzt. Das Konzept sah vor, daß zu sperrende Datensätze mit einem besonderen Kennzeichen versehen werden, das auf die Sperrung der Informationen gemäß § 12 Abs. 2 BVerfSchG hinweist. Der Hinweis soll bewirken, daß die gesperrten Daten ausschließlich dem Datenschutzreferat des BfV zur Verfügung stehen, nicht jedoch den operativen Abteilungen oder sonstigen Teilnehmern am Verbundsystem NADIS. Fragt ein anderer Verbundteilnehmer NADIS nach Speicherungen für die betroffene Person ab, so erhält er keinen Hinweis auf den gesperrten Bestand. Jedoch wird das Datenschutzreferat des Bundesamtes in diesen Fällen benachrichtigt.

Gegen diese Regelung habe ich im Oktober 1992 gegenüber dem Bundesamt für Verfassungsschutz Bedenken geäußert. Wenn zu löschende Daten nur deshalb weiter gespeichert bleiben, weil sonst schutzwürdige Interessen des Betroffenen beeinträchtigt würden, dann muß auch sichergestellt werden, daß die gesperrten Daten nicht mehr zum Nachteil des Betroffenen verwendet werden. Diesem Grundsatz widersprach die Regelung in der Verfahrensbeschreibung, daß gesperrte Datensätze zwar grundsätzlich nicht in Auswertungen, Dokumentationen, Überprüfungslisten aufzunehmen sind, dies aber ausnahmsweise zulässig sein soll, wenn es ausdrücklich verfügt wurde. Ein weiterer Schwachpunkt der vorgesehenen Regelung war, daß dem Datenschutzreferat des BfV eine Kontaktaufnahme mit einem anfragenden Verbundteilnehmer ermöglicht worden wäre mit der Konsequenz, daß dabei gegen das klare Übermittlungsverbot des § 12 Abs. 2 Satz 4 BVerfSchG verstoßen werden kann.

Ich habe auch angeregt, bei gesperrten Datensätzen ein Wiedervorlagedatum vorzumerken, das sich an der voraussichtlichen Dauer der Sperrung des Datensatzes orientieren sollte. Damit soll gewährleistet werden, daß gesperrte Datensätze nicht länger gespeichert bleiben wie es die schutzwürdigen Interessen des Betroffenen erfordern.

Das Bundesamt für Verfassungsschutz ist in seiner Stellungnahme vom Dezember 1992 meinen Forderungen nur in einem Punkt gefolgt: Die ausnahmsweise Aufnahme gesperrter Datensätze in Auswertungen, Dokumentationen und Prüflisten ist jetzt nicht mehr vorgesehen.

Ich habe dem Bundesministerium des Innern meine fortbestehenden Bedenken mitgeteilt. Da die Angelegenheit auch für die Länder von Bedeutung ist, habe ich mit den Landesbeauftragten für den Datenschutz Kontakt aufgenommen.

28 Bundesnachrichtendienst

28.1 Bundesnachrichtendienst überprüft Altdatenbestände

Beim Bundesnachrichtendienst (BND) habe ich schwerpunktmäßig die Durchführung des neuen BND-Gesetzes kontrolliert. Durch dieses Ende 1990 in Kraft getretene Gesetz sind die Informationserhebung

und -verarbeitung des BND erstmals auf eine gesetzliche Grundlage gestellt worden.

Ich habe u. a. folgende Feststellungen getroffen:

— Um die Bediensteten mit der neuen Gesetzesmaterie vertraut zu machen, hat der BND interne Schulungsmaßnahmen durchgeführt. Die Überarbeitung der innerdienstlichen DV-Vorschriften ist in Angriff genommen worden. Ich habe darauf gedrängt, daß die erforderlichen innerdienstlichen Regelungen zur Umsetzung des BND-Gesetzes und anderer datenschutzrechtlicher Vorschriften möglichst umgehend in Kraft gesetzt werden.

Das Bundeskanzleramt hat mir zwischenzeitlich angekündigt, daß die erforderlichen dienstinternen Verfügungen voraussichtlich bis Mitte des Jahres in Kraft treten werden.

— Auch beim BND gibt es das Problem der Bereinigung von Altdatenbeständen. Der BND ist nach § 5 Abs. 1 BDSG in Verbindung mit § 12 Abs. 3 Satz 1 BVerfSchG verpflichtet, bei der Einzelfallbearbeitung und nach festgesetzten Fristen, spätestens nach fünf Jahren, zu prüfen, ob gespeicherte personenbezogene Daten zu berichtigen oder zu löschen sind. Der Gesamtbestand (von Ende 1990) müßte also spätestens fünf Jahre nach Inkrafttreten des BND-Gesetzes, d. h. bis Ende 1995 geprüft sein. Der BND hat mir zunächst erklärt, die 5-Jahresfrist lasse sich bei Fortgang der Arbeiten im bisherigen Tempo infolge organisatorischer und personalwirtschaftlicher Probleme nicht einhalten. Da dies nicht akzeptabel war, habe ich mich an den Chef des Bundeskanzleramtes gewandt. Dieser hat inzwischen mitgeteilt, der BND werde seine Datenbestände fristgerecht überprüfen.

— Gegenstand meiner Kontrolle waren ferner Eingaben von Bürgern. Dabei ging es insbesondere um Art und Umfang des Auskunftsrechts. In den meisten Fällen habe ich erreicht, daß dem Ersuchen der Petenten entsprochen wurde.

28.2 Schwierigkeiten bei datenschutzrechtlicher Kontrolle

Der Ehegatte eines BND-Mitarbeiters, der der Einbeziehung in eine Sicherheitsüberprüfung nicht zugestimmt hatte, wandte sich mit einer Eingabe an mich. Die gebotene datenschutzrechtliche Kontrolle konnte ich bis Redaktionsschluß nicht durchführen. Unter Hinweis auf § 24 Abs. 1 Satz 2 BDSG hat mir der BND nämlich die Einsichtnahme in die Sicherheitsakte des Bediensteten mit der Begründung verweigert, eine Verletzung von Rechten des Ehegatten sei nicht hinreichend dargelegt worden.

Das Verhalten des BND verstieß gegen § 24 Abs.1 (Kontrollauftrag) und Abs. 4 BDSG (Verpflichtung der Bundesbehörden, mich zu unterstützen). Ich habe nämlich festgestellt, daß die Sicherheitsakte auch Bezug zu einer dateimäßigen Datenverarbeitung hat, die meine uneingeschränkte Kontrollkompetenz nach sich zieht. Zudem hat mir der betroffene Mitarbeiter des BND seine Zustimmung zur Einsichtnahme in seine Akten erteilt.

Nachdem ich den Chef des Bundeskanzleramtes eingeschaltet hatte, hat dieser den BND angewiesen, mir Einsicht in die Sicherheitsakte des Petenten zu gewähren.

29 Militärischer Abschirmdienst — Altdatenbereinigung braucht sehr viel Zeit —

Im Jahre 1988 habe ich eine Querschnittskontrolle beim Amt für den Militärischen Abschirmdienst durchgeführt. In meinen Tätigkeitsberichten der vergangenen Jahre (11. TB, S. 70f.; 12. TB, S. 81; 13. TB, S. 76) habe ich hierüber sowie über die bisher erzielten Ergebnisse berichtet. Die aufgrund der damals getroffenen Feststellungen erforderlichen Bereinigungsarbeiten in den Ermittlungsvorgänge des *Abwehrbereichs* II (Abwehr verfassungsfeindlicher Kräfte) aus den Jahren 1978 bis 1987 sind nach Mitteilung des Bundesministeriums der Verteidigung zum Jahresende 1992 abgeschlossen worden. Soweit diese Vorgänge keine relevanten Erkenntnisse mehr enthielten, wurden die Unterlagen vernichtet.

Die anstehende Altdatenbereinigung für den Abwehrbereich III (Spionageabwehr) war wegen der aus den Unterlagen der NVA hinzugekommenen Erkenntnisse verschoben worden. Sie wird nun in zwei Stufen durchgeführt:

Zunächst ist eine *kursorische* Durchsicht der Unterlagen vorgenommen worden, die zum Ziel hatte, daß schnell jedenfalls personenbezogene Daten der Personen, die nicht als verdächtig oder als Mitarbeiter fremder Nachrichtendienste anzusehen sind, in der Datei des MAD gelöscht werden. Dies ist zwischenzeitlich abgeschlossen.

In einer zweiten Stufe werden die Aktenvorgänge auch der übrigen Personen, sorgfältig darauf hin überprüft, ob deren Kenntnis für die Facharbeit des Militärischen Abschirmdienstes nicht mehr erforderlich ist. Diese Arbeiten werden, wie mir das Bundesministerium der Verteidigung mitteilte, bis Ende 1995 durchgeführt sein. Spätestens bis zu diesem Zeitpunkt wird demzufolge der gesamte Datenbestand der Abteilung III des Militärischen Abschirmdienstes unter dem Gesichtspunkt der weiteren Erforderlichkeit der Speicherung überprüft sein.

30 Datensicherung

30.1 Der Sachverstand von Fachleuten wird genutzt — Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik —

Am 1. Januar 1991 ist das „Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informations-

technik (BSI-Errichtungsgesetz — BSIG)" in Kraft getreten; ich habe darüber berichtet (13. TB, S. 80). Gemäß § 3 Abs. 1 Nr. 5 BSIG hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) auch die Aufgabe, den Bundesbeauftragten für den Datenschutz zu unterstützen.

In mehreren Fällen habe ich bereits den besonderen Sachverstand des BSI genutzt:

— Einsatz von Chipkarten in der Krankenversicherung

Ein wesentlicher Punkt bei der Gestaltung der Krankenversichertenkarte (KVK; s. o. 12.4) war deren Schutz gegen unzulässige Speicherungen auf dem Speicherchip.

Auf mein Unterstützungsersuchen hin empfahl das BSI, den Dateninhalt der KVK durch das kryptographische Verfahren der Elektronischen Unterschrift derart zu „versiegeln", daß eine Veränderung weitgehend unmöglich, in jedem Fall aber bemerkbar würde. Unter Verweis auf nicht bezifferte Mehrkosten wurde dieses vom BSI und von mir gemeinsam getragene Konzept abgelehnt. Stattdessen wurde ein Verfahren vorgeschlagen, das weiterhin von einer ungeschützten KVK ausging, jedoch verbesserte Transparenz für den Versicherten sicherstellen will: Durch geeignete, manipulationsgesicherte Lesegeräte soll der Versicherte unter zumutbaren Benutzungsbedingungen insbesondere unzulässige Änderungen bald und sicher bemerken können. Es bleibt abzuwarten, ob dieses Konzept — unter Berücksichtigung der von mir als unerläßlich bezeichneten Anforderungen — dem Schutz der Versicherten Rechnung trägt.

— Beratung der Zentralen ADV-Prüfung der Bundesverbände der Allgemeinen Ortskrankenkassen (AOK), der Betriebskrankenkassen (BKK) und der Innungskrankenkassen (IKK) (ZAP) bei der Entwicklung eines Unix-Leitfadens.

Die ZAP hat mir den Entwurf eines „UNIX-Sicherheitsleitfadens der Zentralen ADV-Prüfung der Bundesverbände der Krankenkassen" mit der Bitte um Stellungnahme zugesandt, „um sicherzustellen, daß dieser Leitfaden alle datenschutzrechtlichen Belange abdeckt". Der Leitfaden war von einer Arbeitsgruppe, in der der AOK-, der IKK- und der BKK-Bundesverband vertreten waren, entwikkelt worden. Er soll Risiken und Schwachstellen von Systemen bei der Verarbeitung personenbezogener Daten analysieren helfen und Lösungsmöglichkeiten aufzeigen.

Gemeinsam mit dem BSI habe ich einige Verbesserungen vorgeschlagen. Hier ist vor allem zu nennen, daß in den „Leitfaden" eine Empfehlung aufgenommen wurde, möglichst nur vom BSI zertifizierte Betriebssysteme aufzunehmen und durch das BSI entwickelte Verfahren zur kryptographischen Verschlüsselung zu berücksichtigen.

— Beratung der Physikalisch-Technischen Bundesanstalt (PTB)

Das gegenwärtige Personaldatenverarbeitungssystem der PTB (s. auch oben 9.5.2) auf einem Großrechner entspricht nicht mehr dem Stand der Technik. Es ist daher vorgesehen, ein neues System zu entwickeln, und zwar entweder in einem APC-Netz (Novell) oder auf einem Mehrplatzsystem (UNIX). Ich habe gemeinsam mit dem BSI vorgeschlagen, den Einsatz einer Datenbank (Oracle) auf dem Mehrplatzsystem vorzusehen. Bei der PTB bestehen bereits solche Verfahren für ein Haushaltssystem und eine Zulassungsdatenbank. Die organisatorische Verantwortung für das System wird und die Administration des Systems soll bei der EDV-Abteilung liegen. Der Rechner des Mehrplatzsystems steht auch dort. Die Datenbankadministration soll jedoch vom Personalreferat verantwortet werden. Eine Entscheidung in dieser Frage ist jedoch noch nicht getroffen worden. Es wurden weitere Beratungsgespräche vereinbart, die ebenfalls unter Beteiligung des BSI durchgeführt werden sollen.

Die Zusammenarbeit mit dem BSI hat sich bereits als sehr nützlich erwiesen. Sie wird sich in den kommenden Jahren sicherlich noch erweitern lassen.

30.2 Gestaltung und Verwendung von Paßwörtern will gelernt sein

Bei Kontrollen und Beratungen ist in den letzten Jahren deutlich geworden, daß in der Benutzerverwaltung für den Zugang zu ADV-Systemen eine erhebliche Schwachstelle liegen kann. Zur Verbesserung der Situation habe ich den obersten Bundesbehörden im Berichtszeitraum „Empfehlungen zur Paßwortgestaltung und zum Sicherheitsmanagement" (siehe Anlage 13) gegeben. Die Empfehlungen enthalten Vorschläge für die Handhabung von Benutzerkennung und Paßwort. Sie sind bei den Benutzern von ADV-Anlagen und in der Fachpresse gut aufgenommen worden. Ich habe auch vorgeschlagen, permanente Benutzerkennungen nur für eigene Bedienstete einzurichten. Für Fremde (Wartung usw.) sollen Benutzerkennungen nur temporär zur kontrollierten Inanspruchnahme vergeben werden; das bedeutet, daß die Paßwörter für diese Kennungen durch die speichernde Stelle ausgegeben werden und dem Wartungspersonal nur von Fall zu Fall zur einmaligen Benutzung mitgeteilt werden sollen. Die verbreitete Praxis, daß das Wartungspersonal selbst Kennungen einrichtet und diese mit einem Paßwort versieht, das auch allen anderen Wartungstechnikern der Lieferfirma bekannt ist, halte ich für ein erhebliches Sicherheitsrisiko. Benutzer haben mir allerdings berichtet, daß diese Umstellung auf völliges Unverständnis beim Wartungspersonal stieß. Es sei argumentiert worden, der Techniker „könne dann nicht mehr an seine eigene Anlage". Dabei wird verkannt, daß für die Datenverarbeitungsanlage und die darauf befindlichen Daten allein der Anwender verantwortlich ist. Ich habe daher gegenüber mehreren Herstellern von Datenverarbeitungsanlagen angeregt, meine Empfehlungen auch beim Wartungspersonal bekannt zu machen. Antworten dazu stehen noch aus.

30.3 Kryptographische Verschlüsselung vielfach dringend zu empfehlen

Bei der Verarbeitung besonders schutzbedürftiger („sensibler") Daten und dem Betrieb besonders gefährdeter ADV-Verfahren und -systeme sind auch besonders wirksame technische und organisatorische Maßnahmen i. S. des § 9 BDSG — insbesondere zum Schutz gegen unbefugte Kenntnisnahme — vorzusehen.

Anhaltspunkte dafür, welche *Daten* als besonders sensibel anzusehen sind, enthält § 28 Abs. 2 Satz 2 BDSG, der für die Datenverarbeitung im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses einen besonderen Schutz für Daten vorsieht, die sich

— auf gesundheitliche Verhältnisse,

— auf strafbare Handlungen,

— auf Ordnungswidrigkeiten,

— auf religiöse oder politische Anschauungen sowie

— bei Übermittlungen durch den Arbeitgeber auf arbeitsrechtliche Rechtsverhältnisse

beziehen.

Auch die Konvention 108 des Europarates geht von einem besonderen Schutzbedarf für bestimmte Datenarten jedenfalls dann aus, wenn sie automatisiert verarbeitet werden. Artikel 6 der Konvention betrifft im wesentlichen die genannten personenbezogenen Daten, aber auch Angaben über die rassische Herkunft und das Sexualleben.

Als besonders gefährdete technische *Systeme* sind — aufgrund ihrer technischen Eigenschaften — grundsätzlich Stand-alone Arbeitsplatzrechner, wie etwa Laptops, und auch — insbesondere über das öffentliche Telefonnetz — vernetzte Systeme anzusehen.

Die erforderlichen Schutzmaßnahmen müssen aufgrund einer *Risikoanalyse* unter Berücksichtigung der Sensibilität der Daten und der sicherheitsrelevanten Eigenschaften des technischen Systems, aber auch der Systemumgebung — z. B. der organisatorischen und baulichen Gegebenheiten — ermittelt und festgelegt werden. Bei der Verarbeitung besonders sensibler Daten oder dem Betrieb besonders gefährdeter Systeme ist in der Regel eine *kryptographische Verschlüsselung* der Daten geboten.

Verschlüsselungsverfahren unterschiedlicher mathematischer Ausgestaltung und unterschiedlicher Sicherheit sind in der Fachwelt hinlänglich bekannt und werden auch am Markt angeboten. Sie werden in der Praxis der öffentlichen Verwaltung bisher außerhalb des Geltungsbereichs der Verschlußsachenanweisung (VS-Bereich) allerdings nur selten eingesetzt.

Einige Betriebssysteme und Datenbanksysteme bieten eine Verschlüsselung optional an. Diese und auch andere reine Softwarelösungen werden gemeinhin als weniger sicher als Hardwarelösungen angesehen, da ein Angreifer z. B. die Verschlüsselungssoftware so manipulieren könne, daß eine Verschlüsselung nur noch vorgetäuscht würde und eine Sicherheit somit in Wirklichkeit nicht mehr bestehe. Für viele Anwendungen sind Softwarelösungen aber durchaus ausreichend. In Kombination mit organistorischen Maßnahmen — z. B. zur Zugangskontrolle — ist im Regelfall auch mit einer solchen Lösung eine angemessene Gesamtsicherheit zu erreichen.

Ich begrüße es daher, daß das Bundesamt für Sicherheit in der Informationstechnik (BSI) jetzt zwei softwaregestützte Verfahren entwickelt hat, die für APC-Anwendungen außerhalb des VS-Bereiches geeignet erscheinen. Es handelt sich um eine Sicherheitsoberfläche für Stand-Alone-Arbeitsplatzrechner mit einer Zwangskryptierung der Dateien der Festplatte sowie um eine Verschlüsselungsroutine für einzelne Dateien. Beide arbeiten mit einem BSI-eigenen Chiffrierverfahren.

Auch die Deutsche Bundespost Telekom mißt inzwischen der krytographischen Verschlüsselung der auf ihren Leitungen übermittelten Daten erhöhte Bedeutung bei. Die vor einigen Jahren beim Fernmeldeamt Siegen eingerichtete Projektgruppe TELESEC hat ein Verschlüsselungsverfahren erarbeitet, das hohe Sicherheit gegen unbefugte Kenntnisnahme des Datenverkehrs gewährleistet. Es soll demnächst als reguläre Dienstleistung angeboten werden; erste Betriebsversuche wurden bereits vorgenommen.

Ich empfehle der speichernden Stelle dringend, sich bei der Verarbeitung sensibler Daten und beim Einsatz besonders gefährdeter technischer Datenverarbeitungssysteme dieser oder anderer kryptographischer Verfahren zu bedienen, um auch angesichts der immer besser werdenden technischen Ausstattung sogenannter Hacker einen angemessenen Schutz ihrer automatisierten Datenverarbeitung zu erzielen.

30.4 Vorsicht bei Protokolldateien

In nahezu allen ADV-Systemen werden Protokolldateien (Log-Dateien) zur Sicherstellung eines ordnungsgemäßen Betriebes der Datenverarbeitungsanlage geführt, in vielen auch zu Zwecken der Datenschutzkontrolle oder der Datensicherung. Diese Dateien sind in der Regel sehr umfangreich: In großen Systemen werden in diese Dateien innerhalb von 24 Stunden 200 000 bis 500 000 Sätze abgelegt, auch Mengen von einer Million in diesem Zeitraum sind keine Seltenheit. Der Inhalt der Protokolldateien ist sehr vielfältig: Es gibt Informationen über die vorhandene Konfiguration, über das Lesen und Beschreiben von Datenträgern, über das Starten und Beenden von Prozessen, über die Aktivitäten der Zentraleinheit (CPU). Es gibt Datenbankstatistiken, Informationen über das Benutzen von Schnittstellen, über die Aktivitäten des Operators und der Benutzer des Systems (User); der Aufbau ist insgesamt als komplex zu bezeichnen.

Die Aufzeichnungen in den Protokolldateien dienen überwiegend der Optimierung des Systems (Tuning) oder dem Zuordnen von Kosten des Systems auf

einzelne Benutzer (Account). Aus Protokolldateien, die für Zwecke der Datenschutzkontrolle oder der Datensicherung geführt werden, können Datenschutz- und IT-Sicherheitsbeauftragte sowie Revisoren Informationen entnehmen über

— bestimmte Dateien,

— bestimmte Programme und

— bestimmte Benutzer (User).

Anders als für die Zwecke Tuning oder Account stehen für die Auswertung der Protokolldateien zu den letztgenannten Zwecken kaum Werkzeuge zur Verfügung: Zwar gibt es Hilfsprogramme (Utilities, Monitore usw.) für die Auswertung der Dateien durch Systemadministratoren; diese sind jedoch für die Auswertung durch Datenschutz- und IT-Sicherheitsbeauftragte sowie Revisoren in aller Regel ungeeignet. Es kommt damit darauf an, Werkzeuge zu entwickeln, die für die Aufgabenstellung Datenschutz, IT-Sicherheit und Revision geeignet sind und es dem Anwender ermöglichen, mit vergleichsweise geringem Aufwand die vorhandenen Informationsmengen für seine Zwecke zu selektieren und auszuwerten.

Von den Behörden meines Zuständigkeitbereiches bin ich auf verschiedene Problempunkte hingewiesen worden, die sich im Zusammenhang mit dem Betrieb und der Nutzung von Protokolldateien ergeben haben. Insbesondere die folgenden beiden Punkte sind aus Datenschutzsicht hierbei von Bedeutung:

— Eine „Totalregistrierung" der Systemnutzer ist nicht nur bedenklich, sondern im allgemeinen auch nicht erforderlich. Sachgerecht sind „intelligente" Protokollierungsverfahren, in denen z. B. nur Zugriffe auf sensible Datenfelder oder die Aktivierung besonderer Programme registriert werden.

— Werden die Daten ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes der Datenverarbeitungsanlage gespeichert — wovon in der Regel auszugehen sein wird —, dürfen sie infolge der besonderen Zweckbindung des § 14 Abs. 4 und des § 31 BDSG auch nur für diese Zwecke verwendet werden. Insbesondere eine Verwendung für eine Verhaltens- und Leistungskontrolle der Benutzer des Systems ist unzulässig.

In einem Rundschreiben habe ich den obersten Bundesbehörden zur Lösung der angesprochenen Probleme praktische Hinweise gegeben (Anlage 14).

30.5 Datennetze können außer Kontrolle geraten — Sicherheit von Datennetzen —

„Downsizing", „Rightsizing", „Client-Server" und „Bürokommunikation" sind Begriffe, die der technische Wandel der zurückliegenden Jahre im Bereich der Datennetze hervorgebracht hat. Gemeint sind damit oftmals die Herauslösung von ADV-Verfahren aus den Abteilungsrechnern, Großrechnern oder Rechenzentren und die Verteilung dieser Anwendungen auf viele kleine, preiswerte Rechner wie APC sowie „Workstations" und deren zunehmende Vernetzung zu einem lokalen Netzwerk (LAN) oder Stadtbezirksnetz (MAN), schließlich sogar die Vernetzung mehrerer lokalen Netzwerke und Rechner zu einem Weitverkehrsnetz (WAN). Die bekannten Netzstrukturen und Prinzipien (vgl. 7. TB Anlage 1 S. 98ff.) bleiben zwar erhalten, die Anzahl der (kleineren) Rechner nimmt aber erheblich zu.

Entsprechend dem technischen Fortschritt werden immer mehr *Terminals durch APC ersetzt* und als Arbeitsplatz („Workstation") in das Netzwerk integriert. Die vorhandenen Groß- und Abteilungsrechner arbeiten zwar weiter, dienen aber in den meisten Fällen nur noch als Programm- und Datenspeicherungsstation (Server) für die Workstations (Clients); die Verarbeitung der Daten findet in den Workstations statt. Die vernetzten Stationen können dabei — z. T. über sehr große Entfernungen — auf die Datenbestände der Server zugreifen. Alle wichtigen Programme und Informationen des Servers sind dann oftmals für alle Arbeitsstationen im Netz frei zugänglich.

Die technisch unproblematische und kostengünstige Vernetzung läuft jedoch oft Gefahr, schnell außer Kontrolle zu geraten: Hier eine weitere „Workstation", dort noch ein Drucker und schließlich noch eine weitere „Applikation", mit der alles „schneller, schöner und leichter" läuft und die immer mehr Nutzern das Arbeiten im Netz ermöglicht. Auch wenn der Zugriff auf die meisten Daten nur mit einem Paßwort möglich ist, enthält ein Netz doch zahlreiche Hard- und Software-*Schwachstellen*, an denen — unabsichtlich aber auch absichtlich — Daten unberechtigt verändert, gelöscht oder kopiert werden können.

Hier ist der Weg offen für Manipulation, unberechtigten Zugriff oder Zerstörung von Daten und zwar in der Regel, ohne daß es sofort auffällt oder Spuren des Verursachers erkennbar sind (vgl. auch o. 30.4). Ein Kopiervorgang vom Server zur Workstation ist schnell durchgeführt, und schon sind die Daten, die eigentlich nicht in das Arbeitsgebiet fallen, auf der lokalen Arbeitsstation verfügbar oder — noch schlimmer — auf eine Diskette kopiert und damit unberechtigtem Zugriff ausgesetzt.

Aber auch ein „schwarz" kopiertes Programm, das im Netz „nur schnell einmal ausprobiert" werden soll, kann zu Schäden führen: Oftmals kommen mit solchen Raubkopien auch Computerviren oder andere schädliche Programme ins Netz — die Folgen sind hinlänglich bekannt. Ungeschulte oder frustrierte Mitarbeiter kopieren ganze Datenbestände auf die Festplatte des APC, um sie zu verändern (bewußt oder unbewußt) und wieder auf den Server zurückzutransferieren. Dort wieder angelangt, lösen sie u. U. ein „Datenchaos" aus. Solche Verhaltensweisen haben natürlich erhebliche Konsequenzen für den Datenbestand des Netzwerkes.

Um dies alles zu verhindern, rate ich seit längerem, APC ohne Diskettenlaufwerk und bei Anwendungen mit sehr sensiblen Daten auch ohne Festplatte einzusetzen. Mittlerweile gehören solche „Diskless Workstations" zum Produktangebot eines jeden APC-Her-

stellers. Weitere Sicherheitsmaßnahmen sind Tastaturverriegelung, Dunkelschaltung des Bildschirms und Verriegelung der lokalen Festplatten durch den Netzwerkadministrator.

Eine weitere Schwachstelle in Datennetzen ist die Anbindung an die öffentlichen Datennetze der Telekom, die insbesondere die „Hacker"-Gefahr mit sich bringt; ich berichtete bereits im 9. Tätigkeitsbericht darüber (vgl. 9. TB S. 72ff.). Um das Eindringen der Hacker in das Netzwerk zu verhindern, rate ich, Modems (Geräte zur Anschaltung eines Rechners an eine öffentliche Datenleitung), die über ein Zugriffskontrollsystem verfügen, vermehrt einzusetzen. Der Anrufer, der in das abgesicherte Computersystem eindringen will, muß dann im Besitz eines Schlüssels (Codewort, Paßwort) sein, damit er auf das Netzwerk und/oder den Rechner zugreifen kann.

Die in den letzten Jahren erstellten Sicherheitskonzepte berücksichtigen im Bereich des Netzwerks immer noch zu wenig das von Fachleuten favorisierte „Zwiebel"-Modell: Die Zwiebel mit ihren vielen Schichten sollte jedem Netzwerk als Vorbild dienen, um durch mehrere übereinanderliegende und einander verstärkende Sicherheitsmaßnahmen der Datensicherheit gerecht zu werden. Wird gewollt oder ungewollt eine Sicherheitsbarriere durchstoßen, sichert ein weiterer „Schutzwall" die Daten. Dazu sind vermehrt Aufklärung und Schulung der Anwender notwendig, da Sicherheitsbarrieren von ihnen oftmals als Arbeitshindernis empfunden werden.

Die Bemühungen des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) zur Bereitstellung von Verschlüsselungsverfahren auch außerhalb des VS-Bereichs kann ich gerade für den Bereich der Datennetze nur begrüßen (s. o. 30.3). Diese Verfahren werden wegen der zunehmenden Vernetzung der APC dringend benötigt, um auch für Netzwerke ausreichende Datensicherheit herstellen zu können.

30.6 Beauftragter für die Sicherheit in der Informationstechnik (IT-Sicherheitsbeauftragter) mit nur schwer zu vereinbarenden Funktionen

Das Bundesministerium des Innern bereitet gegenwärtig in Abstimmung mit den Ressorts eine Empfehlung zur Einrichtung der Funktion eines IT-Sicherheitsbeauftragten sowohl bei den obersten Bundesbehörden als auch — nach deren Vorgaben — im nachgeordneten Bereich vor.

Angesichts der ständig wachsenden Abhängigkeit der Bundesverwaltung von Informationstechnik ist dies sehr zu begrüßen, zumal mit den Bemühungen um IT-Sicherheit, wie sie von den IT-Richtlinien der Bundesregierung (GMBl. 4. Oktober 1988 S. 470ff.) gefordert werden, auch Erfordernissen der Datensicherung i. S. des § 9 BDSG entsprochen wird. In meiner Praxis zeigt sich immer wieder, daß das Niveau der Datensicherung sich alsbald verbessert, wenn ein dafür Verantwortlicher benannt wird. Man kann folglich auch davon ausgehen, daß die beabsichtigte Empfehlung zu einer allgemeinen Erhöhung der IT-Sicherheit führen wird.

Zu betonen ist allerdings, daß auch das entsprechende Personal bereitgestellt werden muß: Nach meiner Erfahrung ist die Personalsituation gerade im IT-Bereich teilweise so angespannt, daß die IT-Sicherheit nicht in dem erforderlichen Ausmaß realisiert werden kann. Eine bloße Empfehlung ohne entsprechende Personalbereitstellung, z. T. auch Personalvermehrung, dürfte daher nicht den gewünschten Erfolg haben.

Die Empfehlung sieht vor, daß folgende Funktionen zusammengefaßt werden können:

— IT-Koordinator (soweit nicht zugleich für den IT-Betrieb zuständig),

— Datenschutzbeauftragter,

— DV-Geheimschutzbeauftragter,

— COMSEC-Beauftragter.

Der DV-Geheimschutzbeauftragte untersteht aber nach den „Richtlinien für den Schutz von Verschlußsachen in der automatisierten Datenverarbeitung (Richtlinien für Daten-VS)" dem Geheimschutzbeauftragten. Gleiches gilt nach den „VS-Fernmelderichtlinien" in der Regel für den COMSEC-Beauftragten. Bei einer Zusammenlegung der Funktionen IT-Sicherheitsbeauftragter, DV-Geheimschutzbeauftragter und/oder COMSEC-Beauftragter mit der Funktion Datenschutzbeauftragter unterstünde der Funktionsträger teilweise dem Geheimschutzbeauftragten. Damit wären Interessenkonflikte unvermeidlich. Zwar wird eine solche Funktionszusammenfassung nicht ausdrücklich empfohlen, sondern nur als „in Betracht kommend" bezeichnet; aber auch dies ist problematisch. Ich habe den BMI daher darauf hingewiesen, daß insoweit eine Funktionstrennung dringend geboten erscheint.

Das BMI hat daraufhin mitgeteilt, daß es bei der laufenden Novellierung der VS-Vorschriften eine *Zusammenarbeitsregelung* — und kein Unterstellungsverhältnis — zwischen dem IT-Sicherheitsbeauftragten und dem Geheimschutzbeauftragten anstrebe. Sobald entsprechende Entwürfe vorliegen, wird zu prüfen sein, ob meine Besorgnisse entkräftet werden können.

30.7 Private Arbeitsplatzcomputer entfernt — APC-Einsatz bei der Deutschen Bundesbahn —

In meinem 13. Tätigkeitsbericht (S. 82) habe ich dem zentralen Systemdienst der Deutschen Bundesbahn empfohlen, sich des Einsatzes von Arbeitsplatzcomputern auf Bahnhöfen anzunehmen, damit die bestehenden Regelungen für Datenschutz und Datensicherheit auch hier eingehalten werden. Ich habe es begrüßt, daß die Deutsche Bundesbahn sowohl meinem generellen Anliegen als auch den vorgetragenen Verbesserungsvorschlägen positiv gegenüber stand und auch ihre Absicht erklärt hat, verstärkt Kontrollen zur Datensicherheit bei den Außendienststellen

durchzuführen, um die Mitarbeiter dort für die Problematik zu sensibilisieren. Gerade letzteres halte ich für besonders wichtig, da nach meiner Erfahrung in der Praxis Regelungen zum Datenschutz am besten durchsetzbar sind, wenn das Datenschutzbewußtsein der Mitarbeiter gezielt entwickelt wird. Bei der Deutschen Bundesbahn ist dies anscheinend noch nicht überall gelungen, denn im Berichtszeitraum wurde noch immer gegen Datenschutzvorschriften verstoßen:

Von Bediensteten der Deutschen Bundesbahn ist mir berichtet worden, daß trotz gegenteiliger Weisung häufig private APC für dienstliche Zwecke in Dienststellen der Deutschen Bundesbahn eingesetzt werden. Dies stellte ich auch bei der Kontrolle eines Bahnhofes fest. Es ergab sich, daß hier sowohl Daten aus dem privaten Umfeld des Eigentümers als auch dienstliche Informationen — darunter eine Datei aller Mitarbeiter des Bahnhofs — gespeichert waren. Die Verwendung dieses privaten APC wurde damit begründet, daß die Kapazität der dienststelleneigenen DV-Technik nicht mehr ausreiche und deshalb der Zeitraum bis zur (bereits zugesagten) Bereitstellung eines dienstlichen APC überbrückt werden solle.

Die beschriebene Nutzung widerspricht der Dienstanweisung der Deutschen Bundesbahn (114/2 Datenschutzanweisung) und wäre nach § 25 Abs. 1 BDSG zu beanstanden gewesen. Die Deutsche Bundesbahn hat jedoch nicht nur die gespeicherten Daten vorher gelöscht und das betreffende Gerät entfernt, sondern auch mit einer Bekanntmachung in ihrem Amtsblatt alle Dienststellenleiter angewiesen sicherzustellen, daß die Datenschutzanweisung beachtet wird und damit auch der Einsatz privater APC unterbleibt. Eine stichprobenweise Kontrolle der Einhaltung dieser Regelung wurde zugesagt. Ich habe daher nach § 25 Abs. 2 BDSG vorerst von einer Beanstandung abgesehen.

30.8 Automatisierte Abrufverfahren bedürfen besonderer Sicherheitsvorkehrungen

Für die Lösung zahlreicher, wichtiger Verwaltungsaufgaben — insbesondere im Bereich der inneren Sicherheit — ist es erforderlich, daß ein großer, zentral geführter Datenbestand einer Vielzahl von Stellen bundesweit für Auskünfte zur Verfügung steht. Sowohl Aufbau, Pflege und Sicherung des Datenbestandes als auch die Kontrolle der Abrufe durch die Nutzer erfordern den Einsatz modernster Informationstechnik. Ein typisches Beispiel hierfür ist die Ermittlung der Halter von Kraftfahrzeugen durch Polizeidienststellen mittels einer automatisierten Abfrage beim Zentralen Verkehrsinformationssystem ZEVIS des Kraftfahrt-Bundesamtes.

Wesentliches Merkmal automatisierter Abrufverfahren ist das Moment der „Selbstbedienung": Zwar ist das gesamte Verfahren unter Berücksichtigung der rechtlichen Vorgaben — insbesondere der Zulässigkeit der betreffenden Datenübermittlungen — gestaltet; der einzelne Abruf wird jedoch von der speichernden Stelle nicht mehr kontrolliert, so daß grundsätzlich die Möglichkeit besteht, daß die berechtigten Stellen Abrufe vornehmen, die im Einzelfall nicht zulässig sind oder deren Umfang über das berechtigte Maß hinausgeht. Diesen Risiken hat der Gesetzgeber durch Aufnahme des § 10 in das neue Bundesdatenschutzgesetz entgegenwirken wollen. Er hat den beteiligten Stellen Pflichten auferlegt, die eine Kontrollierbarkeit der Zulässigkeit des Abrufverfahrens gewährleisten sollen. Ist eine öffentliche Stelle des Bundes beteiligt, ist der Bundesbeauftragte für den Datenschutz über die getroffenen Maßnahmen zu informieren. Nach der zum 1. Dezember 1992 in Kraft getretenen Vorschrift muß die speichernde Stelle auch gewährleisten, daß die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann.

Da mich zahlreiche Anfragen erreicht haben, wie die Vorschrift praktisch umzusetzen ist, habe ich in Abstimmung mit dem Bundesminister des Innern „Hinweise zu automatisierten Abrufverfahren i. S. § 10 BDSG" formuliert und sie den obersten Bundesbehörden zugeleitet.

Sie sind in der Anlage 15 abgedruckt.

30.9 Zugangssicherung sollte nach Wartungsarbeiten überprüft werden

Die zentral im Ausländerzentralregister (AZR) gespeicherten sensiblen personenbezogenen Daten von Ausländern (s. auch 4.1) verlangen auch besondere Schutzmaßnahmen technischer und organisatorischer Art. Diesen Anforderungen entspricht das beim Bundesverwaltungsamt eingerichtete elektronische Zugangssystem, das bestimmte Bereiche wie z. B. die Räume des AZR und des Rechenzentrums besonders schützt. Die Türen sollen nur von den jeweils dort Beschäftigten mit einer entsprechend codierten Magnetkarte geöffnet werden können. Bei einer am Tage nach Durchführung von Wartungsarbeiten durch die mit der Wartung beauftragen Firma von mir durchgeführten Kontrolle habe ich allerdings festgestellt, daß sich auch diese Türen mit Magnetkarten ohne besondere Zugangsberechtigung, die allen Mitarbeitern des BVA den Zugang in die Behörde gewähren, öffnen ließen. Ich habe das Bundesverwaltungsamt sofort auf diesen Mangel aufmerksam gemacht; das BVA hat erfreulicherweise unverzüglich für Abhilfe dieses bei den Wartungsarbeiten erzeugten Fehlers gesorgt. Meine Kontrolle hat darüber hinaus bewirkt, daß das BVA nach Wartungsarbeiten zukünftig die ordnungsgemäße Funktion der Sicherheitsvorkehrungen unverzüglich mit eigenen Mitteln überprüfen wird.

31 Entwicklung des allgemeinen Datenschutzrechts

31.1 Erste Erfahrungen mit dem neuen BDSG

Das neue Bundesdatenschutzgesetz enthält — besonders im öffentlichen Bereich — eine Reihe von erfreulichen Verbesserungen (13. Tätigkeitsbericht S. 6 und

85 ff). Im großen und ganzen hat sich das neue Gesetz nach meiner Erkenntnis auch in der Praxis bewährt.

Allerdings konnte es nicht ausbleiben, daß sich in der praktischen Anwendung der neugefaßten Vorschriften auch Schwierigkeiten zeigten, die nicht unbedingt vorhersehbar waren.

Hierzu gehört die Vorschrift über die Kontrolle durch den Bundesbeauftragten für den Datenschutz in § 24 Abs. 2 Sätze 4 und 5 BDSG. Danach unterliegen bestimmte Daten — vor allem aus den Bereichen Post- und Fernmeldegeheimnis, Arztgeheimnis und Personalaktenwesen — nicht der Kontrolle des Bundesbeauftragten, wenn der Betroffene hiergegen Widerspruch einlegt. Die öffentlichen Stellen haben — unbeschadet des Kontrollrechts — die Betroffenen in allgemeiner Form über das Widerspruchsrecht zu unterrichten. Ich habe im Gesetzgebungsverfahren dieser Regelung nicht widersprochen, obwohl sie mir schon damals problematisch erschien, da ich auch in diesem Fall das informationelle Selbstbestimmungsrecht des Betroffenen respektieren wollte. Inzwischen muß ich feststellen, daß die praktischen Erfahrungen mit dieser Regelung keineswegs gut sind. Bei meiner Dienststelle sind bis jetzt rd. 3 000 Widersprüche eingelegt worden. Sie stammen praktisch nur von Angehörigen des öffentlichen Dienstes, eigentümlicherweise fast nur aus den Bereichen Verteidigung und Deutsche Bundespost. Die Zahl ist relativ gesehen außerordentlich klein, weil sich aus dem Bereich des öffentlichen Dienstes nur etwa jeder Tausendste, von den übrigen Widerspruchsberechtigten (z. B. Inhabern von Fernmeldeanschlüssen) praktisch niemand zu einem Widerspruch veranlaßt sah. Andererseits ist die Zahl — absolut gesehen — groß genug, um einen erheblichen Verwaltungsaufwand zu verursachen. Ich war z. B. gezwungen, eine automatisierte Datei der Widersprecher einzurichten. Nennenswerte praktische Auswirkungen der Regelung auf meine Kontrolltätigkeit sind bisher nicht erkennbar. Vor Kontrollen von Unterlagen, bei denen ein Widerspruchsrecht in Betracht kommt, wird die Datei der Widerspruchsführer abgefragt. Einen Treffer gab es bisher noch nicht.

Viele Widersprüche resultieren im übrigen offensichtlich aus ganz falschen Vorstellungen der Betroffenen. Diese wiederum beruhen auf einer höchst unzulänglichen, oft eher irreführenden Unterrichtung durch die speichernden öffentlichen Stellen. Nur so läßt sich die Häufung von Widersprüchen in den Bereichen der Verteidigung und der Deutschen Bundespost erklären. Aus Anfragen Betroffener war oft zu entnehmen, daß sie den BfD für eine weitere staatliche Stelle hielten, die ihre personenbezogenen Daten kontrollieren will. Als ich klargestellt hatte, daß ich die Behörden darauf kontrolliere, ob sie die Rechte der Bürger beachten, haben viele Betroffene ihren Widerspruch zurückgenommen.

Die Bestimmungen über das Kontrollrecht in den Bereichen Post- und Fernmeldegeheimnis, Arztgeheimnis und Personalaktenwesen sowie über den Widerspruch dagegen, gelten nicht nur für den Bundesbeauftragten sondern gem. § 24 Abs. 6 BDSG auch für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind. Einige Länder haben zunächst bezweifelt, ob diese Vorschrift verfassungskonform ist. Ein Normenkontrollverfahren vor dem Bundesverfassungsgericht wurde allerdings nicht veranlaßt. Andere Länder, vor allem Hamburg, gehen davon aus, daß die Vorschrift des § 24 Abs. 6 BDSG wegen § 1 Abs. 2 Ziff. 2 BDSG nicht in den Ländern gilt, in denen der Datenschutz durch Landesgesetz geregelt ist. Obwohl ich selbst die Vorschrift auf Grund der gewonnenen Erfahrungen durchaus kritisch sehe, halte ich diese Auslegung nicht für richtig. § 24 Abs. 6 BDSG enthält Bundesrecht, das nicht unter Vorbehalt landesrechtlicher Regelung steht und daher entgegenstehendes Landesrecht bricht (Artikel 31 GG). Die Vorschrift des § 24 Abs. 2 BDSG eröffnet den Landesdatenschutzbeauftragten die Kontrolle in Bereichen, in denen bundesrechtlich begründete Geheimnisse einer Kontrolle sonst entgegenstünden. Da diese Freistellung ausdrücklich auf den Kontrollbereich der Landesdatenschutzbeauftragten erstreckt wird, muß insofern auch das damit zusammenhängende Widerspruchsrecht gelten. Aus diesem Grunde ist meiner Ansicht nach der § 24 Abs. 6 BDSG eine Spezialregelung, auf die sich die Subsidiaritätsregelung des § 1 Abs. 2 Ziff. 2 BDSG nach ihrem Sinn und Zweck nicht bezieht.

Probleme haben sich auch bei der Auslegung des § 2 BDSG ergeben, vor allem bei der Frage, welche Vereinigungen des privaten Rechts öffentliche Stellen des Bundes sind. Das neue BDSG faßt in § 2 Vorschriften über die Legaldefinition der vom Gesetz angesprochenen Stellen zusammen, die vorher auf verschiedene Paragraphen verteilt waren. Nach der Begründung zum Regierungsentwurf sollte die Begriffsbestimmung in Absatz 1 (öffentliche Stellen des Bundes) keine materiellen Änderungen zum bisherigen Recht beinhalten.

Ich habe mich eingehend mit der Vorschrift befaßt, insbesondere mit dem ersten Absatz, um meine Kontrollpflichten im Rahmen des neuen BDSG auch korrekt wahrzunehmen. Die Neufassung hat eine Präzisierung mit sich gebracht. Die Rechtslage hat sich zwar gegenüber dem alten BDSG nicht grundlegend geändert. Der neugefaßte Gesetzestext führt aber zu Klarstellungen, aus denen sich durchaus praktische Konsequenzen ergeben.

Eindeutig ist nach wie vor die Rechtslage im öffentlich-rechtlichen Organisationsbereich des Bundes (Behörden, Organe der Rechtspflege, andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, bundesunmittelbare Körperschaften usw.). Neben diesen Behörden und Einrichtungen bezieht die Vorschrift des § 2 Abs. 1 BDSG auch „deren Vereinigungen" mit ein und zwar „ungeachtet ihrer Rechtsform". Das Gesetz will also auch und gerade privatrechtlich organisierte Vereinigungen als öffentliche Stellen des Bundes miterfassen. Diese Vorschrift ist in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und im Düsseldorfer Kreis intensiv diskutiert worden. Zusammen mit den meisten Datenschutzbeauftragten der Länder und der Mehrheit der im Düsseldorfer Kreis vertretenen Aufsichtsbehörden lege ich sie wie folgt aus: Mit „deren Vereinigungen" sind nicht nur Zusammenschlüsse von Behörden,

anderen öffentlich-rechtlich organisierten Einrichtungen, Körperschaften, Anstalten oder Stiftungen gemeint. Der Anwendungsbereich wäre bei solch engem Verständnis so minimal, daß die Vorschrift praktisch ins Leere liefe. Die Bestimmung soll die sog. „Flucht ins Privatrecht" verhindern; d. h. die strengen, für den Umgang des Staates mit personenbezogenen Daten und dessen Kontrolle geschaffenen Vorschriften sollen auch dann gelten, wenn der Staat sich privatrechtlicher Organisationsformen bedient. Sie kann deshalb nur so verstanden werden, daß der hinter den Behörden stehende Rechtsträger, nämlich der Bund selbst, ebenfalls Beteiligter in einer Vereinigung sein kann.

Der Begriff der Vereinigung umfaßt z. B. Vereine, Personengesellschaften (wie die BGB-Gesellschaft, die OHG und KG) wie auch Kapitalgesellschaften (wie AG und GmbH). Voraussetzung für eine Einstufung als öffentliche Stelle ist, daß der Bund eine beherrschende Stellung hat. Es können also auch andere, nicht-öffentliche Stellen beteiligt sein. Soweit an der Vereinigung auch Stellen der Länder beteiligt sind, legt die neue Sondervorschrift für Bund-Länder-Mischvereinigungen (§ 2 Abs. 3 BDSG) fest, in welchen Fällen es sich um eine Bundes- oder Landesstelle handelt. Wenn der Bund die beherrschende Stellung in einer privatrechtlichen Vereinigung innehat, so muß als weitere Voraussetzung hinzutreten, daß die Vereinigung im weitesten Sinne an der Erfüllung einer öffentlichen Aufgabe teilnimmt. Dabei kommen alle Aufgaben des Bundes in Betracht, auch die Mitwirkung an Hilfs-, Neben- und Servicefunktionen.

Ausgehend von dieser Gesetzesauslegung sind aus meiner Sicht einige privatrechtlich organisierte Vereinigungen als öffentliche Stellen des Bundes anzusehen, die unter der Geltung des alten BDSG für nicht-öffentliche Stellen gehalten wurden und deshalb durch die Aufsichtsbehörden der Länder kontrolliert wurden. Hierzu gehört z. B. die Deutsche Postreklame GmbH; mit dem bisher für die datenschutzrechtliche Kontrolle dieser Gesellschaft zuständigen Hessischen Minister des Inneren bin ich einig, daß jetzt der Bundesbeauftragte für den Datenschutz insoweit das zuständige Kontrollorgan ist. Die Deutsche Bundespost — TELEKOM bestreitet meine Zuständigkeit. Ich bemühe mich derzeit um eine Klärung im Einvernehmen mit den zuständigen Bundesressorts.

Erstmalig hat der Bundesgesetzgeber die Zulässigkeit automatisierter Abrufverfahren geregelt (s. auch 30.8). Die Vorschrift (§ 10 BDSG) steht im ersten Abschnitt des Gesetzes, gilt also für öffentliche wie für nicht-öffentliche Stellen. Mich hat vor allem die Frage beschäftigt, wie die im Gesetz vorgesehene Protokollierung der Abrufe zu erfolgen hat und wie die vorgeschriebenen Stichprobenverfahren (§ 10 Abs. 4 Satz 3 und 4 BDSG) gestaltet werden. Der Gesetzgeber hat, um den Behörden und Stellen Zeit für die Einführung der Stichprobenverfahren zu lassen, diese Regelung erst mit 1½-jähriger Verzögerung zum 1. Dezember 1992 in Kraft gesetzt. Die Protokollierung der Abrufe erfolgt nicht zwangsläufig als Vollprotokollierung aller Benutzeraktivitäten. Eine solche kann wegen des damit verbundenen Aufwandes unter Berücksichtigung des Grundsatzes der Angemessenheit (§ 9 Satz 2 BDSG) nur für besonders schutzbedürftige Systeme in Betracht kommen. Die Protokollierung der Abrufe aus weniger schutzbedürftigen Systemen erfolgt stichprobenweise, wobei sich die Stichproben auf Zeiträume, bestimmte Benutzer oder Benutzergruppen, Daten, Dateninhalte oder Ereignisse beziehen können. Die Protokollierung muß nicht in Papierform vorliegen, ein Ablegen auf elektronischen Datenträgern ist ausreichend. Eine einjährige Aufbewahrung wird in der Regel ausreichen. Für alle Protokolldateien gilt die besonders strenge Zweckbindung des § 14 Abs. 4 und des § 31 BDSG; personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

„Geeignete Stichprobenverfahren" sollten flexibel und situationsangepaßt sein. Sie müssen nicht statistisch repräsentativ für den Gesamtbereich sein. Auch eine Auswahl nach bestimmten sachbezogenen Gesichtspunkten kann der Lage angemessen sein. Zugangsberechtigte dürfen sich allerdings nicht darauf verlassen können, daß bestimmte Arten von Abrufen nie oder nur mit äußerst geringer Wahrscheinlichkeit protokolliert werden. Noch wichtiger ist, daß keine Datenfriedhöfe produziert werden. Die speichernden Stellen müssen sich durch zielgerichtete Auswertung der Protokolle vergewissern, daß keine mißbräuchlichen Zugriffe erfolgen. Erst in zweiter Linie dient die Protokollierung der externen Kontrolle durch den BfD und die Aufsichtsbehörden des nicht-öffentlichen Bereichs. Protokolle sind kein Selbstzweck, sondern wegen der im automatisierten Abrufverfahren möglichen Daten-Selbstbedienung notwendiges Instrument einer begleitenden Selbst- und Fremdkontrolle.

31.2 Datenschutz im Grundgesetz

Der Deutsche Bundestag hat im November 1991 die Einsetzung einer gemeinsamen Verfassungskommission, bestehend aus Mitgliedern des Bundestages und des Bundesrates, beschlossen. Die Kommission hat aus Artikel 5 des Einigungsvertrages den Auftrag „sich mit den im Zusammenhang mit der deutschen Einigung aufgeworfenen Fragen zur Änderung oder Ergänzung des Grundgesetzes zu befassen".

Die lebhafte Debatte um eine Verfassungsreform, die nach dem Beitritt der ehemaligen DDR einsetzte, bezog auch die Frage mit ein, ob eine Verankerung des Datenschutzes als eigenständiges Grundrecht im Grundgesetz angestrebt werden soll, wie dies bereits in mehreren Landesverfassungen der Fall ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat mit Entschließung vom 28. April 1992 (s. Anlage 6) der Verfassungskommission einen entsprechenden Formulierungsvorschlag unterbreitet. Darüber hinaus hat die Konferenz empfohlen, auch die unabhängige Datenschutzkontrolle in der Verfassung zu verankern. Im Sinne dieser Empfehlung habe ich bei der Verfassungskommission angeregt, einen neuen Artikel 45d in das Grundgesetz

einzufügen, der die Wahl und die Rechtstellung des Bundesbeauftragten für den Datenschutz verfassungsrechtlich regeln sollte.

In der gemeinsamen Verfassungskommission ist diese Empfehlung beraten worden; sie hat jedoch nicht die für einen Vorschlag zur Grundgesetzänderung erforderliche Zweidrittelmehrheit gefunden. Ich bedauere dies und hoffe, daß damit nicht das letzte Wort gesprochen ist. Zwar besitzt der Datenschutz schon verfassungsrechtliche Qualität, wie das Bundesverfassungsgericht festgestellt hat, indem es aus dem allgemeinen Persönlichkeitsrecht des Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 Grundgesetz ein Recht auf informationelle Selbstbestimmung herleitet. Die jetzt bestehende Chance, dem Persönlichkeitsrecht und der Privatsphäre der Bürger eine noch klarere Verankerung zu geben, sollte man aber nicht ungenutzt verstreichen lassen. Der Datenschutz hat inzwischen eine hohe Akzeptanz und einen festen Stellenwert im Bewußtsein der Bürger. Ich bin deshalb sicher, daß die Aufnahme dieses Grundrechts in das Grundgesetz begrüßt würde, gerade angesichts der Erfahrungen aus vierzig Jahren staatlicher Bevormundung und Überwachung in der ehemaligen DDR. Es bliebe sonst auch wenig verständlich, daß „zum Schutz der Grundrechte" der Soldaten ausdrücklich ein Wehrbeauftragter Eingang in die Verfassung gefunden hat, nicht aber der Bundesbeauftragte für den Datenschutz, der für alle Bürger Aufgaben des Grundrechtsschutzes wahrnimmt.

In ihrer Sitzung am 16./17. Februar 1993 in Berlin hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ihre Empfehlung bekräftigt, die vorgeschlagene Verfassungsergänzung vorzunehmen.

31.3 Neues BDSG und Kirchen

Obwohl ich die Datenverarbeitung bei den Kirchen nicht zu kontrollieren habe, erreichen mich oft Anfragen oder Eingaben zu diesem Bereich.

Die Frage, an welche zuständige Stelle derartige Anliegen jeweils weiterzugeben sind, ist nicht immer einfach zu beantworten. Das neue BDSG hat die Antwort nicht erleichtert. Sein Schweigen zur Anwendbarkeit des Gesetzes auf öffentlich-rechtliche Religionsgesellschaften wird der streitigen Diskussion eher neuen Stoff liefern. Andere neuere Gesetze des Bundes enthalten demgegenüber eindeutige Bestimmungen über den Geltungsbereich bei Kirchen und deren Einrichtungen (vgl. z. B. § 2 Abs. 1 Verwaltungsverfahrensgesetz, § 118 Abs. 2 Betriebsverfassungsgesetz, § 112 Bundespersonalvertretungsgesetz). Der Regierungsentwurf hatte noch ausdrücklich vorgesehen, daß das Gesetz „für öffentlichrechtliche Religionsgesellschaften sowie die ihnen zugeordneten karitativen und erzieherischen Einrichtungen des öffentlichen Rechts" nicht gilt. Für die kirchlichen Einrichtungen des privaten Rechts enthielt der Regierungsentwurf eine Regelung, die eine stark eingeschränkte Geltung vorsah. Der Innenausschuß des Deutschen Bundestages hat diese vorgesehenen Regelungen ersatzlos gestrichen. Eine ausdrückliche Begründung für diese Entscheidung findet sich in den Gesetzesmaterialien nicht.

Da der Gesetzgeber in anderen Gesetzen eine Klarstellung vorgenommen hat, bedauere ich, daß dies beim Bundesdatenschutzgesetz nicht erfolgt ist.

So wird wohl weiter umstritten bleiben, ob das Bundesdatenschutzgesetz ein „für alle geltendes Gesetz" im Sinne des Artikel 140 Grundgesetz in Verbindung mit Artikel 137 III Abs. 1 Weimarer Reichsverfassung ist und ob in diesem Fall seine Anwendung nur auf die privatrechtlich strukturierten Einrichtungen der Kirchen beschränkt sein soll oder sich auch auf bestimmte Tätigkeiten und Aufgaben der Kirchen selbst erstreckt. In der Diskussion werden zwei Gesichtspunkte eine wichtige Rolle spielen: der durch das Bundesverfassungsgericht (Volkszählungsurteil 1983) festgestellte Verfassungsrang des Rechts auf informationelle Selbstbestimmung und die internationale Dimension, die sich aus der Datenschutzkonvention des Europarats und aus der geplanten Datenschutzrichtlinie der EG ergeben.

Ich bin stets davon ausgegangen, daß die Vorschriften der beiden großen Konfessionen[1]) einen ausreichenden Datenschutz gewährleisten, so daß die öffentlichen Stellen des Bundes nach § 15 Abs. 4 BDSG grundsätzlich personenbezogene Daten an die öffentlich rechtlichen Religionsgemeinschaften übermitteln dürfen.

Es ist allerdings an der Zeit, daß nun auch die Kirchen ihre Vorschriften den Anforderungen des Bundesverfassungsgerichtsurteils von 1983 und dem neuen Bundesdatenschutzgesetz anpassen. Mir ist bekannt, daß beide Kirchen an einer entsprechenden Anpassung arbeiten.

32 Nicht-öffentlicher Bereich

Im Rahmen des Düsseldorfer Kreises und seiner Arbeitsgruppen habe ich die praktische Anwendung des Datenschutzrechts im nicht-öffentlichen Bereich verfolgt und mich an der Diskussion über Einzelfragen, die auch meinen Bereich berührten, beteiligt.

32.1 Neues Bundesdatenschutzgesetz

In den Berichtszeitraum fällt vor allem die Anpassung an das neue Bundesdatenschutzgesetz. Soweit ich es beurteilen kann, haben sich im nicht-öffentlichen

[1]) a) Katholische Kirche in den Diözesen der Bundesrepublik Deutschland und in der Diözese Berlin für Berlin (West): „Anordnung über den kirchlichen Datenschutz — KDO", ab April 1978 in den einzelnen Diözesen in Kraft gesetzt
b) Evangelische Kirche in Deutschland: Kirchengesetz über den Datenschutz vom 10. November 1977 (ABl EKD 1978 Seite 2) in der Fassung vom 7. November 1984 (ABl EKD 1984 Seite 506)
beides abgedruckt bei Simitis/Dammann/Mallmann/Reh, Dokumentation zum Bundesdatenschutzgesetz, C 1.1

Bereich bei den datenverarbeitenden Stellen wie auch bei den Aufsichtsbehörden aus der Neufassung des Gesetzes keine grundlegenden Probleme ergeben. Dies ist auch nicht verwunderlich, da das Gesetz für den nicht-öffentlichen Bereich keine tiefer eingreifenden Änderungen mit sich gebracht hat. In den im Düsseldorfer Kreis diskutierten Fragen ging es deshalb mehr um die Auslegung einzelner gesetzlicher Bestimmungen, weniger um grundsätzliche Anpassungsschwierigkeiten. So hat sich dieses Gremium u. a. mit der Auslegung des Begriffs „geschäftsmäßig" (§ 1 Abs. 2 Nr. 3 und § 27 Abs. 1 BDSG) befaßt. Mit dem Düsseldorfer Kreis bin ich der Ansicht, daß es bei der bisherigen Auslegung des Begriffes bleibt, d. h., daß die auf Dauer oder Wiederholung angelegte Datenverarbeitung bzw. Nutzung gemeint ist. Gegenstand der Diskussion war mehrfach auch die Auslegung der Begriffe „öffentliche" und „nicht-öffentliche Stelle" und „Vereinigung" in § 2 BDSG. Die Aufsichtsbehörden teilen meine Rechtsauffassung zu § 2 BDSG (s. 31.1) nicht in allen Punkten. Schwierigkeiten bereitet bei der Auslegung des § 2 vor allem die Abgrenzung anhand des Kriteriums „Aufgaben der öffentlichen Verwaltung". In der Praxis, vor allem bei dem von mir erforderlich gehaltenen Übergang der Zuständigkeit für die datenschutzrechtliche Kontrolle in einigen Fällen sehe ich derzeit keine grundlegenden Differenzen mit den Aufsichtsbehörden.

Eine weitere Vorschrift des neuen BDSG, die den Düsseldorfer Kreis beschäftigt hat, ist der § 27 Abs. 2 BDSG, der die Anwendung der Vorschriften über den nicht-öffentlichen Bereich auf Dateien und auf Daten in Akten beschränkt, die „offensichtlich aus einer Datei entnommen worden sind". Der Begriff „offensichtlich" ist vor allem im Hinblick auf die heute gebräuchlichen Textverarbeitungssysteme nicht einfach auszulegen. Der Düsseldorfer Kreis neigt zu einer sehr engen Auslegung mit Blick darauf, daß § 27 Abs. 2 BDSG lediglich einer Umgehung des Bundesdatenschutzgesetzes entgegenwirken soll und der Anwendungsbereich des Dritten Abschnitts des BDSG weiterhin grundsätzlich auf den dateimäßigen Umgang mit personenbezogenen Daten beschränkt ist.

Da der nicht-öffentliche Bereich durch das neue BDSG keine wesentliche Weiterentwicklung erfahren hat, halte ich nach wie vor bereichsspezifische, den Datenschutz verstärkende Regelungen insbesondere in solchen Bereichen für erforderlich, in denen der Betroffene seinem Vertrags- oder Geschäftspartner nur formal, nicht aber wirklich gleichberechtigt gegenübertritt, wie dies bei Arbeitnehmern, bei Kreditnehmern oder Versicherten in der Privatversicherung der Fall ist. Bedarf für ergänzende bereichsspezifische Regelungen sehe ich auch, soweit Privatunternehmen sich für sensible Datenbereiche interessieren und Datenerhebungsmethoden anwenden, die erfahrungsgemäß die Privatsphäre der Betroffenen besonders berühren, Ich denke dabei insbesondere an Privatdetekteien und private Sicherheitsdienste. Es darf nicht sein, daß private Detekteien und Sicherheitsdienste Freiräume bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten genießen, die Polizeibehörden beim Umgang mit den gleichen Daten aus guten Gründen nicht zustehen.

32.2 Weitergabe von Patientendaten an Verrechnungsstellen nur mit Einwilligung

Zum Arzt/Patientenverhältnis hat es im Berichtszeitraum zwei wichtige höchstrichterliche Urteile gegeben. Seit längerem hat den Düsseldorfer Kreis die Frage beschäftigt, ob Ärzte Behandlungsunterlagen über ihre Patienten ohne deren Einwilligung an privatärztliche Verrechnungsstellen weitergeben dürfen. Die Bedenken dagegen wurden durch ein Urteil des Bundesgerichtshof vom 10. Juli 1991 (Az.: VII ZR 296/90, NJW 1991, 2955ff.) bestätigt. Danach hat der Arzt vor Weitergabe von Behandlungsunterlagen die Einwilligung des Patienten eindeutig und unmißverständlich einzuholen. Ein Aushang in den Praxisräumen reicht hierzu in der Regel nicht aus. In Fortführung dieser Rechtsprechung hat der BGH mit Urteil vom 11. Dezember 1991 (Az.: VIII ZR 4/91 NJW 1992, 737ff.) auch bei Praxisaufgabe die ausdrückliche Einwilligung der Patienten in die Übergabe seiner Daten an einen Praxisnachfolger für geboten gehalten. Ich habe gemeinsam mit dem Düsseldorfer Kreis die durch diese Urteile herbeigeführte Klärung begrüßt.

32.3 Fortschritte bei den Schweigepflichtenentbindungsklauseln, aber immer noch Unbehagen

Die Gespräche über die datenschutzgerechte Neufassung der Schweigepflichtentbindungsklauseln wurden im Berichtszeitraum zwischen den obersten Aufsichtsbehörden, dem Bundesaufsichtsamt für das Versicherungswesen und den Verbänden der Versicherungswirtschaft unter meiner Beteiligung weitergeführt. In den Bereichen Berufsunfähigkeitsversicherung/Pflegerentenversicherung hat man sich inzwischen auch auf neue, datenschutzgerechtere Klauseln geeinigt (s. o. 14.1 sowie Anlage 16; vgl. auch zu den Schweigepflichtentbindungsklauseln in der Kranken-, Unfall- und Lebensversicherung 11. TB, S. 79f. und 109f.). Gegenüber den früher üblichen pauschalen, unbefristeten Freistellungserklärungen stellen die Klauseln einen Fortschritt dar, da sie zumindest benennen, zu welchem Zweck welche Ärzte oder Krankenanstalten von der Schweigepflicht befreit werden sollen, und da sie insgesamt auf zehn Jahre befristet sind. Allerdings verhehle ich nicht, daß bei all diesen Entbindungsklauseln ein gewisses Unbehagen bleibt. Wenn auch niemand gezwungen wird, Versicherungsverträge abzuschließen, so ist doch der Kunde, der Wert auf einen solchen Vertrag legt, gegenüber den Versicherungsunternehmen in einer Position, die Zweifel an der wirklichen Freiwilligkeit der Einwilligung zumindest offenläßt. Derjenige, der die immer noch recht weitgehenden Schweigepflichtentbindungserklärungen nicht unterzeichnen will, hat praktisch keine Chance, einen Versicherungsvertrag zu erhalten.

Besser wäre sicherlich, wenn die Versicherungen eine Schweigepflichtentbindungserklärung in jedem Einzelfall einholten (s. meinen 8. Tätigkeitsbericht S. 54). Da dies angesichts des Verwaltungsaufwandes, der auch in die Versicherungsprämien zu Lasten der Betroffenen einfließen würde, in der Praxis nicht zu

erreichen war, muß man die jetzt gefundenen Lösungen vorläufig akzeptieren.

Ich halte es für erforderlich, daß der Gesetzgeber bei der unter Datenschutzgesichtspunkten ohnehin notwendigen Ergänzung des Versicherungsvertragsgesetzes eine gesetzliche Regelung dieses Problems ins Auge faßt.

32.4 Datenschutz ist auch bei electronic-cash erforderlich

Die Arbeitsgruppe „SCHUFA/Kreditwirtschaft" des Düsseldorfer Kreises hat sich eingehend mit den datenschutzrechtlichen Aspekten des sogenannten „electronic-cash-Verfahrens" beschäftigt, das im bargeldlosen Zahlungsverkehr immer mehr an Bedeutung gewinnt. Der Kunde zahlt mit Hilfe seiner Eurocheque-Karte, indem er die Karte und seine Geheimnummer in einen Kassenautomaten eingibt, der eine Autorisierungszentrale abfragt und in Sekunden die Mitteilung erhält, ob gezahlt werden kann. Andere modifizierte bargeldlose Zahlungsverfahren, die ebenfalls auf der Eurocheque-Karte beruhen, sogenannte Lastschriftverfahren, ersparen dem Kunden die Eingabe der Geheimnummer, in diesem Fall genügt seine Unterschrift.

Die Aufsichtsbehörden vertreten einmütig die Ansicht, daß bei diesen Verfahren personenbezogene Daten verarbeitet werden, auch wenn — z. B. bei den Autorisierungszentralen — offenbar nur die Bankleitzahl und das Bankkonto gespeichert werden. Ich halte diese Rechtsauffassung für richtig. Sie wird allerdings von der Kreditwirtschaft bestritten. Noch besteht in diesem Bereich ein erhebliches Transparenzdefizit: Kaum einer der Kunden, der per „electronic-cash" bezahlt, weiß, welche Datenverarbeitung bei welchen Stellen er damit auslöst und welche „Datenspuren" er hinterläßt. Datenschutzrechtliche Bedenken bestehen auch dagegen, daß die Ursache der fehlgeschlagenen Autorisierung dem Händler im einzelnen angezeigt wird. So kann er dem Fehlercode 13 entnehmen, daß der Kaufbetrag durch den freien Verfügungsrahmen nicht gedeckt ist. Eine Zusammenfassung dieses Codes mit anderen zu neutraleren Fehlmeldungen wäre weniger diskriminierend. Die Rechte der Betroffenen auf Benachrichtigung, Auskunft, Berichtigung und Löschung müssen in allen Verfahrensstadien des elektronischen Zahlungsvorganges beachtet werden. Um seine Rechte wahrnehmen zu können, muß der Kunde allerdings umfassend über den gesamten Weg der ihn betreffenden Daten unterrichtet sein.

Die Gespräche mit den Vertretern der Kreditwirtschaft über diese neuen, noch nicht ganz ausgeloteten Bereiche des Datenschutzes im bargeldlosen Zahlungsverkehr dauern noch an.

32.5 Datenübermittlung im Rahmen von Allfinanzkonzepten nur mit Einwilligung

Die Arbeitsgruppen Versicherungswirtschaft und Kreditwirtschaft des Düsseldorfer Kreises befassen sich zur Zeit mit den sog. „Allfinanz-Konzepten". In zunehmendem Maße arbeiten Versicherungsunternehmen mit Banken und Bausparkassen zusammen. Sie bilden Unternehmensgruppen, die sich gegenseitig personenbezogene Informationen zukommen lassen. Die Vertragsbeziehung zwischen einem Kunden und einem dieser Unternehmen ermöglicht es, die Kundendaten, die auch sehr sensibler Natur sein können, an andere Unternehmen, die an der Unternehmensgruppe beteiligt sind, zum Zweck der Kundenwerbung weiterzugeben. Dies kann zwar, muß aber durchaus nicht immer im Interesse des Kunden liegen. Daher muß er in eine derartige Übermittlung, die normalerweise nicht im Rahmen des Vertragsverhältnisses erfolgt und deshalb nicht auf § 28 Abs. 1 Nr. 1 BDSG gestützt werden kann, ausdrücklich einwilligen (§ 4 Abs. 2 BDSG).

Ziele der Verhandlungen, die zur Zeit mit den Vertretern der Versicherungswirtschaft geführt werden, sind eine umfassende Information des Kunden sowie die Ausarbeitung einer hinreichend konkreten und exakten Einwilligungserklärung, die auch folgenlos abgelehnt werden kann. Auch diese Gespräche sind noch nicht abgeschlossen. Die Versicherungswirtschaft hat ihre grundsätzliche Bereitschaft zu erkennen gegeben, die Vorstellungen der Datenschutzaufsichtsbehörden zu berücksichtigen.

33. Ausland und Internationales

Der internationale Datenschutz hat im Berichtszeitraum stark an Bedeutung gewonnen. Die Anzahl der Staaten, die ein Datenschutzgesetz haben oder ein solches vorbereiten, hat sich weiter vergrößert.

Schwerpunkt der praktischen Arbeit im internationalen Bereich war im Berichtszeitraum die Entwicklung innerhalb der Europäischen Gemeinschaft. Sie ist dadurch gekennzeichnet, daß die Beratung des Entwurfs einer Datenschutz-Richtlinie fortschreitet — allerdings langsamer als erwartet — und daß zugleich — mit größtem Nachdruck — am Aufbau europäischer Informationssysteme gearbeitet wird, so etwa für die Polizei (s. o. 24.1.2, 24.2.1 und 24.2.2), den Zoll (s. o. 26.3) und die Umsatzsteuer (s. o. 6.5 sowie insgesamt unten 33.4). Es ist offensichtlich, daß es dabei zu unkoordinierten Entwicklungen kommen kann, die den Datenschutz gefährden. In dieser Situation hat es sich als sehr günstig erwiesen, daß meine europäischen Kollegen und ich bei der Entwicklung des Schengener Informationssystems darauf bestanden haben, nur Länder mit einem vollentwickelten Datenschutz am Informationsverbund teilnehmen zu lassen. Dies erlaubt es, heute allen Versuchen entgegenzutreten, bei den neuen Projekten hinter das Schengener Niveau zurückzugehen.

Für meine Dienststelle werfen die zunehmenden internationalen Aufgaben gravierende haushaltsmäßige und personelle Probleme auf. Der Datenschutz muß sich aber gerade in diesen Jahren mit aller Kraft in die internationalen Entwicklungen einschalten, weil sonst Fehlentwicklungen drohen, die auf lange Zeit nicht zu korrigieren wären. Ich hoffe deshalb sehr, bei Regierung und Parlament die notwendige Unterstützung zu finden.

33.1 Entwicklung des Datenschutzes im Ausland

Nachdem in Portugal, Spanien und Belgien Datenschutzgesetze verabschiedet worden sind, sind Italien und Griechenland die letzten weißen Flecken auf der EG-Datenschutzlandkarte. Auch außerhalb der EG ist die Entwicklung weiter gegangen. Die Schweiz, Ungarn und die Tschechoslowakei haben Datenschutzgesetze erlassen; das Gesetz für die ehemalige Tschechoslowakei gilt nach der Teilung des Landes in beiden Republiken weiter.

Es ist zu begrüßen, daß Portugal, Spanien und Belgien sich entschlossen haben, nicht die Verabschiedung der EG-Datenschutzrichtlinie abzuwarten, sondern ihre Datenschutzgesetze zu verabschieden, sobald dies möglich war, und später notwendig werdende Korrekturen in Kauf zu nehmen. Dies entspricht dem Schutzbedürfnis der Betroffenen, mittelbar aber auch dem Datenverarbeitungsinteresse der betreffenden Länder, da eine Teilnahme an europäischen Informationssystemen entsprechend den Schengener Grundsätzen nur für Länder möglich ist, die über ein funktionierendes Datenschutzsystem verfügen.

Bemerkenswert ist auch die Entwicklung im pazifischen Raum, wo nach Australien und Japan inzwischen auch Neuseeland ein Datenschutzgesetz besitzt und andere Länder, wie Singapur und Hongkong, mit entsprechenden Vorarbeiten befaßt sind.

33.2 Internationale Zusammenarbeit der Datenschutz-Kontrollinstanzen

Die Zusammenarbeit mit Partnereinrichtungen anderer Länder auf globaler Ebene hat ihren Schwerpunkt weiterhin in jährlichen, an wechselnden Orten stattfindenden Konferenzen. Im Herbst 1991 hat aus Anlaß des 10jährigen Bestehens der Datenschutzkonvention des Europarats dessen Generalsekretärin die XIII. Internationale Konferenz der Datenschutzbeauftragten in den Räumen des Europarats in Straßburg empfangen. Die Konferenzthemen gruppierten sich entsprechend dieser besonderen Situation vor allem um die Verbindungen zwischen den Menschenrechten im allgemeinen und dem Datenschutz im besonderen, wie er sich in Gesetzen und anderen Regelwerken, in der gerichtlichen Spruchpraxis und in Entscheidungen der Datenschutzbeauftragten widerspiegelt. Außerdem ging es um das Aufzeigen der Wirkungsgeschichte der Datenschutzkonvention des Europarats und seiner Empfehlungen in der Datenschutzgesetzgebung innerhalb und außerhalb Europas. Die Mitglieder der deutschen Delegation hielten Referate über die Regelungen zum Umgang mit der Datenerbschaft der Staatssicherheit, den Datenschutz im Arbeitsverhältnis und Vertragsregelungen zum grenzüberschreitenden Datenverkehr.

Die XIV. Internationale Konferenz fand auf Einladung des australischen Privacy Commissioner im November 1992 in Sydney statt. Themen der Konferenz waren u. a. der Datenschutz im pazifischen Raum, der Umgang mit genetischen Daten und die Praxis des Datenschutzes in Ämtern und Unternehmen. Die deutsche Delegation steuerte Referate über die praktischen Erfahrungen beim Umgang mit den Stasi-Unterlagen, über die Arbeitsweise von Datenschutz-Kontrollinstanzen und über Gesundheitskarten bei. Auf der Grundlage eines Arbeitsgruppenberichts zu aktuellen Fragen der Telekommunikation unterstrich die Konferenz in einem einmütig gefaßten Beschluß die Bedeutung des Fernmeldegeheimnisses in der Telekommunikation einschließlich der Satellitenkommunikation und die Notwendigkeit seines Schutzes gegen eine exzessive Überwachung (Wortlaut abgedruckt in Anlage 17).

In der Europäischen Gemeinschaft haben sich im Berichtszeitraum feste Formen der Zusammenarbeit zwischen den Datenschutzbeauftragten herausgebildet. Die Konferenz der Datenschutzbeauftragten der Mitgliedstaaten der Gemeinschaft trifft sich regelmäßig, meist am Amtssitz desjenigen Kollegen, dessen Land gerade die Präsidentschaft im Ministerrat inne hat. Daneben finden Treffen auch an zentralen Orten, überwiegend in Brüssel, statt. Ganz im Mittelpunkt der Beratungen stand in den letzten beiden Jahren das Projekt einer EG-Datenschutzrichtlinie. Daneben wurden auch bereichsspezifische Angelegenheiten behandelt, so insbesondere der Aufbau europäischer Informationssysteme.

Neben der allgemeinen Zusammenarbeit hat die Entwicklung spezifischer Kooperationsformen in einzelnen Sektoren eingesetzt. So hat sich im Berichtszeitraum auf der Grundlage des Schengener Durchführungsübereinkommens (Artikel 115) eine aus den Datenschutzinstanzen der Vertragsstaaten zusammengesetzte — zunächst provisorische — gemeinsame Kontrollinstanz gebildet, die den Aufbau des technischen Systems begleiten wird. Bedauerlicherweise sind dabei gewisse Schwierigkeiten eingetreten, weil dem Schengener Übereinkommen Länder beigetreten sind und eine gleichberechtigte Mitwirkung in der DatenschutzKontrollinstanz verlangen, obwohl sie noch kein Datenschutzgesetz oder noch keine unabhängige nationale Datenschutzinstanz haben.

Vergleichbare gemeinsame Kontrollinstanzen, in denen ebenfalls die Datenschutzbeauftragten der Mitgliedstaaten vertreten sein werden, wird es wohl auch für die anderen geplanten europäischen Informationssysteme geben. Auch wenn dabei eine optimale Koordinierung stattfindet, wie ich es anstrebe, stellen sich doch an die Datenschutzbeauftragten und ihre Dienststellen erhebliche zusätzliche Anforderungen. Meine Beratungsaufgabe gegenüber den Ministerien hat sich aufgrund der vielfältigen europäischen Aktivitäten entsprechend ausgeweitet und umfaßt auch die Teilnahme an internationalen Verhandlungsterminen.

33.3 Europarat

Der Europarat hat zwei weitere bereichsspezifische Empfehlungen verabschiedet (vgl. auch die Liste der bisherigen Empfehlungen 12. TB S. 93f.), die

— Empfehlung zum Schutz personenbezogener Daten beim Zahlungsverkehr und damit verbundenen Vorgängen (R (90)19) und die

— Empfehlung für die Übermittlung der von öffentlichen Stellen gespeicherten personenbezogenen Daten an Dritte (R (91)10).

Der Entwurf einer Empfehlung zur Telekommunikation befindet sich noch in der Abstimmung. Danach steht eine Empfehlung zum Datenschutz in der Medizin an. Daneben befaßt sich der Europarat mit der Frage eines Beitritts der Europäischen Gemeinschaft zur Datenschutzkonvention (vgl. 13. TB S. 88) und mit den damit verbundenen Konsequenzen für die Verfahrensweise in den verschiedenen Beratungs- und Entscheidungsgremien.

33.4 Europäische Informationssysteme

Die vom Europäischen Rat in Maastricht vereinbarte Zusammenarbeit der Mitgliedsstaaten in den Bereichen Justiz und Inneres hat im Berichtszeitraum zahlreiche Vorhaben initiiert oder vorangebracht, die auch datenschutzrechtlich von erheblicher Bedeutung sind. Ich habe bereits früher auf das Schengener Durchführungsübereinkommen mit dem dort vorgesehenen Informationssystem — SIS — hingewiesen (12. TB S. 95ff.). Neuerdings wird ein Europäisches Informationssystem (EIS) vorbereitet, an dem auch diejenigen EG-Mitgliedsstaaten teilnehmen sollen, die dem Schengener Übereinkommen nicht beigetreten sind (s. 24.2.1). Die seit langem diskutierten Pläne zum Aufbau eines unionsweiten Systems zum Austausch von Informationen im Rahmen eines Europäischen Polizeiamtes (EUROPOL) waren bereits bis zum Entwurf einer Ministervereinbarung gediehen; mangels Einigung über den vorläufigen Sitz der Einrichtung konnte das Vorhaben jedoch nicht — wie ursprünglich vorgesehen — am 1. Januar 1993 gestartet werden (s. 24.2.2). Schließlich haben sich die Zollverwaltungen der EG-Mitgliedsstaaten schon weitgehend über die Einrichtung eines gemeinsamen Zollinformationssystems (CIS) zur Bekämpfung zollrechtlicher Verstöße geeinigt, die nicht in die Zuständigkeit der EG selbst fallen (s. 26.3). Ferner wird über die Einführung eines europaweiten Systems zur Erfassung der Fingerabdrücke von Asylbewerbern — EURODAC — diskutiert; letzteres Vorhaben ist jedoch über das Stadium von Projektanalysen noch nicht hinausgekommen.

Allen genannten Vorhaben ist gemeinsam, daß ungeachtet unterschiedlicher Zielsetzungen gemeinschaftsweite Informationssysteme zur Verarbeitung und Nutzung auch personenbezogener Daten geschaffen werden sollen. Ich setze mich dafür ein, den im Schengener Durchführungsübereinkommen erreichten Datenschutz-Standard auch zum Maßstab für die anderen Projekte zu machen. Dies bedeutet insbesondere einen in etwa gleichwertigen Datenschutz in allen Vertragsstaaten spätestens zum Inkrafttreten der jeweiligen Vereinbarung; ferner die Sicherstellung der Rechte des Betroffenen sowie eine unabhängige Datenschutzkontrolle auf nationaler und internationaler Ebene. Keinesfalls dürfen die strengen datenschutzrechtlichen Bestimmungen im Inland durch Teilnahme deutscher Behörden an internationalen Informationssystemen unterlaufen werden.

33.5 EG-Datenschutz-Richtlinie

Die Absicht der Kommission, die Datenschutzrichtlinie (zu deren Inhalt und allgemeinen Problemen s. 13. TB S. 87ff.) noch vor Beginn des EG-Binnenmarktes in Kraft zu setzen, hat sich nicht verwirklichen lassen. Nach sehr intensiven Beratungen hat das europäische Parlament eine Vielzahl von Änderungswünschen beschlossen. Auf dieser Grundlage sowie unter Berücksichtigung des Diskussionsstandes im Ministerrat, der seine Beratungen parallel zu denen des europäischen Parlaments weitergeführt hat, sowie zahlreicher Stellungnahmen von nationalen und europäischen Interessenverbänden hat die Kommission am 15. Oktober 1992 einen geänderten Vorschlag (gem. Artikel 149 Abs. 3 EWG-Vertrag) vorgelegt (KOM(92) 422 endg. — SYN 287).

Dieser geänderte Vorschlag ist im allgemeinen gut aufgenommen worden. Er beinhaltet auch aus der Sicht der Datenschutzbeauftragten eine ganze Reihe wichtiger Verbesserungen. So entspricht beispielsweise die Zusammenfassung der Regelungen für den öffentlichen und den nicht-öffentlichen Bereich einer Empfehlung der Datenschutzinstanzen der EG-Mitgliedstaaten. Bei der Frage der Anmeldung und Registrierung von Dateien bei den nationalen Datenschutzbehörden ist die Kommission deren Empfehlungen gefolgt, keine flächendeckende, sondern nur eine streng selektive Registrierung vorzusehen. Auch bei der Zusammenarbeit der nationalen Datenschutzinstanzen auf europäischer Ebene in Form der sogenannten Gruppe für Datenschutz wurden deren Verbesserungsvorschläge (z. B. den Vorsitzenden aus ihrer Mitte zu wählen) berücksichtigt. Von den Forderungen, die die Datenschutzbeauftragten des Bundes und der Länder am 29. Januar 1991 formuliert haben (vgl. 13. TB S. 107f.), sind allerdings einige wichtige Punkte noch offen. Ich bin bemüht, in den fortdauernden Beratungen mit meinen europäischen Kollegen weitere Verbesserungen zu erreichen. Im übrigen stehe ich mit der Bundesregierung in enger Fühlungnahme, was ihre Verhandlungsziele im Ministerrat betrifft.

Besonderes Gewicht messe ich folgenden Themen bei:

a) Der geänderte Vorschlag fordert, ohne insoweit zwischen dem öffentlichen und nicht-öffentlichen Bereich zu differenzieren, daß der Datenschutz durch „unabhängige" Datenschutzbehörden kontrolliert wird und daß diese über „wirksame Eingriffsbefugnisse" verfügen. Damit könnte das dem Bundesdatenschutzgesetz und den Landesdatenschutzgesetzen zugrunde liegende Modell des unabhängigen Datenschutzbeauftragten, der nicht durch Eingriffe in Form verbindlicher Anordnungen, sondern durch seine moralisch-politische Autorität und seinen direkten Zugang zum Parlament wirkt, in Frage gestellt sein. Die Datenschutzbeauftragten in Deutschland erfreuen sich jedoch,

wie sich nicht zuletzt an der Stärkung ihrer Stellung durch die neuere Gesetzgebung zeigt, einer sehr großen Akzeptanz, was ihren institutionellen Rahmen betrifft. Ich begrüße es daher, wenn die Bundesregierung sich entschieden dafür einsetzt, daß das deutsche Modell der Datenschutzbeauftragten beibehalten werden kann. Der Wortlaut des geänderten Richtlinienvorschlags ist in dieser Frage nicht eindeutig, zumal wenn man den französischen Originaltext zugrunde legt, der allgemeiner von „pouvoirs effectifs d'intervention" spricht. Daß die Datenschutzbeauftragten in Deutschland die Möglichkeit haben, „wirkungsvoll zu intervenieren", wird wohl niemand bestreiten. Ich gehe davon aus, daß die Bundesregierung das Problem im Ministerrat in geeigneter Weise abklärt.

b) Ein wichtiges Beratungsthema ist die Frage, welcher Spielraum den Mitgliedstaaten nach Inkrafttreten der Richtlinie noch verbleibt, insbesondere soweit es um die Fortentwicklung des allgemeinen und des bereichsspezifischen Datenschutzes geht. Die Richtlinie enthält keine ausdrückliche Öffnungsklausel zugunsten eines weitergehenden Schutzes. Die Kommission macht aber geltend, daß die Richtlinie den Mitgliedstaaten eine erhebliche Bandbreite zulässiger Regelungen eröffne und daß alle in den Mitgliedsstaaten gegenwärtig bestehenden Datenschutzregelungen sich innerhalb dieser Bandbreite bewegten. Eine ausdrückliche Öffnungsklausel sei daher nicht erforderlich und im übrigen mit dem angestrebten Ziel der Harmonisierung nicht vereinbar. Die Frage, ob die Offenheit für die künftige Entwicklung des Datenschutzes durch eine entsprechende Klausel ausdrücklich anerkannt wird — was ich vorziehen würde — oder ob sie als „eingebautes" Strukturmerkmal der Richtlinie betrachtet wird, ist letztlich nicht von entscheidender Bedeutung. In jedem Fall müssen die Mitgliedstaaten aber einen ausreichenden Spielraum behalten, um den Datenschutz auch künftig nicht nur zu erhalten, sondern ihn auch neuen technologischen und gesellschaften Anforderungen anpassen zu können. Besonders für Länder mit einem weitentwickelten bereichsspezifischen Datenschutz, wie die Bundesrepublik Deutschland, ist dies eine entscheidende Frage. Aber auch die Datenschutzbeauftragten der anderen EG-Mitgliedstaaten fordern eine solche Offenheit. Ich gehe davon aus, daß die Bundesregierung diese Zielvorstellung teilt, und würde es begrüßen, wenn sie bei den anstehenden Verhandlungen auf diesen Punkt besonders Gewicht legt.

c) Eine Verpflichtung zur Bestellung eines unternehmens- oder behördeninternen Datenschutzbeauftragten (entsprechend § 36 BDSG) sieht der Richtlinienentwurf nicht vor. Manche Beobachter glauben, damit seien die Tage dieser Datenschutzbeauftragten gezählt, weil der internationale Wettbewerbsdruck oder auch der Harmonisierungsanspruch international tätiger Unternehmen den deutschen Gesetzgeber über kurz oder lang zwingen werde, die Datenschutzbeauftragten abzuschaffen. Ich teile diese Auffassung nicht, da die vom Datenschutzbeauftragten wahrgenommenen Funktionen in jedem Falle zu erfüllen sind. Wenn dafür als organisatorische Vorgabe ein teilweise unabhängig gestellter Datenschutzbeauftragter gefordert wird, so sind ins Gewicht fallende Mehrkosten — bei sachgerechter Organisation — nicht erkennbar. Eine ausdrückliche Erlaubnis durch die Richtlinie ist überflüssig, da den Mitgliedstaaten in allen von der Richtlinie nicht geregelten Fragen ohnehin die volle Gestaltungsfreiheit erhalten bleibt. Allerdings bin ich der Auffassung, daß die Einrichtung des Datenschutzbeauftragten in den Partnerländern noch besser bekannt gemacht werden sollte, damit sie dort mehr Nachahmung findet.

33.6 Informationstätigkeit

Wachsende Nachfrage nach Informationen über den Datenschutz registriere ich auch aus dem Ausland. Während in den früheren Jahren hauptsächlich Anfragen und Besuche von ausgesprochenen Fachexperten zu verzeichnen waren — meist im Zusammenhang mit der Ausarbeitung von Datenschutzprogrammen in ihren Ländern —, erreichen mich heute auch viele Anfragen von öffentlichen und privaten datenverarbeitenden Stellen, von multinationalen Unternehmen, Beratungsfirmen und wissenschaftlichen Instituten, aber auch von Einzelpersonen. Neben dem deutschsprachigen Informationsmaterial stehen mir für solche Anfragen auch eine englische und eine französische Übersetzung des BDSG und neuerdings auch eine von Inter-Nationes im Auftrag des Bundespresseamtes in Deutsch, Englisch und Französisch herausgegebene Schrift „Datenschutz in Deutschland", verfaßt von Dr. H. Horstkotte, zur Verfügung. Diese beschreibt nicht nur den wesentlichen Inhalt des BDSG, sondern auch die historische Entwicklung des Datenschutzes, Fragen der grenzüberschreitenden Datenübermittlung und die Bereiche Gesundheit, Arbeit und Medien als Beispiele des Datenschutzes auf einzelnen Problemfeldern.

34 Aus zurückliegenden Tätigkeitsberichten — Bilanz —

1. Zu dem im 13. TB (S. 8) berichteten Fall der *Auskunftsverweigerung durch das BKA* konnte auf der Grundlage meiner Beanstandung — mit einiger Verzögerung — noch in der Weise Abhilfe geschaffen werden, daß das BKA dem Betroffenen die Auskunft in dem gebotenen Umfang erteilt hat.

2. Im 13. Tätigkeitsbericht S. 29 hatte ich die Frage erörtert, wie die Frist für die Tilgung einer in der ehemaligen DDR ergangenen Verurteilung aus dem Bundeszentralregister zu berechnen sei, wenn aus einer auch nach unserem Recht eintragungsfähigen Verurteilung und einer nicht-eintragungsfähigen gerichtlichen Entscheidung eine Gesamtstrafe gebildet worden war. Ich hatte empfohlen, in solchen Fällen für die Berechnung der Tilgungsfrist die Dauer der wegen der nicht-eintragungsfähigen Tat verhängten Strafe von

der Dauer der gebildeten Gesamtstrafe abzuziehen. Der Generalbundesanwalt — Dienststelle Bundeszentralregister — hat meine Empfehlung sowohl bei der Berechnung der Tilgungsfrist als auch bei der Frist für die Nichtaufnahme in ein Führungszeugnis erfreulicherweise aufgegriffen. Er hat eine entsprechende Arbeitsanweisung und ein Programm für die Berechnung der Fristen erstellt.

3. Die im *Zentralen Fahrerlaubnisregister der DDR* gespeicherten Daten über den Entzug von Führerscheinen werden gemäß dem Einigungsvertrag vorläufig vom Kraftfahrt-Bundesamt in einer besonderen Datei geführt (13. TB S. 30f.). Das Bundesministerium für Verkehr beabsichtigt, demnächst den Entwurf für eine endgültige gesetzliche Regelung vorzulegen.

4. Bei einer Kontrolle beim *Bundesministerium für Raumordnung, Bauwesen und Städebau* (BMBau) hatte ich eine Reihe von Mängeln festgestellt (13. TB S. 41). Das BMBau ist meinen Anregungen zu deren Behebung gefolgt.

5. Über mögliche datenschutzrechtliche Verbesserungen durch die *Postdienst-Datenschutzverordnung*, insbesondere bei der Anschriftenmitteilung, habe ich berichtet (13. TB S. 47f.). Die Verordnung ist am 1. Juli 1991 wie vorgesehen in Kraft getreten und hat sich bewährt.

6. Die Ermittlung von *Anschriften für anlaßbezogene Werbemaßnahmen durch Postzusteller* habe ich kritisiert (13. TB S. 50). Nach dem Inkrafttreten der Postdienst-Datenschutzverordnung besteht Einvernehmen mit der Generaldirektion Postdienst, daß solche Anschriftenermittlungen nicht zu den Aufgaben des Postdienstes gehören.

7. Bei der *Postbank* hatte ich beanstandet, daß sie die überziehungsbedingten Sperrungen von Gehaltskonten der Postbediensteten an deren Personalstelle übermittelt (13. TB S. 50). Durch die Einräumung eines Dispositionslimits für die Kontoinhaber ist dieses Problem wesentlich entschärft. Die Postbank-Card, deren Ausgabe an alle Teilnehmer am Gehaltskontoverfahren begonnen hat, und die damit verbundenen neuen Auszahlungsverfahren ermöglichen darüber hinaus eine Dekkungsanfrage bei jeder Abhebung, so daß eine Sperrmitteilung in Zukunft entbehrlich ist.

8. Das Fehlen notwendiger Rechtsgrundlagen für die Verarbeitung personenbezogener Daten für Zwecke des *Luftverkehrs* habe ich bedauert (13. TB S. 57). Diese Defizite bestehen weit überwiegend noch immer, s. dazu 18.9 in diesem Bericht.

9. Am 2. Januar 1991 hat das Bundesministerium des Innern die *Sicherheitsrichtlinien* des Bundes (11. TB S. 60) nochmals geändert. Im wesentlichen sind Anpassungen der Verwaltungsvorschriften an das neue Bundesverfassungsschutzgesetz (13. TB S. 72) vorgenommen worden. Nunmehr ist die Zustimmung des Betroffenen in jedem Fall Voraussetzung für die Durchführung einer Sicherheitsüberprüfung. Im übrigen ist der betroffene Personenkreis dadurch eingeschränkt worden, daß eine sicherheitsempfindliche Tätigkeit erst nach Vollendung des 16. Lebensjahres übertragen werden darf. Das Ermessen des Bundesamtes für Verfassungsschutz, aus operativen Erwägungen in Verdachtsfällen vorläufig davon abzusehen, den Geheimschutzbeauftragten über das Ergebnis nachträglicher Überprüfungsmaßnahmen zu unterrichten, ist entfallen. Außerdem fragt das Bundesamt für Verfassungsschutz im Rahmen seiner Mitwirkung nun direkt bei der Grenzschutzdirektion Koblenz an. Zuvor hatte das BKA Erkenntnisse aus Grenzfahndungsbestand und Grenzaktennachweis vermittelt. Über die nähere Ausgestaltung dieser Verfahrensvereinfachung bestehen Meinungsverschiedenheiten zwischen dem Bundesministerium des Innern und mir, die noch nicht behoben sind.

10. Im Berichtszeitraum habe ich gegenüber dem Bundesministerium des Innern und dem Bundesamt für Verfassungsschutz eindringlich auf die Notwendigkeit der Überarbeitung der *Verkartungspläne* des Bundesamtes für Verfassungsschutz hingewiesen, um eine *Anpassung dieser Verwaltungsvorschriften an die gesetzlichen Regelungen des neuen Bundesverfassungsschutzgesetzes* (13. TB S. 72) zu erreichen. Nachdem das neue Gesetz mehr als zweieinhalb Jahre in Kraft getreten war, habe ich meine Forderung dem Innenausschuß des Deutschen Bundestages vorgetragen. Hieraufhin hat das Bundesministerium des Innern zugesagt, bis spätestens zum 30. Juni 1993 die Verkartungspläne für alle Abteilungen des Bundesamtes für Verfassungsschutz in überarbeiteter, der neuen Sach- und Rechtslage angepaßten Form in Kraft zu setzen.

11. Auf die Notwendigkeit der Verbesserung der *Regelungen des BMVg für den Einsatz von PC*, die auch die Verwendung privater PC umfassen, habe ich hingewiesen (13. TB S. 75 f., 76, aber auch 12. TB S. 85). Das BMVg hat inzwischen Durchführungsbestimmungen zum — neuen — Bundesdatenschutzgesetz in seinem Geschäftsbereich erlassen (VMBl 1991 S. 293ff.), die entsprechende Bestimmungen enthalten. Insbesondere hat das BMVg darin auch das *Verbot der Nutzung privater Hard- und Software* zur Verarbeitung personenbezogener Daten aus seinen früheren einschlägigen Vorschriften übernommen. Außerdem hat es in einer Anlage zu den Durchführungsbestimmungen eingehende technische und organisatorische Maßnahmen für den *dienstlichen Einsatz von Informationstechnik* vorgeschrieben. Darüber hinaus wird jedem Anwender im Beschäftsbereich des BMVg ein Merkblatt zur DV-Sicherheit für die Nutzer von Rechnern am Arbeitsplatz an die Hand gegeben, das ständig aktualisiert wird. Damit ist meinem Anliegen grundsätzlich Rechnung getragen.

12. Dem Rechtsausschuß des Deutschen Bundestages liegt als federführendem Ausschuß bereits seit längerem der Regierungsentwurf eines Gesetzes zur Änderung von Vorschriften über das *Schuldnerverzeichnis* (BT-Drucksache 12/193) zur Bera-

tung vor (s. 13. TB S. 89 Nr. 3). In einer Stellungnahme an die Vorsitzenden des Rechtsausschusses und des Innenausschusses des Deutschen Bundestages habe ich hierzu einige Empfehlungen gegeben. Im Hinblick auf die unzureichende Bestimmung des § 915 ZPO zu diesem Fragenkreis halte ich die baldige Verabschiedung einer gesetzlichen Regelung, die datenschutzrechtlichen Anforderungen entspricht, für erforderlich.

13. Meine Bedenken dagegen, daß in Pfändungs- und Überweisungsbeschlüssen auch mehrere *Drittschuldner* aufgenommen werden (s. 13. TB S. 89 Nr. 4), sind in der mit der Überarbeitung des Zwangsvollstreckungsrechts betrauten Arbeitsgruppe der Justizministerkonferenz beraten worden. Wie ich aus einem mir erst kürzlich vom BMJ zugeleiteten Auszug aus dem Schlußbericht der Arbeitsgruppe entnommen habe, wird darin vorgeschlagen, § 829 Abs. 1 ZPO dahingehend zu ergänzen, daß die Pfändung mehrerer Geldforderungen gegen verschiedene Drittschuldner auf Antrag des Gläubigers durch *einheitlichen* Beschluß ausgesprochen werden *soll*. Die Begründung für diese damit — aus Kostengründen — nach wie vor zu erwartende regelmäßige Zusammenfassung mehrerer Drittschuldner in einem Pfändungs- und Überweisungsbeschluß beruft sich darauf, „die Unterrichtung der Drittschuldner von weiteren gepfändeten Forderungen gegen weitere Drittschuldner" erscheine „in vielerlei Hinsicht *sinnvoll* und in manchen Fällen darüber hinaus *erforderlich*". Aus meiner Sicht kann es überhaupt nur darauf ankommen, *ob* die Zusammenfassung mehrerer Drittschuldner in einem Pfändungs- und Überweisungsbeschluß und damit ein Eingriff in das Persönlichkeitsrecht der Betroffenen in Abwägung mit dem öffentlichen Interesse und den Interessen beteiligter Dritter *erforderlich* ist. Eine erste Durchsicht der Argumente hat mich hiervon nicht überzeugen können. Ich werde gegenüber dem BMJ noch eingehend Stellung nehmen.

14. Über einen erfolgreichen Betriebsversuch zur Einrichtung von *Diskretionszonen* vor Postschaltern habe ich berichtet (13. TB S. 91 Nr. 17). Inzwischen sind nicht nur in allen Poststellen der alten Bundesländer mit mehr als zwei Schaltern, sondern auch in den neuen Bundesländern in großem Umfang Diskretionszonen markiert worden.

15. Nachdem das Gesetz über die *Statistik im Handwerk* in der 11. Legislaturperiode nicht mehr verabschiedet wurde (13. TB S. 92 Nr. 29), hat das Bundesministerium für Wirtschaft inzwischen einen neuen Entwurf vorgelegt, der dem früheren im wesentlichen entspricht.

16. Bereits in meinem 12. TB (S. 60) und meinem 13. TB (S. 93 Nr. 37) habe ich über eine datenschutzgerechte Verfahrensorganisation beim *Sozialamt der Deutschen Bundespost (SAP)* berichtet. Das Direktorium der Deutschen Bundespost hat mir im Berichtszeitraum vorgetragen, daß betriebliche und organisatorische Belange unabdingbar für eine Änderung der im 13. TB beschriebenen Verfahren, insbesondere für eine Zentralisierung von Botendienst und zentralem Schreibdienst bei dem SAP zusammen mit der Versorgungsanstalt der Deutschen Bundespost (VAP) sprechen. Ich halte das nunmehr vorgeschlagene Verfahren aus datenschutzrechtlicher Sicht für vertretbar, weil das Nähere über die Behandlung personenbezogener Daten durch die zentralisierten Dienste in einer Verwaltungsvereinbarung zwischen dem SAP und dem VAP geregelt werden soll. Auf deren datenschutzgerechte Ausgestaltung werde ich hinwirken.

Anlage 1 (zu 4. / u. a.)

Deutscher Bundestag
12. Wahlperiode

Drucksache 12/4094

13. 01. 93

Annahme der Beschlußempfehlung durch Beschluß des Deutschen Bundestages vom 05. 02. 93 (Plenarprotokoll 12/138)

Beschlußempfehlung und Bericht

des Innenausschusses (4. Ausschuß)

zu den Unterrichtungen durch den Bundesbeauftragten für den Datenschutz

a) Zehnter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes (BDSG)
— Drucksache 11/1693 —

b) Elfter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes (BDSG)
— Drucksache 11/3932 —

c) Zwölfter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes (BDSG)
— Drucksache 11/6458 —

d) Dreizehnter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes (BDSG)
— Drucksache 12/553 —

A. Problem

Der Bundesbeauftragte hat gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes vom 27. Januar 1977 in seinem Zehnten Tätigkeitsbericht über seine Arbeit im Jahr 1987 berichtet. Sein Elfter Tätigkeitsbericht bezieht sich auf das Jahr 1988, der Zwölfte auf das Jahr 1989 und der Dreizehnte Tätigkeitsbericht auf seine Arbeit im Jahr 1990 und die ersten Monate des Jahres 1991.

B. Lösung

Der Innenausschuß hat beschlossen, dem Deutschen Bundestag zu empfehlen, der anliegenden Beschlußempfehlung zu den Bereichen Bundesamt für Verfassungsschutz, Beihilfeverfahren, Wehrstammkarten der ehemaligen Nationalen Volksarmee, Telefondatenverarbeitung in der Bundesregierung, Arbeitnehmerdatenschutz, gesetzliche Regelung der Sicherheitsüberprüfung, Ausländerzentralregister, Verbot oder Einschränkung genomanalytischer Untersuchungen, Bundeskriminalamtgesetz und Bundesgrenzschutzgesetz sowie ISDN-Verbindungsdaten und sonstige Kommunikationsdaten zuzustimmen.

Mehrheit im Ausschuß

C. Alternativen

Mehrheitlich abgelehnt wurde der aus dem anliegenden Bericht ersichtliche Antrag der Gruppe BÜNDNIS 90/DIE GRÜNEN zur Fassung einer Beschlußempfehlung.

D. Kosten

Keine

Beschlußempfehlung

Der Bundestag wolle beschließen,

1. Bundesamt für Verfassungsschutz:

   a) Der Deutsche Bundestag stellt fest, daß der Bundesminister des Innern zugesagt hat, spätestens bis zum 30. Juni 1993 die Verkartungspläne für alle Abteilungen des Bundesamtes für Verfassungsschutz in überarbeiteter, der neuen Sach- und Rechtslage angepaßter Form in Kraft zu setzen.

   b) Der Deutsche Bundestag empfiehlt der Bundesregierung, bei Anwendung des § 15 BVerfSchG

      aa) davon auszugehen, daß die Vorschrift auch in Fällen, in denen die Voraussetzungen dieser Vorschrift nicht vorliegen, — vorbehaltlich des Absatzes 2 — eine Auskunftserteilung zuläßt,

      bb) deshalb auch der Umfang der Auskunft nicht zwingend auf Speicherungen zu dem Sachverhalt beschränkt ist, der konkret vorgetragen wurde,

      cc) an die Darlegung eines konkreten Sachverhaltes und eines besonderen Interesses an der Auskunft keine zu strengen Anforderungen zu stellen.

2. Beihilfeverfahren; eigenes Antragsrecht für Angehörige:

   Der Deutsche Bundestag nimmt zur Kenntnis, daß die Praxis dahin gehend geändert worden ist, daß der Beihilfeberechtigte nicht gegen den Willen von im Rahmen der Beihilfe berücksichtigungsfähigen Angehörigen Kenntnis von deren eingereichten Belegen erhält, und geht davon aus, daß alle Bundesbehörden entsprechend verfahren.

3. Wehrstammkarten der ehemaligen NVA:

   Der Deutsche Bundestag fordert die Bundesregierung auf, die Datenfelder auf den Wehrstammkarten der ehemaligen NVA, die für die Durchführung der Aufgaben der Bundeswehr nicht erforderlich sind, immer zu löschen, wenn eine Wehrstammkarte im Zusammenhang mit der Bearbeitung eines Vorganges vorgelegt wird. Nicht erforderlich sind die 15 Datenfelder, die im einzelnen zwischen dem Bundesminister der Verteidigung und dem Bundesbeauftragten für den Datenschutz festgelegt worden sind.

4. Telefondatenverarbeitung in der Bundesregierung; Dienstanschlußvorschriften:

   Die Bundesregierung hat den Entwurf von neuen „Allgemeinen Verwaltungsvorschriften über die Einrichtung und Nutzung dienstlicher Fernmeldeanlagen für die Bundesverwaltung mit Ausnahme der Deutschen Bundespost (Dienstanschlußvor-

schriften — DAV —)" erstellt. Die Bundesregierung wird aufgefordert, die neuen DAV unverzüglich in Kraft zu setzen.

5. Der Deutsche Bundestag fordert die Bundesregierung auf,

   — bereichsspezifische Regelungen zum Arbeitnehmerdatenschutz sowie

   — eine gesetzliche Regelung der Sicherheitsüberprüfung, die den Vorgaben der Verfassungsrechtsprechung Rechnung trägt,

   so rechtzeitig vorzulegen, daß sie in dieser Legislaturperiode verabschiedet werden können.

6. Ausländerzentralregister:

   Der Deutsche Bundestag fordert die Bundesregierung auf, den Entwurf einer gesetzlichen Grundlage für die Verarbeitung personenbezogener Daten im Ausländerzentralregister so schnell wie möglich einzubringen.

7. Verbot oder Einschränkung genomanalytischer Untersuchungen:

   Der Deutsche Bundestag hält es für notwendig, die erforderlichen speziellen gesetzlichen Regelungen zu treffen.

8. Novelle zum BKA- und BGS-Gesetz:

   Der Deutsche Bundestag hält es für erforderlich, die Rechtsvorschriften über die Verarbeitung personenbezogener Daten im BKA- und BGS-Gesetz noch in dieser Legislaturperiode zu verabschieden.

9. ISDN-Verbindungsdaten und sonstige Kommunikationsdaten:

   In der „Fangschaltungsentscheidung" vom 25. März 1992 — I BvR 1430/88 — hat das Bundesverfassungsgericht das Fehlen einer verfassungsgemäßen gesetzlichen Grundlage jedenfalls für diejenigen in der TDSV geregelten Sachverhalte festgestellt, die dem Schutz des Fernmeldegeheimnisses aus Artikel 10 Abs. 1 Grundgesetz unterliegen. Der Deutsche Bundestag fordert die Bundesregierung auf, unverzüglich einen Gesetzentwurf vorzulegen, der dem Urteil des Bundesverfassungsgerichts Rechnung trägt.

Bonn, den 21. Dezember 1992

Der Innenausschuß

Hans Gottfried Bernrath	**Dr. Heribert Blens**	**Dr. Burkhard Hirsch**	**Peter Paterna**
Der Vorsitzende	Berichterstatter		

Bericht der Abgeordneten Dr. Heribert Blens, Dr. Burkhard Hirsch und Peter Paterna

I. Allgemeines

1. Der Zehnte Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz wurde zuletzt in der 13. Sitzung des 12. Deutschen Bundestages am 12. März 1991 an den Innenausschuß federführend und an den Petitionsausschuß, den Rechtsausschuß, den Ausschuß für Wirtschaft, den Ausschuß für Arbeit und Sozialordnung, den Verteidigungsausschuß, den Ausschuß für Gesundheit, den Ausschuß für Post und Telekommunikation, den Ausschuß für Raumordnung, Bauwesen und Städtebau und den Ausschuß für Forschung, Technologie und Technikfolgenabschätzung zur Mitberatung überwiesen.

2. Der Elfte Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz wurde zuletzt in der 13. Sitzung des 12. Deutschen Bundestages am 12. März 1991 an den Innenausschuß federführend und an den Petitionsausschuß, den Rechtsausschuß, den Finanzausschuß, den Ausschuß für Wirtschaft, den Ausschuß für Arbeit und Sozialordnung, den Verteidigungsausschuß, den Ausschuß für Gesundheit, den Ausschuß für Verkehr, den Ausschuß für Post und Telekommunikation, den Ausschuß für Raumordnung, Bauwesen und Städtebau und den Ausschuß für Forschung, Technologie und Technikfolgenabschätzung zur Mitberatung überwiesen.

3. Der Zwölfte Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz wurde zuletzt in der 13. Sitzung des 12. Deutschen Bundestages am 12. März 1991 an den Innenausschuß federführend und an den Ausschuß für Wahlprüfung, Immunität und Geschäftsordnung, den Petitionsausschuß, den Rechtsausschuß, den Finanzausschuß, den Ausschuß für Wirtschaft, den Ausschuß für Arbeit und Sozialordnung, den Verteidigungsausschuß, den Ausschuß für Gesundheit, den Ausschuß für Umwelt, Naturschutz und Reaktorsicherheit, den Ausschuß für Post und Telekommunikation und den Ausschuß für Forschung, Technologie und Technikfolgenabschätzung zur Mitberatung überwiesen.

4. Der Dreizehnte Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz wurde in der 47. Sitzung des 12. Deutschen Bundestages am 10. Oktober 1991 an den Innenausschuß federführend und an den Rechtsausschuß, den Ausschuß für Arbeit und Sozialordnung, den Verteidigungsausschuß, den Ausschuß für Post und Telekommunikation, den Ausschuß für Raumordnung, Bauwesen und Städtebau, den Ausschuß für Forschung, Technologie und Technikfolgenabschätzung und den Ausschuß für Gesundheit zur Mitberatung überwiesen.

II. Empfehlungen der mitberatenden Ausschüsse

1. Der Petitionsausschuß hat dem Innenausschuß in der 12. Wahlperiode folgende, seine Stellungnahmen aus der 11. Wahlperiode abändernden Voten zum Zehnten, Elften und Zwölften Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz übermittelt:

„Der Petitionsausschuß hat in seiner Sitzung am 25. September 1991 den Zehnten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (Drucksache 11/1693) beraten, soweit darin Vorgänge des Petitionsausschusses angesprochen sind (Nummer 3.2 und Nummer 7.1.3). Hierzu gibt er folgende Stellungnahme ab:

Zu Nummer 3.2

Der Bundestag hat in seiner Geschäftsordnung das Recht auf Einsicht in Akten, die sich in der Verwahrung des Bundestages oder eines Ausschusses befinden, geregelt. Danach — und auch nach anderen Vorschriften — hat der Petent kein Recht auf Akteneinsicht. Der Petitionsausschuß kann daher in seine nach § 110 Abs. 1 GO-BT aufzustellenden Verfahrensgrundsätze ein Einsichtsrecht des Petenten in die beim Petitionsausschuß geführten Akten nicht aufnehmen.

An dieser Rechtslage hat auch das Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20. Dezember 1990, das am 1. Juni 1991 in Kraft trat und u. a. auch das Akteneinsichtsrecht in Verwaltungsakten regelt, nichts geändert, da es auf den parlamentarischen Bereich des Deutschen Bundestages und somit auf die Tätigkeit des Petitionsausschusses keine unmittelbare Anwendung findet.

Ob eine künftige parlamentsspezifische Datenschutzregelung eine andere Regelung bringen wird, bleibt abzuwarten.

Der Petitionsausschuß schlägt von sich aus nicht die Einführung eines Einsichtsrechts durch Änderung der Geschäftsordnung des Bundestages oder durch eine gesetzliche Regelung vor.

Ein Petent bekommt vom Ausschuß auch nach der geltenden Rechtslage alle Auskünfte über die Behandlung seiner Petition, die er für die Wahrnehmung seines Petitionsrechts als notwendig erachtet, sofern dadurch nicht die Erfüllung der Aufgaben des Petitionsausschusses beeinträchtigt wird oder andere Vorschriften die entsprechende Auskunft verbieten. Insbesondere der ihm erteilte Endbescheid gibt dem Petenten die Möglichkeit zur Prüfung, ob sein Recht auf Entgegen-

nahme, sachliche Prüfung und Bescheidung seiner Petition erfüllt worden ist.

Zu Nummer 7.1.3

Die beteiligte oberste Bundesbehörde war letztlich zur Vorlage der Personalakten bereit. In einem Verwaltungsstreitverfahren erreichte jedoch der betroffene Bedienstete, daß der Behörde die Vorlage bis zur rechtskräftigen Entscheidung in der Hauptsache untersagt wurde. Diese wurde inzwischen mit einem Vergleich erledigt. Dem Petitionsausschuß wurden die wesentlichen Teile der Personalakte und die Disziplinarakte des früheren Beamten vorgelegt. Insbesondere die die Privatsphäre des ehemaligen Beamten betreffenden Aktenteile wurden einvernehmlich von der Vorlage ausgenommen.

Der Petitionsausschuß ist der Auffassung, daß das Recht auf informationelle Selbstbestimmung nicht dazu führen kann, dem in der Petition belasteten Bediensteten das Recht einzuräumen, eine sachgerechte Behandlung der Petition durch den Petitionsausschuß zu verhindern. Der Petitionsausschuß geht auch davon aus, daß der BfD bei genauer Kenntnis des dem Aktenvorlageersuchen zugrundeliegenden Sachverhalts den Vorgang nicht zum Anlaß für die Aufnahme in seinen Bericht und zur Kritik genommen hätte.

Den Elften und Zwölften Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz — Drucksachen 11/3932 und 11/6458 —, die ebenfalls am 25. September 1991 beraten wurden, hat der Ausschuß zur Kenntnis genommen."

2. Der Rechtsausschuß hat in der 12. Wahlperiode einstimmig beschlossen, den Zehnten, Elften, Zwölften und Dreizehnten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz zur Kenntnis zu nehmen.

   Zu dem Elften und Zwölften Tätigkeitsbericht hat er sich den Kritikpunkten des Bundesbeauftragten für den Datenschutz angeschlossen

   — zu den Regelungen über die Ermittlungs- und Fahndungsmethoden,

   — zu den besonderen Regelungen über die Datenverarbeitung,

   — zur Akteneinsicht

   und hat auch aus seiner Sicht vor allem für regelungsbedürftig gehalten

   — die engere Festlegung der Zuverlässigkeit erkennungsdienstlicher Behandlung und der Voraussetzungen für den Fahndungsabgleich sowie die weitere Verwendung der dabei gewonnenen Daten,

   — die Verbesserung des Schutzes der Persönlichkeitsrechte bei der Erhebung persönlicher Daten von Angeklagten und Zeugen in Strafverfahren,

   — den allenfalls begrenzten Einsatz der Genomanalyse im Strafverfahren.

3. Der Ausschuß für Wirtschaft hat in der 12. Wahlperiode seine Voten aus der 11. Wahlperiode zum Zehnten, Elften und Zwölften Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz bestätigt, in denen er den Zehnten, Elften und Zwölften Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz zur Kenntnis genommen hat.

4. Der Ausschuß für Arbeit und Sozialordnung hat in der 12. Wahlperiode einstimmig bei Abwesenheit der Mitglieder der Gruppen PDS/Linke Liste und BÜNDNIS 90/DIE GRÜNEN folgende Stellungnahme zum Zehnten, Elften und Zwölften Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz beschlossen:

   „Der Bundesregierung wird empfohlen, noch im Laufe des Jahres 1991 einen Gesetzentwurf vorzulegen, der die bereichsspezifischen Vorschriften des Datenschutzes im Bereich der sozialen Sicherung an die Novelle zum Bundesdatenschutzgesetz anpaßt."

   Hinsichtlich des Dreizehnten Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz hat der Ausschuß für Arbeit und Sozialordnung dem Innenausschuß in seiner 31. Sitzung am 13. November 1991 mit den Stimmen der Mitglieder der Fraktionen der CDU/CSU, der SPD und der F.D.P. bei Abwesenheit der Mitglieder der Gruppen PDS/Linke Liste und BÜNDNIS 90/DIE GRÜNEN Kenntnisnahme empfohlen, wobei er mit der gleichen Mehrheit — bei Enthaltung eines Mitglieds der Fraktion der CDU/CSU — die Aufforderung des Datenschutzbeauftragten an die Bundesregierung unterstützt hat, noch in dieser Wahlperiode den Arbeitnehmerdatenschutz gesetzlich zu regeln und im Rahmen der Novellierung des SGB X sicherzustellen, daß bei den Trägern der Selbstverwaltung auch in dezentralen Einrichtungen Ansprechpartner oder Datenschutzbeauftragte bestellt werden.

5. Der Verteidigungsausschuß hat in der 12. Wahlperiode auf eine erneute Beratung des Zehnten, Elften und Zwölften Tätigkeitsberichts verzichtet und auf seine Stellungnahme aus der 11. Wahlperiode verwiesen.

   In der 11. Wahlperiode hatte er den Zehnten, Elften und Zwölften Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz einstimmig zur Kenntnis genommen.

   Den Dreizehnten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz hat der Verteidigungsausschuß in der 12. Wahlperiode in seiner Sitzung am 6. November 1991 zur Kenntnis genommen.

6. Der Ausschuß für Gesundheit hat in der 12. Wahlperiode den Zehnten, Elften, Zwölften und Dreizehnten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz zur Kenntnis genommen.

7. Der Ausschuß für Post und Telekommunikation hat in der 12. Wahlperiode seine Stellungnahme

aus der 11. Wahlperiode zum Zehnten, Elften und Zwölften Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz bestätigt. In der 11. Wahlperiode hatte der Ausschuß für das Post- und Fernmeldewesen einstimmig folgende Stellungnahme zum Zehnten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz beschlossen:

„Der Ausschuß für das Post- und Fernmeldewesen hat die Kapitel des Berichtes, die die Deutsche Bundespost betreffen, in seiner Sitzung am 28. September 1988 eingehend beraten.

Der Ausschuß begrüßt die von der DBP erklärte Bereitschaft, den BfD bei datenschutzmäßig wesentlichen Vorgängen, insbesondere wenn es sich um Infrastrukturaufgaben handelt, möglichst frühzeitig schon im Planungsstadium zu informieren, wenn die beabsichtigten Regelungen hinreichend konkretisiert sind. Der BMP wird aufgefordert, sich weiterhin mit Nachdruck zu bemühen, daß neu eingerichtete Dateien registriert und veröffentlicht werden.

Der Ausschuß erwartet, daß durch die zwischenzeitlich intensivierten und weiter in Aussicht genommenen Kontakte zwischen dem Bundesbeauftragten für den Datenschutz und dem Bundesminister für das Post- und Fernmeldewesen die gegenseitige Zusammenarbeit weiter erleichtert und verbessert wird und bittet, die erklärte Bereitschaft zur Verbesserung der Zusammenarbeit mit dem BfD ernsthaft in allen Abteilungen des Hauses durchzusetzen.

Der Ausschuß geht davon aus, daß die zwischenzeitlich vom Bundesminister für das Post- und Fernmeldewesen eingeleiteten Maßnahmen die Bearbeitungsdauer der Vorgänge, die der BfD dem Hause zuleitet, verkürzen werden. Im Interesse der reibungslosen Zusammenarbeit zwischen BfD und BMP und einer beschleunigten Erledigung von Anfragen ist es in diesem Zusammenhang sachdienlich, wenn der BfD und der BMP in den Fällen unklarer oder strittiger Kompetenz unbürokratisch miteinander Kontakt aufnehmen.

Der Ausschuß bittet den Innenausschuß, über die unter Abschnitt 7.4 des Tätigkeitsberichtes aufgeworfenen Fragen, die die Zusammenarbeit mit der Personalvertretung auf dem Gebiet des Datenschutzes zum Inhalt haben, wegen ihrer grundsätzlichen Bedeutung eine Klärung herbeizuführen."

Hinsichtlich des Elften und Zwölften Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz hatte der Ausschuß für Post und Telekommunikation in der 11. Wahlperiode folgende Stellungnahme abgegeben:

„Der Ausschuß für Post und Telekommunikation hat sich in seinen Beratungen am 9. Mai, am 12. September und am 19. September 1990 im wesentlichen auf die Kapitel 6 Post- und Fernmeldewesen (Drucksache 11/3932) und Kapitel 7 Post und Telekommunikation (Drucksache 11/6458) beschränkt.

Es konnte erfreulicherweise festgestellt werden, daß eine erhebliche Anzahl der vom BfD erhobenen Einwände und Bedenken nach übereinstimmender Ansicht von Ausschuß, BMPT und BfD als inzwischen geklärt betrachtet werden können.

In Übereinstimmung mit dem Bundesbeauftragten für den Datenschutz ist der Ausschuß der Auffassung, daß das diensteintegrierende digitale Fernmeldenetz (ISDN) wichtige datenschutzrechtliche Probleme aufwirft. Die technischen Möglichkeiten des ISDN und das Grundrecht auf unbeobachtete Kommunikation müssen sorgfältig gegeneinander abgewogen werden.

Der Ausschuß begrüßt die Bereitschaft des BMPT, datenschutzrechtliche Probleme und geplante Maßnahmen frühzeitig mit dem BfD zu erörtern. Das gilt insbesondere für die ab 1. Juli 1991 zu erlassenden Rechtsverordnungen. Da es fraglich ist, ob die derzeit bei ISDN praktizierte Datenspeicherung durch die bis 1. Juli 1991 geltende TKO gedeckt ist, hat die Bundesregierung für die neuen Rechtsverordnungen eine stärkere Präzisierung der Rechtsgrundlage bereits in Aussicht gestellt.

Dabei ist der Schutz von Kommunikationsdaten nicht nur des Anrufenden (A-Teilnehmer), sondern auch des Angerufenen (B-Teilnehmer) angemessen zu gewichten.

Die Gewährleistung des Datenschutzes muß in Einklang gebracht werden mit dem berechtigten Interesse der Postkunden, auf Wunsch eine nachprüfbare Rechnung zu erhalten, und mit dem Interesse der Post, bei Gebührenstreitigkeiten für die Richtigkeit der erstellten Rechnung Beweis antreten zu können. Eine Reihe schwieriger Fragen, die in diesem Zusammenhang auftreten, konnten zum gegenwärtigen Zeitpunkt nicht abschließend geklärt werden. Sie werden aufgezeigt mit der Bitte, der federführende Innenausschuß möge sie in seinem Bericht zur besonderen Beachtung empfehlen:

— Trennung von *Verbindungsdaten,* die für den Aufbau der Verbindung gebraucht werden und dann sofort gelöscht werden können, und *Gebührendaten,* die für die Abrechnung gebraucht werden und deshalb für eine bestimmte Zeit gespeichert bleiben müssen. Eine Auswertung nach B-Teilnehmern soll auf keinen Fall möglich sein; der Konflikt mit dem Transparenz-Gebot des BDSG ist diesbezüglich bis auf weiteres ungelöst.

— Es sollte geprüft werden, ob die Speicherung von Vermittlungs- und Gebührendaten über das Verbindungsende hinaus grundsätzlich (bezüglich des B-Teilnehmers) nur anonymisiert erfolgen darf

  oder

  ob der Teilnehmer sollte wählen können zwischen

a) Ablehnung der Speicherung,
d. h. Löschen des Datensatzes sofort nach Errechnung der Gebühren und damit Verzicht des Kunden auf entsprechende Beweismittel

b) anonymisierter Speicherung,
z. B. durch Verkürzung der Zielnummer

c) vollständiger Speicherung der Zielnummern,
die jedoch Rechte des Angerufenen beeinträchtigen kann.

Differenziertere Lösungen wären z. B.

d) auf die Speicherung der B-Teilnehmer im Ortsverkehr zu verzichten (pauschale Abrechnung durch Summenzählung) und nur Ferngespräche zu speichern, und zwar anonymisiert durch Wegfall von mindestens zwei Endziffern,

e) die Bildung von Fallgruppen, z. B. „Nahbereich", „Ausland", mit unterschiedlichen Regelungen.

— Eine Sonderregelung ist erforderlich für sogenannte kritische Ziel-Nummern (Seelsorge, Beratungsstellen etc.), die eine Anonymität als Basis ihrer Beratungstätigkeit voraussetzen. Es ist zu prüfen, ob sie in den Block der Sonderdienst-Rufnummern gelegt werden können, die mit den Ziffern „11" beginnen. Sie sollten keine Rufnummernanzeige ermöglichen und ggf. auch nicht im Einzelgesprächsnachweis ausgewiesen werden.

Die Erwartung, daß durch die Einführung der Chipkarte die Gefahr des Mißbrauchs beim Funktelefon im C-Netz beseitigt wird, hat sich leider nicht bestätigt. Da Chipkarten nicht nur bei Funktelefonen, sondern auch bei öffentlichen Kartentelefonen eingesetzt werden, muß die Problematik umfänglicher erörtert werden, als vom BfD bisher (lediglich für Funktelefone) dargestellt. Es muß u. a. erwogen werden, ob auf die Anwendung bestimmter Techniken, deren Kontrolle zu Konflikten mit Belangen des Datenschutzes führen, verzichtet werden sollte

oder

ob der Betreiber des Systems, der diesem Mißbrauch nur durch umfangreiche prophylaktische Speicherung begegnen könnte, verpflichtet werden sollte, diesen Mißbrauch zu seinen Lasten hinzunehmen, vergleichbar dem SB-Einzelhandel, der eine bestimmte Diebstahlsquote einkalkuliert.

Es sollte geprüft werden, ob es technisch möglich und kostenmäßig vertretbar wäre, bei ISDN-fähigen Endgeräten technische Vorkehrungen vorzusehen, die es ermöglichen, daß der anrufende Teilnehmer das Erscheinen seiner Rufnummer auf dem Display des Gerätes des angerufenen Teilnehmers fallweise unterbinden kann. In diesem Zusammenhang wäre zu klären, ob auf dem Gerät des angerufenen Teilnehmers dann erkennbar ist, ob der Anrufer sich nicht zu erkennen geben kann (weil er einen analogen Anschluß hat) oder ob der Anrufer das Erscheinen seiner Nummer — obwohl technisch möglich — unterdrückt.

Es ist darauf zu achten, daß für alle mit der Speicherung von Daten verbundenen Probleme EG-konforme Lösungen gefunden werden.

Der Ausschuß legt besonderen Nachdruck auf den zukünftig stärker zu beachtenden Aspekt der Daten*sicherheit* insbesondere auf den Übertragungsstrecken."

Zum Dreizehnten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz hat der Ausschuß für Post und Telekommunikation in der 12. Wahlperiode folgende Stellungnahme abgegeben:

„Der Ausschuß für Post und Telekommunikation hat in seiner 27. Sitzung am 14. Oktober 1992 die Unterrichtung durch den Bundesbeauftragten für den Datenschutz gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes (BDSG) — BT-Drucksache 12/553 — Ziffer 7.4 Telefondatenverarbeitung (Seite 44 des Berichts) beraten.

Er empfiehlt dem federführenden Innenausschuß einvernehmlich, hinsichtlich des Entwurfs einer Allgemeinen Verwaltungsvorschrift über die Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Bundesverwaltung (Dienstanschlußvorschriften — DAV —) auf eine Abkoppelung des datenschutzrechtlichen Teils vom haushaltsrechtlichen Teil zu drängen, um möglichst schnell ein Inkraftsetzen der DAV sicherzustellen."

Im übrigen hat er in seiner 29. Sitzung am 11. November 1992 die auf den Geschäftsbereich des Bundesministeriums für Post und Telekommunikation bezogenen Teile des Dreizehnten Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz zur Kenntnis genommen.

8. Der Ausschuß für Raumordnung, Bauwesen und Städtebau ist in der 12. Wahlperiode in seiner 6. Sitzung am 17. April 1991 übereingekommen, die Stellungnahme des Ausschusses für Raumordnung, Bauwesen und Städtebau des 11. Deutschen Bundestages vom 8. November 1989 zu dem Zehnten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz unverändert zu übernehmen und — beschränkt auf Ziffer 4.7 dieses Berichts — einvernehmlich Kenntnisnahme zu empfehlen.

Der Ausschuß hat in seiner 6. Sitzung am 17. April 1991 zudem beschlossen, die Stellungnahme des Ausschusses für Raumordnung, Bauwesen und Städtebau des 11. Deutschen Bundestages vom 16. Mai 1990 zum Elften Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz unverändert zu übernehmen und — beschränkt auf Ziffer 23.4 (Wohnungsvermietung) — dem federführenden Ausschuß zu empfehlen, den Bericht zustimmend zur Kenntnis zu nehmen und die

Fragen zu prüfen, ob der Umfang des Fragerechts des Vermieters gesetzlich geregelt werden sollte und ob die Grenzen im Vermieterinformationssystem bereichsspezifisch gesetzlich eindeutig bestimmt werden sollten.

Der Ausschuß hat sich des weiteren in seiner 27. Sitzung am 12. Februar 1992 mit dem Dreizehnten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz befaßt und sich dabei auf Kapitel 5 „Bauwesen" beschränkt. Er hat den Bericht insoweit zur Kenntnis genommen.

Der Ausschuß hat festgestellt, daß die datenschutzrechtlichen Defizite im Bundesministerium für Raumordnung, Bauwesen und Städtebau inzwischen behoben seien. Was die Mängel des § 5 AFWoG betrifft, erwartet der Ausschuß, daß neben Baden-Württemberg und Hamburg auch die übrigen Länder zu einer Regelung finden, die datenschutzrechtlich unbedenklich ist.

9. Der Ausschuß für Forschung, Technologie und Technikfolgenabschätzung hat in der 12. Wahlperiode seine Stellungnahme aus der 11. Wahlperiode zum Zehnten, Elften und Zwölften Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz bestätigt. In der 11. Wahlperiode hatte er den Zehnten, Elften und Zwölften Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz zur Kenntnis genommen.

10. In der 12. Wahlperiode hat der Ausschuß für Wahlprüfung, Immunität und Geschäftsordnung zum Zwölften Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz folgende Stellungnahme abgegeben:

„1. Der Ausschuß für Wahlprüfung, Immunität und Geschäftsordnung bestätigt den Hinweis des Bundesdatenschutzbeauftragten in seinem 12. Tätigkeitsbericht, daß das geltende Bundesdatenschutzgesetz nicht auf ‚die besonderen Fragen' eingeht, ‚die bei der Verarbeitung personenbezogener Daten durch den Deutschen Bundestag und seine Mitglieder auftreten' (BT-Drucksache 11/6458, S. 19, Tz. 2)

2. Der Ausschuß bekräftigt seine Absicht, eine geschäftsordnungsrechtliche Regelung des Datenschutzes im Bundestag zu verabschieden, wie er es bereits in seiner mitberatenden Stellungnahme vom 16. Mai 1990 zu den Gesetzentwürfen zur Änderung des Bundesdatenschutzgesetzes (BT-Drucksache 11/2175, 11/3729, 11/3730, 11/4306) verlangt hat.

3. Der Ausschuß empfiehlt dem federführenden Innenausschuß im übrigen, den 12. Tätigkeitsbericht des Datenschutzbeauftragten (BT-Drucksache 11/6458) zur Kenntnis zu nehmen."

Bezogen auf den Gesetzentwurf der Bundesregierung auf Drucksache 11/4306 hatte der Ausschuß für Wahlprüfung, Immunität und Geschäftsordnung der 11. Wahlperiode gutachtlich empfohlen, folgende Änderungen aufzunehmen:

1. In Artikel 1 wird in § 24 Abs. 3 folgender Satz 3 angefügt: „Der Bundesbeauftragte für den Datenschutz ist verpflichtet, den Deutschen Bundestag bei der Wahrnehmung der Aufgaben gemäß § 37a Satz 3 zu beraten, falls er dazu aufgefordert wird."

2. In Artikel 1 ist nach § 37 folgender § 37a einzufügen:

„§ 37a

Dieses Gesetz ist vom Deutschen Bundestag, seinem Präsidenten, seinen Mitgliedern und seinen Gliederungen anzuwenden, soweit von ihnen Verwaltungsaufgaben wahrgenommen werden. Gleiches gilt für Dritte, die die in Satz 1 Genannten in ihrer Tätigkeit unterstützen. Im übrigen regelt der Deutsche Bundestag für die Wahrnehmung seiner Aufgaben den Schutz personenbezogener Daten selbständig; §§ 8 und 24 Abs. 3 Satz 3 bleiben unberührt."

Der Ausschuß der 11. Wahlperiode hatte des weiteren zu den Gesetzentwürfen auf den Drucksachen 11/3730 und 11/2175 mitberatend und zu dem Gesetzentwurf auf Drucksache 11/4306 gutachtlich empfohlen, folgende Entschließung anzunehmen:

„Der Deutsche Bundestag stellt fest, daß das Bundesdatenschutzgesetz auf diejenigen Tätigkeiten des Parlaments, die nicht reine Verwaltungstätigkeit sind, keine Anwendung findet. Die verfassungsrechtlichen Vorschriften der Artikel 20, 38, 46 und 47 GG schließen es im System der Gewaltenteilung aus, den Deutschen Bundestag wie eine Exekutiveinrichtung zu behandeln und der Kontrolle durch den Bundesbeauftragten für den Datenschutz zu unterwerfen.

Der Deutsche Bundestag erklärt, daß er die Regelungslücke im geltenden Bundesdatenschutzgesetz schließen und den Datenschutz durch eigene Vorkehrungen sichern will. Er befindet sich dabei in Übereinstimmung mit den Feststellungen und Anregungen des Bundesbeauftragten für den Datenschutz im Zwölften Tätigkeitsbericht. Aus der neu in das Bundesdatenschutzgesetz eingeführten Vorschrift des § 37a leitet der Deutsche Bundestag folgende Selbstbindung ab, die er im einzelnen in der Geschäftsordnung des Deutschen Bundestages regeln wird:

Für die zu schaffende eigenständige Datenschutzregelung sollen die folgenden Leitlinien gelten:

1. Bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist nach Maßgabe der Grundsätze des Bundesdatenschutzgesetzes zu verfahren,

2. für die bei der Datenverarbeitung beschäftigten Personen gilt § 5 des Bundesdatenschutzgesetzes,

3. in einer Übersicht über die bei den einzelnen Stellen geführten Dateien sind Angaben aufzunehmen, die eine wirksame interne Datenschutzkontrolle ermöglichen,

4. ein internes Datenschutzkontrollorgan stellt die Einhaltung der eigenständigen Datenschutzregelung des Deutschen Bundestages sicher und überwacht die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme."

11. Der Finanzausschuß hat in der 12. Wahlperiode seine Voten zum Elften und Zwölften Tätigkeitsbericht aus der 11. Wahlperiode bestätigt. In der 11. Wahlperiode hatte er den Elften und Zwölften Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz zur Kenntnis genommen.

12. Der Ausschuß für Verkehr hat in der 12. Wahlperiode an seiner Stellungnahme aus der 11. Wahlperiode zum Elften und Zwölften Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz festgehalten.

    In der 11. Wahlperiode hatte er beschlossen, den Elften und Zwölften Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz zur Kenntnis zu nehmen und dem Innenausschuß mitgeteilt, die Fraktionen seien sich einig darüber gewesen, daß die Verfahrensweise der Deutschen Bundesbahn bei Führung der Kinder-Schwarzfahrerkartei und bei der Unterrichtung der Eltern nicht angemessen sei. Sie hätten sich vorbehalten, die Angelegenheit zunächst fraktionsintern zu beraten und diese dann nochmals zu gegebener Zeit aufzugreifen.

13. Der Ausschuß für Umwelt, Naturschutz und Reaktorsicherheit hat auf die Mitberatung des Zwölften Tätigkeitsberichts in der 11. und 12. Legislaturperiode verzichtet.

III. Zu den Beratungen im Innenausschuß

1. Zum Beratungsverfahren

Der Innenausschuß der 11. Wahlperiode hat den Zehnten und Elften Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz anberaten. Der Innenausschuß der 12. Wahlperiode hat die Beratungen in seiner 40. Sitzung am 7. Oktober 1992, seiner 41. Sitzung am 14. Oktober und seiner 42. Sitzung am 29. Oktober 1992 fortgesetzt.

Der Zwölfte Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz wurde ebenfalls durch den Innenausschuß der 11. Wahlperiode anberaten.

Der Innenausschuß der 12. Wahlperiode hat die Beratungen in seiner 5. Sitzung am 20. März 1991, der 40. Sitzung am 7. Oktober 1992, der 41. Sitzung am 14. Oktober 1992 sowie in der 42. Sitzung am 29. Oktober 1992 fortgesetzt.

Der Dreizehnte Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz wurde in der 40. Sitzung des Innenausschusses der 12. Wahlperiode am 7. Oktober 1992, der 41. Sitzung am 14. Oktober sowie in der 42. Sitzung am 29. Oktober 1992 beraten.

Den Beratungen im Innenausschuß lagen neben den Tätigkeitsberichten des Bundesbeauftragten für den Datenschutz insbesondere auch ausführliche Stellungnahmen der Bundesregierung zu den Tätigkeitsberichten zugrunde.

In seiner 47. Sitzung am 9. Dezember 1992 hat der Innenausschuß mit den Stimmen der Koalitionsfraktionen und der Fraktion der SPD bei Stimmenthaltung der Gruppen BÜNDNIS 90/DIE GRÜNEN und der PDS/Linke Liste die vorangestellte Beschlußempfehlung beschlossen.

Mit den Stimmen der Koalitionsfraktionen und der Fraktion der SPD, gegen die Stimme der Gruppe BÜNDNIS 90/DIE GRÜNEN bei Enthaltung der Gruppe der PDS/Linke Liste wurde folgender Antrag der Gruppe BÜNDNIS 90/DIE GRÜNEN zur Fassung der Beschlußempfehlung zum Zehnten, Elften, Zwölften und Dreizehnten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz abgelehnt:

„Der Innenausschuß wolle beschließen:

1. Der Bundestag sieht es als erforderlich an, daß die bestehende Regelungslücke für den Datenschutz in privaten Akten im Bundesdatenschutzgesetz (BDSG) unverzüglich geschlossen wird und fordert die Bundesregierung zur Vorlage eines entsprechenden Gesetzentwurfs auf.

2. Der Bundestag spricht sich dafür aus, mit einer Ergänzung zum BDSG — und einer Änderung der jeweiligen Geschäftsordnungen — eine Datenschutzregelung für den parlamentarischen Bereich des Bundestages und des Bundesrates einzuführen.

3. Der Bundestag spricht sich dafür aus, im Rahmen der von der Gemeinsamen Verfassungskommission vorbereiteten Änderung des Grundgesetzes den Datenschutz und die individuelle Informationsfreiheit (allgemeines Einsichtsrecht in Behördenakten wie z. B. in den USA) als Grundrechte zu verankern.

4. Der Bundestag fordert die Bundesregierung auf, unverzüglich Gesetzentwürfe zum Datenschutz in folgenden Bereichen vorzulegen, wo gemäß der Rechtsprechung des Bundesverfassungsgerichts der Übergangsbonus inzwischen abgelaufen ist und die praktizierte Datenverarbeitung rechtswidrig wird, wenn nicht sehr rasch präzise Regelungen ergehen:

   a) Arbeitnehmerdatenschutz

   b) Sicherheitsüberprüfungen

c) Ausländerzentralregister

d) Verbesserung des Datenschutzes der VerbraucherInnen, besonders bei Banken und Versicherungen

e) Verbot oder Einschränkung gentechnischer Maßnahmen an Menschen (z. B. zur Strafverfolgung, Arbeitnehmer-Screening u. a.)

f) Teile der Datenverarbeitung von Bundeskriminalamt und Bundesgrenzschutz mangels präziser Novelle zum BKA- und BGS-Gesetz

g) Speicherung von ISDN-Verbindungsdaten und sonstiger Kommunikationsdaten (z. B. anläßlich Fangschaltungen oder anderer Überwachungen).

5. Der Bundestag sieht es als notwendig an, Verbesserungen der datenschutzrechtlichen Vorschriften in folgenden Bereichen vorzunehmen:

a) Melderahmenrecht (u. a. Widerspruchsrecht gegen massenhafte Daten-Transfers an Parteien; Streichung der Hotelmeldepflicht sowie polizeilicher Zugriffsbefugnisse auf Hotel- und Krankenhaus-Unterlagen;

b) Verkehrszentralregister

c) Regelung der Datenverarbeitung im Schengener und EG-Rahmen (SIS/EIS, Verbesserung des neuen Richtlinienvorschlags der EG-Kommission; Verbesserung der Kontrolldichte der Datenschutzbeauftragten, u. a.)

6. Der Bundestag fordert die Bundesregierung auf, ihre Verwaltungspraxis im nachgeordneten Bereich datenschutzfreundlicher als bisher zu gestalten (z. B. Auskunftspraxis des Bundesamts für Verfassungsschutz; gesamter Bereich Post/Telekom; APIS-Datei des polizeilichen Staatsschutzes; u. a. m.)

7. Der Bundestag hält es für erforderlich, den Aufbau des Datenschutzes in den neuen Ländern weiter intensiv zu unterstützen. Hierzu muß dem Bundesbeauftragten für den Datenschutz das notwendige Personal zur Verfügung gestellt werden. Außerdem dürfen Daten-„Altlasten" aus der ehemaligen DDR (z. B. die PKZ) für Verwaltungszwecke grundsätzlich nicht weiter verwendet werden."

2. Zur Beschlußempfehlung

Die Beschlußempfehlung des Innenausschusses bezieht sich insbesondere auf Bereiche, deren Beratung seitens des Bundesbeauftragten für den Datenschutz als besonders wesentlich angesehen worden war.

Der Bundesbeauftragte hat im übrigen darauf hingewiesen, daß die seit der Zuleitung seiner Tätigkeitsberichte an den Deutschen Bundestag verstrichene Zeit dazu geführt habe, daß viele der in den Berichten aufgeführten datenschutzrechtlichen Probleme durch den Gesetzgeber, nach Erörterung in den mitberatenden Ausschüssen, oder als Folge weiterer Verhandlungen und Gespräche, die er mit der Bundesregierung und anderen beteiligten öffentlichen Stellen geführt habe, inzwischen gelöst seien. Mit zahlreichen weiteren Fragen, die in den Tätigkeitsberichten angesprochen seien, werde sich der Innenausschuß voraussichtlich in anderem Zusammenhang befassen können, insbesondere bei der Beratung der in seinen Berichten dringend empfohlenen Gesetze oder im Zusammenhang mit dem von der Bundesregierung vorzulegenden Bericht über das Zentrale Verkehrsinformationssystem ZEVIS.

Einige Fragen seien durch Zeitablauf weniger aktuell geworden. Bei anderen hätten sich durch Neuentwicklungen auch auf technischem Gebiet neue Gesichtspunkte ergeben, die eine Lösung der aufgezeigten Fragen in absehbarer Zeit ohne Inanspruchnahme des Innenausschusses als möglich erscheinen ließen.

a) *Zu Nummer 1* (Bundesamt für Verfassungsschutz)

aa) Neufassung der Verkartungspläne der einzelnen Abteilungen des Bundesamtes für Verfassungsschutz
(Elfter Tätigkeitsbericht Nr. 19.3, S. 67 f.)

Der Bundesbeauftragte für den Datenschutz hat gegenüber dem Innenausschuß darauf hingewiesen, daß für die Abteilungen IV und VIII des Bundesamtes für Verfassungsschutz im wesentlichen noch die verbesserungsbedürftigen Verkartungspläne gelten würden, auf die er im Elften Tätigkeitsbericht hingewiesen habe; bei den Verkartungsplänen der Abteilungen II, III und VI stehe 1¾ Jahre nach Inkrafttreten des neuen Verfassungsschutzgesetzes die Anpassung an das neue Recht immer noch aus, obwohl er auf die Notwendigkeit hingewiesen habe, sämtliche Verkartungspläne des Bundesamtes für Verfassungsschutz aufgrund der nunmehr eingetretenen veränderten Gesetzeslage, aber auch wegen der veränderten politischen Situation zu überarbeiten. Ein weiteres Zuwarten könne aber im Interesse der von Datenspeicherungen gerade in kritischen Randbereichen betroffenen Bürger nicht mehr hingenommen werden.

Der Innenausschuß hat sich einstimmig den o. g. Ausführungen des Bundesbeauftragten für den Datenschutz angeschlossen und die aus der Beschlußempfehlung ersichtliche Terminierung beschlossen.

bb) Auskunftserteilung durch das Bundesamt für Verfassungsschutz
(Dreizehnter Tätigkeitsbericht Nr. 19.1, S. 72 f.)

Der Bundesbeauftragte für den Datenschutz hat gegenüber dem Innenausschuß in Ergänzung seiner Ausführungen im Elften Tätigkeitsbericht vorgetragen, nach

§ 15 Abs. 1 des neuen Verfassungsschutzgesetzes erteile das Bundesamt für Verfassungsschutz (BfV) dem Betroffenen auf Antrag unentgeltlich Auskunft über die zu seiner Person gespeicherten Daten, soweit er hierzu auf einen konkreten Sachverhalt hinweise und ein besonderes Interesse an einer Auskunft darlege. Diese Regelung werde vom Bundesamt für Verfassungsschutz, offenbar mit Unterstützung des Bundesministeriums des Innern, in mehrfacher Hinsicht nicht im Sinne der Absicht des Gesetzgebers, die Position des Bürgers zu verbessern, ausgelegt: Das BfV lege § 15 Abs. 1 anscheinend so aus, daß es eine Auskunft nicht erteilen dürfe, wenn die in § 15 Abs. 1 BVerfSchG genannten Voraussetzungen nicht vorlägen. Es lehne Auskunftsbegehren ab, bei denen der Bürger nicht auf einen relevanten konkreten Sachverhalt hinweise, ohne zu prüfen, ob die Auskunft nicht doch ohne Gefahr für die Sicherheitsaufgaben des BfV erteilt werden könnte. Offenbar teile die Bundesregierung die Auffassung des BfV. Ein Verbot, Auskunft auch in Fällen zu erteilen, in denen der Betroffene nicht auf einen konkreten Sachverhalt hinweise, könne er indes § 15 Abs. 1 BVerfSchG nicht entnehmen. Die Vorschrift besage lediglich, daß der Betroffene, wenn er auf einen konkreten Sachverhalt hinweise und ein besonderes Interesse an einer Auskunft darlege, einen Rechtsanspruch auf Auskunft habe, sofern nicht die Voraussetzungen des Absatzes 2 vorlägen. Die Vorschrift verbiete aber keineswegs, dem Betroffenen im Rahmen der Ausübung pflichtgemäßen Ermessens auch dann Auskunft zu geben, wenn die Voraussetzungen des § 15 Abs. 1 nicht vorlägen und auch § 15 Abs. 2 einer Auskunftserteilung nicht entgegenstehe. Die Grundposition des BfV führe dazu, daß auch das Wort „soweit" in § 15 Abs. 1 dahin gehend verstanden werde, dem Bürger dürfe nur insoweit Auskunft erteilt werden, als er auf einen konkreten Sachverhalt hingewiesen und ein besonderes Interesse an der Auskunft dargelegt habe. Das führe zu Auskünften, die einen unrichtigen Eindruck vermittelten oder unvollständig seien. In diesen Fällen werde bei der derzeitigen Praxis nicht geprüft, ob man dem Betroffenen im Rahmen des nach § 15 Abs. 2 BVerfSchG Zulässigen noch weitere Auskunft geben könnte. Das BfV stelle zu hohe Anforderungen an den Hinweis auf einen konkreten Sachverhalt. In einer Reihe von Fällen trügen Bürger Sachverhalte vor, die zwar aus ihrer — unzutreffenden — nicht aber aus der Sicht des BfV zu einem Tätigwerden des BfV geführt haben könnten. Gerade in solchen Fällen könne es zur Beruhigung der Bürger beitragen, die Auskunft zu erteilen, daß beim BfV eine Speicherung — zumindest wegen des vorgetragenen Sachverhalts — nicht vorliege. In solchen Fällen trete erfahrungsgemäß auch eine Gefährdung der Aufgabenerfüllung des BfV durch eine Auskunftserteilung nicht ein. Die Regelung in § 15 Abs. 1 führe — insbesondere nach der Praxis des BfV — dazu, daß ein Betroffener, wenn er überhaupt eine Chance für eine Auskunft haben wolle, einen konkreten Sachverhalt vortragen müsse, „der — zumindest aus der Sicht eines verständigen Bürgers — geeignet erscheinen könnte, ein Tätigwerden des Verfassungsschutzes auszulösen". Damit werde vom Bürger eine Art Selbstbezichtigung verlangt, die verfassungsrechtlich bedenklich sei, (BVerfGE 65/1/46). Daß auch andere Regelungen möglich seien, zeigten z. B. die Verfassungsschutzgesetze der Länder Hessen und Schleswig-Holstein, die den Auskunftsanspruch des Bürgers nicht vom Vortrag eines konkreten Sachverhalts und der Darlegung eines besonderen Interesses an der Auskunft abhängig machten. Auch das bayerische Verfassungsschutzgesetz fordere als Voraussetzung für die nach pflichtgemäßem Ermessen zu erteilende Auskunft nicht den Hinweis auf einen konkreten Sachverhalt.

Der Innenausschuß hat sich Erfahrungsberichte der Bundesländer Schleswig-Holstein und Hessen zum Thema Auskunftserteilung durch den Verfassungsschutz nach Landesrecht geben lassen.

Die Landesregierung von Schleswig-Holstein hat zu der Thematik dargelegt, daß im Gegensatz zur Bundesregelung § 25 des schleswig-holsteinischen Verfassungsschutzgesetzes (LVerfSchG) weder einen Hinweis auf einen konkreten Sachverhalt noch die Darlegung eines besonderen Interesses an einer Auskunft durch die betroffene Bürgerin oder den betroffenen Bürger voraussetze. Die betroffene Person habe grundsätzlich einen Anspruch auf Auskunft. Der Antrag könne aber im Wege der Ermessensentscheidung nach § 25 Abs. 2 LVerfSchG ganz oder teilweise abgelehnt werden, wenn das öffentliche Interesse an der Geheimhaltung der Daten überwiege. Ein spürbar vermehrtes Antragsaufkommen sei kurz nach der Veröffentlichung des Verfassungsschutzgesetzes festgestellt worden. Gegenwärtig würden nur noch vereinzelt Anträge gestellt. Zusammenfassend könne festgestellt werden, daß die Auskunftsregelung des schleswig-holsteinischen Verfassungsschutzgesetzes den Belangen der Bürgerinnen und Bürger, aber auch den Sicherheitsinteressen der Verfassungsschutzbehörde im vollem Umfang gerecht werde. Neben einer Vollauskunft seien abgestufte Teilauskünfte bis hin zu einer Auskunftsverweigerung in begründeten Einzelfällen möglich. Durch die bislang erteilten Auskünfte hätten sich keine nega-

tiven Auswirkungen auf die Funktion der schleswig-holsteinischen Verfassungsschutzbehörde abgezeichnet. Versuche einer Ausforschungskampagne seien nicht festgestellt worden. Kritik an der Auskunftspraxis von seiten des Landesbeauftragten für den Datenschutz sei bislang nicht aufgekommen.

Die Regierung des Landes Hessen hat mitgeteilt, daß eine Neufassung des geltenden § 18 Hessischen LfV-Gesetzes nicht notwendig erscheine.

Der Innenausschuß hat sich den Vorschlägen des Bundesbeauftragten für den Datenschutz zur Anwendung des § 15 BVerfSchG in seiner Beschlußempfehlung weitgehend angeschlossen. Seitens der Fraktion der CDU/CSU und seitens der Bundesregierung wurde jedoch auch betont, es solle beim Wortlaut des § 15 BVerfSchG bleiben, der in schwierigen Verhandlungen zustande gekommen sei. Die Gesetzgebung dürfe nicht nur auf die augenblickliche Situation abstellen. In den 80er Jahren hätten beispielsweise linksorientierte Gruppen versucht, den Verfassungsschutz auszuforschen.

b) *Zu Nummer 2* (Beihilfeverfahren; eigenes Antragsrecht für Angehörige — Zwölfter Tätigkeitsbericht Nr. 6.6.1, S. 33f.)

Der Innenausschuß hat sich der Forderung des Bundesbeauftragten für den Datenschutz, durch Änderung der Beihilfevorschriften einen Beihilfeanspruch von Familienangehörigen eines Beihilfeberechtigten zuzulassen, nicht angeschlossen. Er ist vielmehr den Ausführungen der Bundesregierung gefolgt, die erklärt hat, aus der Fürsorgepflicht des Dienstherrn nach § 79 BBG ergäben sich keine eigenen Ansprüche von Angehörigen des Beihilfeberechtigten gegenüber dem Dienstherrn.

Seitens der Bundesregierung wurde betont, in der Praxis könnten die betreffenden Familienangehörigen ihre Belege unmittelbar der Beihilfestelle zuleiten, während der Beihilfeberechtigte hierauf lediglich pauschal Bezug nehme, z. B. indem er angebe, daß es um ein Rezept gehe. Es seien hieraus keine weiteren Rückschlüsse ziehbar. Desgleichen würden die Belege von der Beihilfestelle auch unmittelbar an das betroffene Familienmitglied zurückgesandt.

Der Innenausschuß hat sich der Auffassung der Bundesregierung angeschlossen, daß die vom Bundesbeauftragten für den Datenschutz angesprochenen Probleme durch eine vernünftige, praxisorientierte Gestaltung gelöst werden könnten, und geht davon aus, daß dies in der Praxis geschieht.

c) *Zu Nummer 3* (Wehrstammkarten der ehemaligen Nationalen Volksarmee — Dreizehnter Tätigkeitsbericht Nr. 2.13.3, S. 34)

Der Innenausschuß hat sich mit seiner Beschlußempfehlung zum Thema Wehrstammkarten der ehemaligen Nationalen Volksarmee einem Vorschlag des Bundesbeauftragten für den Datenschutz angeschlossen. Das Bundesministerium der Verteidigung hatte zunächst Bedenken gegen den Vorschlag geltend gemacht, weil es einen erheblichen Mehraufwand befürchtete, hat jedoch zugestanden, entsprechend dem Vorschlag des Bundesbeauftragten zu verfahren. Der Bundesbeauftragte für den Datenschutz hat den Innenausschuß davon unterrichtet, daß von den ursprünglich vereinbarungsgemäß zu löschenden 16 Datenfeldern sich das Datenfeld „Staatliche Auszeichnungen" mittlerweile als ein mögliches Beweismittel z. B. in Mauerschützenprozessen als unverzichtbar erwiesen habe, und er gegen diese Korrektur der zu löschenden Datenfelder keine Bedenken habe.

d) *Zu Nummer 4* (Telefondatenverarbeitung in der Bundesregierung; Dienstanschlußvorschriften — Zehnter Tätigkeitsbericht Nr. 7.3, S. 30/31; Elfter Tätigkeitsbericht Nr. 5.3, S. 26/27; Dreizehnter Tätigkeitsbericht Nr. 7.2; S. 44)

Der BfD hat in seinem Dreizehnten Tätigkeitsbericht beanstandet, daß der Entwurf der „Allgemeinen Verwaltungsvorschriften über die Einrichtung und Nutzung dienstlicher Fernmeldeanlagen für die Bundesverwaltung mit Ausnahme der Deutschen Bundespost (Dienstanschlußvorschriften — DAV)", aus Gründen, die nicht mit dem Datenschutz zusammenhingen, immer noch nicht in Kraft gesetzt worden sei. Der Entwurf dieser Allgemeinen Verwaltungsvorschriften berücksichtige seine Empfehlungen weitgehend.

Die Bundesregierung hat auf Seite 18 ihrer Stellungnahme zum Dreizehnten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz ausgeführt, die Verabschiedung der „Allgemeinen Verwaltungsvorschriften über die Einrichtung und Benutzung dienstlicher Fernmeldeanlagen für die Bundesverwaltung mit Ausnahme der Bundespost (Dienstanschlußvorschriften — DAV)" habe sich bisher verzögert, weil die Abstimmung zwischen den Ressorts noch nicht abgeschlossen werden konnte. Insbesondere sei weiterhin strittig, ob der Bundesminister für Post und Telekommunikation und die nachgeordneten Ämter außerhalb der Unternehmen der Deutschen Bundespost in die DAV einzubeziehen seien.

Im Innenausschuß wurde einstimmig auf eine baldige Inkraftsetzung der Dienstanschlußvorschriften gedrängt.

Seitens der Bundesregierung wurde versichert, daß die Dienstanschlußvorschriften zum 1. Januar 1993 in Kraft treten werden. Noch offene haushaltsrechtliche Fragen würden auf Arbeitsebene geklärt werden.

e) *Zu Nummer 5* (Bereichsspezifische Regelungen zum Arbeitsnehmerdatenschutz — gesetzliche Regelung der Sicherheitsüberprüfung)

Der Bundesbeauftragte für den Datenschutz hat erklärt, er fordere seit langem eine bereichsspezifische Regelung zum Arbeitnehmerdatenschutz. Die Bundesregierung habe bereits zugesagt, einen entsprechenden Gesetzentwurf noch in dieser Legislaturperiode vorzulegen.

Seitens der Bundesregierung wurde dargelegt, sie teile nicht die Auffassung der Gruppe BÜNDNIS 90/DIE GRÜNEN, daß sich für den Gesetzgeber aus der Rechtsprechung des Bundesverfassungsgerichts eine konkrete Frist zur Regelung des Arbeitnehmerdatenschutzes ergebe. Das Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 (Volkszählungsurteil) habe für den Schutz der informationellen Selbstbestimmung im nicht-öffentlichen Bereich, und damit auch im Arbeitsrecht, zwar Bedeutung. Jedoch gelte das Recht auf informationelle Selbstbestimmung als Grundrecht im Privatrechtsverkehr nicht unmittelbar; es sei vielmehr als objektive Wertentscheidung auch im Privatrecht zu berücksichtigen. Hierbei sei zu beachten, daß das Recht auf informationelle Selbstbestimmung mit anderen Grundrechten kollidieren könne und deshalb im Sinne einer Konkordanz der verfassungsrechtlichen Wertvorstellungen ein Ausgleich zwischen den verschiedenen Grundrechtspositionen vorzunehmen sei. Dies werde die Bundesregierung bei der gesetzlichen Regelung des Arbeitnehmerdatenschutzes berücksichtigen. Der Bundesminister für Arbeit und Sozialordnung habe die dazu erforderlichen umfangreichen Vorarbeiten aufgenommen.

Zum Thema gesetzliche Regelung der Sicherheitsüberprüfung hat der Bundesbeauftragte für den Datenschutz betont, eine dies betreffende Aufforderung sei bereits mit Beschluß vom 19. September 1990 (Plenarprotokoll) 11/225 S. 17789a) ergangen. Mit der Kabinettvorlage des zwischen den Ressorts bereits abgestimmten Entwurfs eines Sicherheitsüberprüfungsgesetzes sei noch für dieses Jahr zu rechnen.

Die Bundesregierung hat bestätigt, daß beabsichtigt sei, den Entwurf eines Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes im Dezember 1992 dem Kabinett zur Beratung und Beschlußfassung vorzulegen.

Der Innenausschuß hält eine Verabschiedung bereichsspezifischer Regelungen zum Arbeitnehmerdatenschutz sowie einer gesetzlichen Regelung der Sicherheitsüberprüfung, die den Vorgaben der Verfassungsrechtsprechung Rechnung trägt, noch in der 12. Legislaturperiode für notwendig.

f) *Zu Nummer 6* (Ausländerzentralregister)

Der Innenausschuß hat sich mit Nummer 6 seiner Beschlußempfehlung einer Forderung des Bundesbeauftragten für den Datenschutz angeschlossen.

Der Bundesbeauftragte für den Datenschutz hatte zu der Thematik ausgeführt, seit vielen Jahren habe er auf die Dringlichkeit hingewiesen, den Anforderungen des Bundesverfassungsgerichtes entsprechend eine gesetzliche Grundlage für die Verarbeitung personenbezogener Daten im Ausländerzentralregister zu schaffen. Ein von der Bundesregierung beim Deutschen Bundestag eingebrachter Entwurf (Drucksache 11/5828) sei in der 11. Legislaturperiode nicht abschließend beraten worden und müsse deshalb erneut eingebracht werden. Ein Arbeitspapier habe der Bundesminister mit Stand 15. Juli 1991 vorgelegt, zu dem er mit Schreiben vom 14. Oktober 1991 Stellung genommen habe. Auf die Dringlichkeit der Fortführung der Arbeiten an diesem Entwurf weise er hin; aus seiner Sicht seien vorrangige und nachdrückliche Bemühungen erforderlich, wenn der Entwurf noch in dieser Legislaturperiode Gesetz werden solle.

Seitens der Bundesregierung wurde dargelegt, das Bundesverfassungsgericht habe den Übergangsbonus nicht näher definiert, insbesondere keine Frist gesetzt. Es bestehe die politische Absicht, das Gesetz so rasch wie möglich, jedenfalls in dieser Legislaturperiode, in Kraft zu setzen. Den vom Bundesminister des Innern erlassenen vorläufigen Richtlinien sei zu entnehmen, daß bereits jetzt der Datenschutz zugunsten der Ausländer im vollen Umfang angewandt und beachtet werde.

g) *Zu Nummer 7* (Verbot oder Einschränkung genomanalytischer Untersuchungen — u. a. Dreizehnter Tätigkeitsbericht Nr. 4.2, S. 39 ff.)

Der Bundesbeauftragte für den Datenschutz hat zu der Thematik ausgeführt, an dem Konzept, die Bemühungen um die Genomanalyse im Strafverfahren nicht mit der Vorbereitung des Strafverfahrensänderungsgesetzes zu koppeln, solle festgehalten werden. Die Stellungnahme der Bundesregierung zum Dreizehnten Tätigkeitsbericht, Seite 15, wonach „die Erarbeitung spezieller gesetzlicher Regelungen ... nicht aufgegeben worden" sei, sei wenig aussagekräftig. Er habe erneut und wiederholt die Unerläßlichkeit einer Regelung in dieser Legislaturperiode betont und — mit Blick auf die erforderliche gründliche Beratung in den gesetzgebenden Körperschaften — auf die Notwendigkeit zügiger Fortsetzung der Arbeiten hingewiesen. Der Bundesminister der Justiz habe erklärt, daß die mit der Verwirklichung der

deutschen Einheit verbundenen besonderen Belastungen zwar dazu geführt hätten, daß die Arbeiten etwas an Vordringlichkeit eingebüßt hätten. Aus Gründen der Klarstellung werde aber nach wie vor die Schaffung einer besonderen gesetzlichen Regelung für den genetischen Fingerabdruck befürwortet, um den in weiten Teilen der Bevölkerung anzutreffenden, mit der Gentechnik ganz allgemein verbundenen Befürchtungen zu begegnen, der Einsatz solcher Untersuchungen im Strafverfahren führe zu übermäßigen, den Kern der Persönlichkeit berührenden Eingriffen. Inzwischen habe ihm der Bundesminister der Justiz — parallel zur Beteiligung der Landesjustizverwaltungen — Anfang d. J. einen neuen überarbeiteten Referentenentwurf zugänglich gemacht, zu dem er im März d. J. eine eingehende Stellungnahme abgegeben habe. Er würde begrüßen, wenn diese Arbeiten mit Nachdruck weiter verfolgt würden. Die Versicherungswirtschaft in der Bundesrepublik Deutschland zeige weiterhin die von der Enquete-Kommission des Deutschen Bundestages „Chancen und Risiken der Gentechnologie" in ihrem Bericht vom 6. Januar 1987 (Drucksache 10/6775, S. 174) bescheinigte Zurückhaltung hinsichtlich des Einsatzes von genetischen Tests, die Auskunft über den Gesundheitszustand und die Lebenserwartung des Versicherungsnehmers geben sollten. Diese Zurückhaltung sei von Versicherungen in anderen Mitgliedstaaten der EG aber bereits aufgegeben worden. In seinem Schreiben vom 8. Oktober 1991 an die mit Fragen der Genomanalyse beschäftigten Ausschüsse des Deutschen Bundestages habe er bedauert, daß die Bundesregierung z. Z. keinen Handlungsbedarf in diesem Bereich sehe (vgl. Drucksache 11/8520, S. 23). Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder habe in ihrer Entschließung vom 26./27. Oktober 1989 Genomanalysen im Versicherungswesen als grundsätzlich nicht erforderlich sowie mit dem Prinzip der Versicherungen als unvereinbar bezeichnet, Risiken abzudecken und nicht auszuschließen, und eine entsprechende Klarstellung im Versicherungsvertragsgesetz gefordert. In seinem Schreiben vom 8. Oktober 1991 habe er ebenfalls bedauert, daß sich die Bundesregierung noch nicht dazu entschließen konnte, den Einsatz genomanalytischer Methoden im Arbeitsverhältnis gesetzlich zu verbieten. Aus datenschutzrechtlicher Sicht sei das gesetzliche Verbot genomanalytischer Methoden in diesem Bereich die einzige Möglichkeit, das Recht auf informationelle Selbstbestimmung des Arbeitnehmers zu sichern.

Die Bundesregierung hat zu der Thematik dargelegt, Anfang 1992 sei vom Bundesministerium der Justiz ein Referentenentwurf einer gesetzlichen Regelung zur Verwendung des genetischen Fingerabdrucks für Zwecke der Strafverfolgung an die zu beteiligenden Stellen (Landesjustizverwaltungen, BGH, GBA, BMI, BfD, Verbände) zur Stellungnahme versandt worden. Der Entwurf sei zwischenzeitlich auf der Grundlage der eingegangenen Stellungnahmen überarbeitet worden. Er solle demnächst den Bundesressorts zur Abstimmung zugeleitet werden. Der Gesetzentwurf verfolge das Ziel, den Einsatz gentechnischer Maßnahmen durch normklare Festlegung der Voraussetzungen und Beschränkungen einzugrenzen. Vorgeschlagen werde eine Regelung über Voraussetzungen und Inhalt der Untersuchung mit genomanalytischen Methoden, verfahrenssichernde Rahmenbedingungen sowie Vorschriften über die Verwendung von Untersuchungsmaterial und seine Vernichtung.

Der Innenausschuß hält die Schaffung spezieller gesetzlicher Regelungen für notwendig.

h) *Zu Nummer 8* (Novelle zum Bundeskriminalamtgesetz und Bundesgrenzschutzgesetz)

Der Bundesbeauftragte für den Datenschutz hat erklärt, nach Abgabe des Dreizehnten Tätigkeitsberichts (dort Nummer 17.1, S. 70) habe sich der Sachstand zum Entwurfsverfahren eines neuen BGSG nicht fortentwickelt. Für ein neues BKAG sei im Oktober d. J. ein überarbeiteter Referentenentwurf vorgelegt worden, der seine früheren Vorschläge im wesentlichen unberücksichtigt lasse. Er gehe davon aus, daß nicht mit einem kurzfristigen Abschluß der Ressortabstimmung zu rechnen sein werde.

Seitens der Bundesregierung wurde bestätigt, unabhängig von der Frage, inwieweit über den rein rechtspolitischen Handlungsbedarf hinaus vor dem Hintergrund des sog. „Übergangsbonus" verfassungsrechtlich notwendiger Regelungsbedarf bestehe, liefen derzeit die Arbeiten an der Novellierung des Bundeskriminalamtgesetzes zur Schaffung bereichsspezifischer Datenschutzregelungen. Zur Zeit befinde sich der Entwurf in der Abstimmung zwischen den Ressorts. Ein Entwurf einer umfassenden Novellierung des Bundesgrenzschutzgesetzes, in dem die notwendigen bereichsspezifischen Datenschutzregelungen aufgenommen worden seien, sei erarbeitet und werde derzeit im Bundesministerium des Innern und im nachgeordneten Bereich abgestimmt. Beide Entwürfe würden sobald wie möglich zur Beschlußfassung vorgelegt.

Der Innenausschuß hält es für erforderlich, die Rechtsvorschriften über die Verarbeitung personenbezogener Daten im BKA- und BGS-Gesetz noch in dieser Legislaturperiode zu verabschieden.

i) *Zu Nummer 9* (ISDN-Verbindungsdaten und sonstige Kommunikationsdaten)

Mit Nummer 9 der Beschlußempfehlung hat sich der Innenausschuß einer Forderung des Bundesbeauftragten für den Datenschutz angeschlossen. Dieser hatte zur Begründung ausgeführt, die Speicherung von ISDN-Verbindungs-

daten und sonstigen Kommunikationsdaten — auch im Zusammenhang mit Fangschaltungen usw. — sei in der Telekom-Datenschutzverordnung (TDSV) und der Teledienstunternehmen-Datenschutzverordnung (UDSV) geregelt. In der „Fangschaltungsentscheidung" vom 25. März 1992 — 1 BvR 1430/88 — habe das Bundesverfassungsgericht das Fehlen einer verfassungsgemäßen gesetzlichen Grundlage jedenfalls für diejenigen in der TDSV geregelten Sachverhalte festgestellt, die dem Schutz des Fernmeldegeheimnisses aus Artikel 10 Abs. 1 Grundgesetz unterlägen, und den Gesetzgeber aufgefordert, alsbald einen verfassungsgemäßen Zustand herzustellen. Er habe bereits im Juni d. J. dem Bundesminister für Post und Telekommunikation einige Punkte als Konsequenz aus der genannten Entscheidung mitgeteilt und sei seitdem mit ihm in dieser Angelegenheit im Gespräch.

Seitens der Bundesregierung wurde betont, der Bundesminister für Post und Telekommunikation sei unverzüglich in die Prüfung der aus dem Verfassungsgerichtsbeschluß zu ziehenden Folgerungen sowohl für die technisch-betrieblichen Abläufe bei der Deutschen Bundespost TELEKOM als auch für die erforderliche gesetzliche Regelung eingetreten. Dabei sei die Komplexität vorläufiger und im Endzustand anzustrebender Lösungen deutlich geworden, die sowohl die verfassungsrechtlichen Anforderungen beachteten, als auch die Anfrage der Allgemeinheit nach Telekommunikationsdienstleistungen, und bestimmte damit verbundene Sachverhalte angemessen berücksichtigten. Erste Gespräche mit dem Bundesbeauftragten für den Datenschutz (BfD) zu der Frage, in welcher Weise die Entscheidung des Bundesverfassungsgerichts zweckmäßig umzusetzen sei, seien unmittelbar danach geführt worden. Ausgehend von den Ergebnissen dieser Unterredungen seien mittlerweile erste Formulierungsvorschläge einer gesetzlichen Ermächtigungsgrundlage für Eingriffe in das Fernmeldegeheimnis von der dazu eingerichteten Arbeitsgruppe erarbeitet worden. Es sei vorgesehen, diese Formulierungsvorschläge dem — derzeit über den Sachstand der Arbeitsgruppe unterrichteten — Bundesbeauftragten für den Datenschutz in Kürze zuzuleiten. Der Bundesbeauftragte für den Datenschutz werde sodann — entsprechend der vom Bundesminister für Post und Telekommunikation gegebenen Zusage — zu den Sitzungen der Arbeitsgruppe fallweise eingeladen werden. Auch würden die Erörterungen mit den betroffenen Ressorts alsbald fortgesetzt. Zudem wurde darauf hingewiesen, daß das Bundesverfassungsgericht den zeitlichen Übergangsraum bis zu einer gesetzlichen Regelung nicht eingegrenzt habe, so daß eine Gesetzesanpassung ggf. im Rahmen einer Poststrukturreform II, spätestens aber noch in dieser Legislaturperiode erfolgen werde.

3. Weitere erörterte Themen

Der Innenausschuß hat sich neben den in der Beschlußempfehlung angesprochenen Punkten auch mit der Thematik „Datenschutz im Beitrittsgebiet" befaßt (siehe Dreizehnter Tätigkeitsbericht Nr. 2, S. 17 ff.). Er hat sich insbesondere zu folgenden Bereichen aktualisierte Berichte geben lassen:

— Stand der Datenschutzgesetzgebung in den einzelnen Ländern

— Einheitliche Regelung durch die Innenministerkonferenz der Länder für die Einstellungs- und Personalfragebögen (S. 25 des Dreizehnten Tätigkeitsberichts)

— Ersetzung der Personenkennzahl in „angemessener Frist" (Verpflichtung durch den Einigungsvertrag) (S. 28 des Dreizehnten Tätigkeitsberichts)

— Stand des Sozialdatenschutzes in der Arbeitsverwaltung (S. 31 f. des Dreizehnten Tätigkeitsberichts)

— Krebsregister (S. 32 f. des Dreizehnten Tätigkeitsberichts)

— Datenspeicher „Gesellschaftliches Arbeitsvermögen" — Nutzung einer anonymisierten Kopie durch die BfA — Voraussetzungen (S. 35 des Dreizehnten Tätigkeitsberichts).

Der Innenausschuß hat es jedoch für entbehrlich gehalten, diese Themen im Rahmen der Beschlußempfehlung aufzugreifen. Dies gilt auch für zahlreiche im Antrag der Gruppe BÜNDNIS 90/DIE GRÜNEN angesprochenen Themen.

Bonn, den 21. Dezember 1992

Dr. Heribert Blens **Dr. Burkhard Hirsch** **Peter Paterna**

Berichterstatter

Anlage 2 (zu 1.5, 5.1.1)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. Juni 1991 — gegen die Stimme Bayerns — zum Bundesratsentwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität

Schon seit Jahren haben Datenschutzbeauftragte von Bund und Ländern eine angemessene gesetzliche Regelung zu den in die Freiheitsrechte der Bürger eingreifenden Strafverfolgungsmaßnahmen, wie der Rasterfahndung, des Einsatzes Verdeckter Ermittler und des Einsatzes besonderer technischer Observationsmittel gefordert. Sie bedauern, daß hierzu die Bundesregierung nicht schon längst einen Entwurf vorgelegt hat. Der Bundesrat mit seinem Ende April 1991 beschlossenen Gesetzentwurf wird diesem Anliegen ebenfalls nicht gerecht.

Zum Schutz der Persönlichkeitsrechte der Bürger wie im Interesse wirksamer Aufgabenerfüllung durch die Strafverfolgungsorgane bedarf es klarer Rechtsgrundlagen. Der Datenschutz stellt sich Bemühungen nicht entgegen, den zunehmenden Herausforderungen, denen die Bürger unseres Staates durch die organisierte Kriminalität, insbesondere durch die Drogenkriminalität, ausgesetzt sind, in erforderlicher Weise zu begegnen. Über dieses Ziel schießt der Bundesratsentwurf aber hinaus. Zwar enthält der Entwurf gegenüber früheren Vorschlägen des Bundesrates insofern eine Verbesserung, als nunmehr die Rasterfahndung und der Einsatz Verdeckter Ermittler an einen Straftatenkatalog gebunden werden sollen. Es bestehen aber weiterhin Bedenken, daß schwerwiegende Eingriffe in die Privatsphäre, wie der Einsatz von Peilsendern, schon bei „Straftaten von erheblicher Bedeutung" möglich sind.

Mit diesem schwammigen Begriff statt eines präzisen Kataloges von Straftaten wird der Einsatz der geheimen Ermittlungsmethoden weit über den Bereich der organisierten Kriminalität hinaus ausgedehnt. Diese Mittel werden damit für sämtliche Straftaten außerhalb der Bagatell- und Kleinkriminalität verfügbar.

Nach dem Gesetzentwurf wären auch über völlig unbeteiligte Personen heimliche Bild- und Filmaufnahmen zulässig, wenn es „der Erforschung des Sachverhalts" oder der „Aufenthaltsermittlung des Täters" dient. Gegen unverdächtige Personen sollen Wanzen und Peilsender eingesetzt werden können, wenn eine „Verbindung" — was immer darunter verstanden werden soll — mit dem Täter vermutet wird.

Selbst in privaten Wohnungen sollen Gespräche, die im Beisein eines Verdeckten Ermittlers geführt werden, heimlich abgehört und aufgezeichnet werden.

Es ist außerdem problematisch, daß derart schwerwiegende Eingriffe wie der Einsatz Verdeckter Ermittler nach dem Gesetzentwurf nicht in allen Fällen vom Richter angeordnet werden müssen, sondern weitgehende Eilkompetenzen für Polizei und Staatsanwaltschaft vorgesehen sind.

Ein weiteres Problem liegt darin, daß durch den Einsatz geheimer Ermittlungsmethoden gewonnene Informationen in zu weitem Umfang für andere Zwecke verwendet werden können. Offen bleibt insbesondere, ob die gewonnenen Erkenntnisse der Polizei für eine jahrelange Speicherung zur vorbeugenden Straftatenbekämpfung überlassen werden dürfen. Dies sieht der Gesetzentwurf undifferenziert nicht nur für Tatverdächtige, sondern sogar für andere Personen wie Begleiter oder zufällig betroffene Dritte vor.

Die Datenschutzbeauftragten halten es deshalb für dringend geboten, daß Bundestag und Bundesrat im weiteren Gesetzgebungsverfahren diese Probleme aufgreifen und die — wiederholt geäußerten — datenschutzrechtlichen Vorschläge berücksichtigt werden. Die Stellungnahme der Bundesregierung zu dem Entwurf des Bundesrates sollte diese Bemühungen unterstützen.

Anlage 3 (zu 1.8, 9.2)

Entschließung der 42. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1991 zum Datenschutz im Recht des öffentlichen Dienstes

I.

Die Daten von Arbeitnehmern werden im Laufe ihres beruflichen Lebens in vielfältiger Weise vom Arbeitgeber verarbeitet. Allein schon im Hinblick auf die große Zahl der über Arbeitnehmer erhobenen Daten und mit Rücksicht auf die Abhängigkeit des Arbeitnehmers vom Arbeitgeber ist eine gesetzliche Regelung der Verarbeitung von Personaldaten zwingend erforderlich. Auch gegenüber Beamten und anderen im öffentlichen Dienst Tätigen kann die Verarbeitung ihrer Daten nicht allein auf die hergebrachten Grundsätze des Berufsbeamtentums gestützt oder in Verwaltungsvorschriften geregelt werden. Vielmehr ist eine gesetzliche Grundlage vonnöten. Sie muß umso konkreter sein, je tiefer in das Persönlichkeitsrecht der Betroffenen eingegriffen wird.

II.

In der Auseinandersetzung um das Recht des öffentlichen Dienstes beeinträchtigen zwei grundlegende Fehleinschätzungen eine angemessene Regelung des Datenschutzes. Es trifft nicht zu, daß die Kenntnis des Dienstherrn über seine Bediensteten alle persönlichen Lebensumstände vollständig und lückenlos umfassen muß. Es ist ferner unrichtig, daß gesetzliche Regelungen überflüssig sind, weil stets die Einwilligung der Betroffenen eingeholt werden kann.

Zum einen wäre es mit der Würde des Menschen unvereinbar, wollte man ihn in seiner ganzen Persönlichkeit registrieren. Zwar ist der Angehörige des öffentlichen Dienstes dem Staat gegenüber besonders eng verpflichtet; er bleibt aber auch gegenüber seinem Dienstherrn Grundrechtsträger: Auch seine personenbezogenen Daten dürfen nur erhoben und verarbeitet werden, soweit das für die Begründung und Abwicklung des Dienstverhältnisses erforderlich ist.

Zum anderen macht der Rückgriff auf die Einwilligung gesetzliche Regelungen keineswegs überflüssig. Zwar ist die Erhebung und Verarbeitung personenbezogener Daten mit Einwilligung des Betroffenen grundsätzlich auch dann zulässig, wenn eine gesetzliche Grundlage fehlt. Die Einwilligung wird jedoch zur Farce, wenn sie faktisch erzwungen wird, weil z. B. eine Bewerbung ohne Einwilligung nicht berücksichtigt wird. Soweit bestimmte Angaben verfügbar sein müssen, sind sie gesetzlich präzise vorzuschreiben, aber zugleich auf den erforderlichen Umfang zu begrenzen.

III.

Neben der Neuordnung des Personalaktenrechts bedürfen auch andere Teilbereiche des öffentlichen Dienstrechts der datenschutzgerechten gesetzlichen Regelung. Die Konferenz der Datenschutzbeauftragten des Bundes und Länder hält insbesondere die Lösung folgender Probleme für vorrangig:

1. Bewerbung um Einstellung in den öffentlichen Dienst

Es ist — für den Bewerber transparent — festzulegen,

- welche personenbezogenen Informationen von ihm verlangt bzw. über ihn eingeholt, wie sie genutzt werden dürfen und wann sie zu löschen sind,
- ob und unter welchen Voraussetzungen und in welchem Stadium des Verfahrens der Bewerber sich Tests, Untersuchungen und Überprüfungen zu unterziehen hat,
- ob und inwieweit private Institutionen daran mitwirken und welche vertraglichen Sicherungen zum Schutz personenbezogener Daten zu vereinbaren sind,
- daß die Daten jeweils erst zu dem Zeitpunkt, in dem sie für das Verfahren erforderlich werden, und mit dem geringstmöglichen Eingriff erhoben werden.

2. Sicherheitsüberprüfungen

Es ist bereichsspezifisch gesetzlich festzulegen,

- wer im öffentlichen Dienst einer Sicherheitsüberprüfung unterzogen wird,
- welche personenbezogenen Daten dafür erhoben und verarbeitet werden,
- wie das Verfahren gestaltet wird, insbesondere welche Stellen mit welchen Befugnissen am Verfahren beteiligt sind und unter welchen Voraussetzungen Sicherheitsbedenken anzunehmen sind,
- daß die im Rahmen der Sicherheitsüberprüfung erhobenen Daten grundsätzlich nur für diesen Zweck verwendet werden dürfen,
- daß der Betroffene über das Ergebnis der Sicherheitsüberprüfung zu unterrichten ist.*)

*) Auf ihre Forderungen zur Sicherheitsüberprüfung (Geheimschutzgesetz) in den Entschließungen vom 13. September 1985, 18. April 1986 und 22. März 1990 nimmt die Konferenz Bezug.

3. Ärztliche Untersuchung

Es ist durch Gesetz oder ergänzende Rechtsverordnung festzulegen,

- unter welchen Voraussetzungen die ärztliche Untersuchung eines Bewerbers oder Bediensteten angeordnet werden kann,
- daß jede ärztliche Untersuchung einen präzisen Untersuchungsauftrag voraussetzt, der Anlaß und Gegenstand der Untersuchung möglichst exakt definiert und den Umfang der Untersuchung eingrenzt,
- wie das Arztgeheimnis und der Datenschutz sicherzustellen sind,
- wann und in welchem Umfang Versicherungen und früher behandelnde Ärzte über frühere Untersuchungen und Maßnahmen befragt werden und diese offenbaren dürfen,
- daß Ärzte und Versicherungen Daten nicht ohne Kenntnis des Betroffenen und nur mit Einwilligung des Bewerbers offenbaren dürfen,
- daß die Unterlagen der ärztlichen Untersuchungen nicht für andere Zwecke verwendet werden und nicht mit solchen vermengt werden dürfen, die anderen Zwecke dienen, und daß sie zu vernichten sind, sobald sie nicht mehr benötigt werden,
- daß der Arzt der personalverwaltenden Stelle nur das Endergebnis seiner Untersuchungen und — soweit erforderlich — nur tätigkeitsbezogene Risiken mitzuteilen hat,
- daß dem Betroffenen ein Recht auf Einsicht in die beim Arzt verbliebenen Untersuchungsunterlagen zusteht.

4. Beihilfen

Gesetzlich festzulegen sind die Grundlagen eines datenschutzgerechten Beihilfeverfahrens, insbesondere die Abschottung der Beihilfestelle, das Verbot automatisierter Speicherung von Diagnosedaten und anderen medizinischen Einzelangaben, die Zweckbindung der Daten sowie ein eigener Beihilfeanspruch der Angehörigen.

5. Personalinformationssysteme

Es muß dienstrechtlich gewährleistet sein, daß

- automatisierte Systeme zur Verarbeitung von Personaldaten zu unterschiedlichen Zwecken (z. B. Urlaubsdatei, Telefondatenerfassung, PC-Betriebsdaten) nicht zu umfassenden Persönlichkeitsprofilen verknüpft werden,
- alle vorgesehenen Auswertungen von Personaldaten in einer Übersicht, die dem Betroffenen zugänglich sein muß, zusammengefaßt werden,
- Kontrollen der Bediensteten mit Hilfe automatisierter Systeme unzulässig sind; Ausnahmen bedürfen einer gesetzlichen, insbesondere personalvertretungsrechtlichen Regelung.

IV.

Die Datenschutzbeauftragen des Bundes und der Länder fordern die für das Personalrecht zuständigen Minister und den Gesetzgeber auf, die auf der Grundlage der Rechtsprechung des Bundesverfassungsgerichts verfassungsrechtlich notwendigen Vorschriften zu erlassen.

Anlage 4 (zu 1.8, 9.1)

Entschließung der 43. Konferenzder Datenschutzbeauftragten des Bundes und der Länder vom 23./24. März 1992 zum Arbeitnehmerdatenschutz

I.

Im Rahmen des Arbeitsverhältnisses werden personenbezogene Daten aus ganz unterschiedlichen Lebensbereichen des Arbeitnehmers erhoben und gespeichert. Diese Daten verwendet der Arbeitgeber nicht nur für eigene Zwecke. Aus dem Arbeitsverhältnis ergeben sich auch Auskunfts-, Bescheinigungs- und Meldepflichten, die der Arbeitgeber gegenüber öffentlichen Stellen zu erfüllen hat. Durch die Möglichkeit, im Arbeitsverhältnis anfallende personenbezogene Daten miteinander zu verknüpfen und sie — losgelöst vom Erhebungszweck — für andere Verwendungen zu nutzen, entstehen Gefahren für das Persönlichkeitsrecht des Arbeitnehmers. Mit der Intensität der Datenverarbeitung, insbesondere durch Personalinformationssysteme und digitale Telekommunikationsanlagen, nehmen die Kontroll- und Überwachungsmöglichkeiten des Arbeitgebers zu.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb bereits seit 1984 bereichsspezifische und präzise gesetzliche Bestimmungen zum Arbeitnehmerdatenschutz. Bundestag, Bundesrat und Bundesregierung haben ebenfalls eine Regelungsnotwendigkeit bejaht; gleichwohl stehen bundesgesetzliche Regelungen über den allgemeinen Arbeitnehmerdatenschutz immer noch aus.

Die Notwendigkeit zur gesetzlichen Regelung besteht unabhängig davon, ob Arbeitnehmerdaten in automatisierten Dateien, in Akten oder in sonstigen Unterlagen verarbeitet werden. Der erhöhten Gefährdung durch die automatisierte Datenverarbeitung ist durch spezifische Schutzvorschriften Rechnung zu tragen.

Angesichts der besonderen Abhängigkeit des Arbeitnehmers im Arbeitsverhältnis und während der Phase einer Bewerbung um einen Arbeitsplatz ist durch Gesetz zu untersagen, daß Rechte, die dem Arbeitnehmer nach einschlägigen Datenschutzvorschriften zustehen, durch Rechtsgeschäft, Tarifvertrag und Dienst- oder Betriebsvereinbarung ausgeschlossen werden. Außerdem ist durch Gesetz festzulegen, daß eine Einwilligung des Arbeitnehmers oder Bewerbers nur dann als Grundlage einer Datenerhebung, -verarbeitung oder -nutzung in Frage kommt, wenn die Freiwilligkeit der Einwilligung sichergestellt ist, also die Einwilligung ohne Furcht vor Nachteilen verweigert werden kann. Deshalb dürfen allein aufgrund einer Einwilligung z. B. keine Gesundheitszeugnisse, Ergebnisse von Genomanalysen u.ä. angefordert werden, wenn sie den Rahmen des Fragerechts des Arbeitgebers überschreiten.

II.

Die gesetzliche Ausgestaltung des Arbeitnehmerdatenschutzes muß insbesondere folgende Grundsätze beachten:

1. Die Datenerhebung muß grundsätzlich beim Arbeitnehmer erfolgen.

2. Der Arbeitgeber darf Daten des Arbeitnehmers — auch durch Befragen des Arbeitnehmers oder Bewerbers — nur erheben, verarbeiten oder nutzen, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Arbeitsverhältnisses erforderlich oder sonst gesetzlich vorgesehen ist. Dabei ist der Grundsatz der Zweckbindung zu beachten. Auch ist zwischen der Bewerbungs- und Einstellungsphase zu unterscheiden.

3. Der Arbeitgeber darf Daten, die er aufgrund gesetzlicher Vorgaben für andere Stellen (z. B. Sozialversicherungsträger) erheben muß, nur für diesen Zweck verwenden.

4. Eine Datenauswertung und -verknüpfung, die zur Herstellung eines umfassenden Persönlichkeitsprofils des Arbeitnehmers führen kann, ist unzulässig.

5. Beurteilungen und Personalauswahlentscheidungen dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden.

6. Notwendige Datenübermittlungen zwischen Arzt und Arbeitgeber sind eindeutig zu regeln. Dem Arbeitgeber darf grundsätzlich nur das Ergebnis der ärztlichen Untersuchung zugänglich gemacht werden. Darüber hinaus dürfen ihm — soweit erforderlich — nur tätigkeitsbezogene Risikofaktoren mitgeteilt werden. Medizinische und psychologische Befunde sind getrennt von den übrigen Personalunterlagen aufzubewahren. Die Ergebnisse medizinischer oder psychologischer Untersuchungen und Tests des Beschäftigten dürfen automatisiert nur verarbeitet werden, wenn dies dem Schutz des Beschäftigten dient.

7. Dem Arbeitnehmer sind umfassende Auskunfts- und Einsichtsrechte in die Unterlagen einzuräumen, die sein Arbeitsverhältnis betreffen. Diese Rechte müssen sich auch auf Herkunft, Verarbeitungszwecke und Empfänger der Daten sowie die Art und Weise ihrer Auswertung erstrecken.

8. Dem Personal-/Betriebsrat muß ein Mitbestimmungsrecht bei der Einführung, Anwendung und der wesentlichen Änderung von automatisierten Dateien mit personenbezogenen Daten der Arbeitnehmer für Zwecke der Personalverwaltung zustehen. Das gilt auch bei sonstigen technischen Einrichtungen, mit denen das Verhalten und die Leistung der Beschäftigten überwacht werden kann.

9. Gesetzlich festzulegen ist, welche Daten der Arbeitnehmervertretung für ihre Aufgabenerfüllung zugänglich sein müssen und wie der Datenschutz bei der Verarbeitung von Arbeitnehmerdaten im Bereich der Arbeitnehmervertretung gewährleistet wird. Regelungsbedürftig ist auch das Verhältnis zwischen dem Personal-/Betriebsrat und dem behördlichen/betrieblichen Datenschutzbeauftragten.

10. Die Befugnis des Personal-/Betriebsrats, sich unmittelbar an die Datenschutzkontrollinstanzen zu wenden, ist gesetzlich klarzustellen.

11. Arbeitnehmerdaten dürfen nur dann ins Ausland übermittelt werden, wenn dort ein dem deutschen Recht vergleichbarer Datenschutzstandard gewährleistet ist oder wenn der Betroffene nach den oben genannten Grundsätzen (vgl. Abschnitt I Abs. 4) eingewilligt hat.

Anlage 5 (zu 1.8, 4.2)

Entschließung der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. April 1992 — gegen die Stimme Bayerns in Abwesenheit Sachsens — zur Neuregelung des Asylverfahrens (BT-Drucksache 12/2062)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält Änderungen des Gesetzentwurfs zur Neuregelung des Asylverfahrens für erforderlich, insbesondere der geplanten Regelungen

1. über die erkennungsdienstliche Behandlung von Asylbewerbern zur Sicherung der Identität (§ 16 Abs. 1) und
2. über die Nutzung der dabei gewonnenen erkennungsdienstlichen Unterlagen zur Strafverfolgung und zur Gefahrenabwehr (§ 16 Abs. 5).

zu 1.:

Nach dem geltenden Recht sind Lichtbilder und Fingerabdrücke bei Asylbewerbern nur dann zu fertigen, wenn deren Identität nicht eindeutig bekannt ist. Demgegenüber sieht der Gesetzentwurf zur Neuregelung des Asylverfahrens vor, daß von sämtlichen Asylbewerbern — bis auf wenige Ausnahmen — Lichtbilder und Fingerabdrücke zu fertigen sind. Dies ist mit dem Verfahrensgrundsatz der Verhältnismäßigkeit nicht vereinbar:

Der Staat hat selbstverständlich das Recht zu wissen, mit wem er es zu tun hat. Jeder — gleichgültig ob Deutscher oder Ausländer — muß sich deshalb durch Dokumente ausweisen können; nur wenn Zweifel an der Identität bestehen, kommen erkennungsdienstliche Maßnahmen in Betracht. Dieser Grundsatz unserer Rechtsordnung muß auch im Rahmen der Neuregelung des Asylverfahrens beachtet werden. Nur wenn feststeht, daß die Identität eines hohen Anteils der Asylbewerber — also nicht bloß einzelner oder bestimmter Gruppen — zweifelhaft ist, wäre eine erkennungsdienstliche Behandlung aller Asylbewerber gerechtfertigt. Gerade dies aber ist bisher nicht hinreichend belegt: In der amtlichen Begründung des Gesetzentwurfs ist allein davon die Rede, daß nach Feststellung niederländischer Behörden 20 % der Asylbewerber unter falschem Namen einen weiteren Asylantrag stellen. Aussagekräftige Angaben, in welchem Umfang in der Bundesrepublik Deutschland Asylbewerber unter Täuschung über ihre Identität gleich bei der ersten Antragstellung oder nach dessen Ablehnung erneut versuchen, Asyl zu erhalten, fehlen bislang.

Zu 2.:

Bei der zentralen Auswertung der Fingerabdrucke von Asylbewerbern durch das Bundeskriminalamt muß — ungeachtet dessen, ob das Bundeskriminalamt dabei in eigener Zuständigkeit oder für das Bundesamt für die Anerkennung ausländischer Flüchtlinge tätig wird — unbedingt folgendes sichergestellt sein:

- Fingerabdrücke von Asylbewerbern, die unter Beachtung des zu Nr. 1 Gesagten gefertigt wurden, dürfen nur gespeichert werden, soweit dies zur Sicherung der Identität unbedingt erforderlich ist. Dazu reicht die bisher vom Bundeskriminalamt angewandte Methode der sogenannten Kurzsatzverformelung der Fingerabdrücke aus. Gerade aber dabei soll es nicht bleiben: Mit der bevorstehenden Einführung von AFIS — einem neuen automatisierten Fingerabdruckverfahren — sollen künftig auch die Fingerabdrücke von Asylbewerbern, die allein zur Feststellung deren Identität gefertigt wurden, genauso erfaßt und ausgewertet werden wie die Fingerabdrucke mutmaßlicher oder tatsächlicher Straftäter. Asylbewerber würden damit von vorherein wie Straftäter behandelt. Eine solche Verfahrensweise wird dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot nicht gerecht. Zudem unterläuft sie die in § 16 Abs. 4 des Gesetzentwurfs vorgesehene Trennung der erkennungsdienstlichen Unterlagen von Asylbewerbern und Straftätern. Um die gebotene Differenzierung sicherzustellen, sollte — über das Trennungsgebot des § 16 Abs. 4 hinaus — die Verformelung auf den Abdruck eines Fingers des Asylbewerbers beschränkt werden, da dies zur eindeutigen Feststellung seiner Identität genügt.
- Die Datenschutzbeauftragten verkennen nicht, daß es unter Umständen im vorwiegenden Allgemeininteresse notwendig sein kann, im Rahmen asylrechtlicher Identitätsfeststellung gefertigte Fingerabdrücke für Zwecke der Strafverfolgung zu nutzen. Weil eine solche Verwendung einen neuen und zudem erheblichen Eingriff in das Grundrecht auf Datenschutz darstellt, darf sie nicht — wie es der Gesetzentwurf aber vorsieht — praktisch voraussetzungslos erfolgen. Notwendig ist vielmehr, die Voraussetzungen in einem abschließenden Straftatenkatalog aufzuführen; darin könnten auch die in der amtlichen Begründung des Gesetzentwurfs erwähnten Fälle des Sozialhilfebetrugs enthalten sein.
- Ein entsprechender Maßstab ist an die Regelung anzulegen, wann zur Identitätssicherung gefertigte Fingerabdrücke von Asylbewerbern zur polizeilichen Gefahrenabwehr genutzt werden dürfen. Eine solche Nutzung sollte nur zugelassen werden, soweit dies zur Abwehr einer gegenwärtigen erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist.

Anlage 6 (zu 1.8, 31.2)

Entschließung der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. April 1992 — gegen die Stimme Bayerns — zum Grundrecht auf Datenschutz

1. Seit dem Volkszählungsurteil des Bundesverfassungsgerichts im Jahre 1983 ist allgemein anerkannt, daß die Grundrechte auch die Befugnis des einzelnen umfassen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden. Die Datenschutzbeauftragten treten dafür ein, dieses Recht ausdrücklich im Grundgesetz zu verankern. Damit würde

   — für die Bürger deutlicher erkennbar, daß unsere Verfassung ihr Recht auf Datenschutz in gleicher Weise garantiert wie die traditionellen Grundrechte,

   — der wachsenden Bedeutung des Datenschutzes für das Funktionieren der freiheitlichen Demokratie Rechnung getragen und auf die negativen Erfahrungen der DDR-Geschichte reagiert,

   — der Grundrechtskatalog dem technologischen Wandel angepaßt und

   — die Konsequenz aus den positiven Erfahrungen gezogen, die in mehreren Ländern des Bundes und im Ausland mit ähnlichen Verfassungsbestimmungen gemacht wurden.

   Die Konferenz begrüßt deshalb die Vorstellungen, die in der Verfassungskommission des Bundesrates entwickelt worden sind.

   Die Datenschutzbeauftragten empfehlen der Gemeinsamen Verfassungskommission des Bundestages und Bundesrates im Zusammenhang mit Artikel 1 und Artikel 2 GG den nachfolgenden Text zur Beratung:

   „Jeder hat das Recht, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen. Dazu gehört das Recht auf Auskunft und Einsicht in amtliche Unterlagen. Dieses Recht darf nur durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden, soweit überwiegende Interessen der Allgemeinheit es erfordern."

2. Darüber hinaus empfiehlt die Konferenz, die unabhängige Datenschutzkontrolle, die für die Verwirklichung des Grundrechts auf Datenschutz im Alltag von entscheidender Bedeutung ist, in der Verfassung zu verankern.

3. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es zusätzlich für erforderlich, in die Verfassungsdiskussion folgende Punkte miteinzubeziehen, die sich aus der Entwicklung der Informationstechnik ergeben:

   — Stärkung der Grundrechte aus Artikel 10 und 13 im Hinblick auf neue Überwachungstechniken

   — Recht auf Zugang zu den Daten der Verwaltung (Aktenöffentlichkeit, Informationsfreiheit)

   — Instrumente zur Technikfolgenabschätzung.

Anlage 7 (zu 1.8, 21.11)

Entschließung der 44. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Datenschutz bei internen Telekommunikationsanlagen

Der zunehmende Einsatz von digitalen Telekommunikationsanlagen (TK-Anlagen) in Wirtschaft und Verwaltung birgt Datenschutzrisiken in sich, denen durch eine datenschutzfreundliche Ausgestaltung der Technik und durch geeignete bereichsspezifische Regelungen entgegengewirkt werden muß. Telefongespräche stehen — auch wenn sie von einem Dienstapparat aus geführt werden — unter dem Schutz des Grundgesetzes.

Dies hat das Bundesverfassungsgericht in seiner neueren Rechtsprechung hervorgehoben.

Der Schutz des Fernmeldegeheimnisses und des nicht-öffentlich gesprochenen Wortes ist gerade bei Arbeitnehmern bedeutsam, da diese sich in einem besonderen Abhängigkeitsverhältnis befinden; aber auch das informationelle Selbstbestimmungsrecht Dritter, die anrufen oder angerufen werden, muß gewahrt werden.

Entsprechende bundesrechtliche Regelungen für interne TK-Anlagen sind überfällig, da in diesen Anlagen — insbesondere wenn sie digital an das öffentliche ISDN angeschlossen sind — umfangreiche Sammlungen sensibler personenbezogener Daten entstehen können, die sich auch zur Verhaltens- und Leistungskontrolle eignen und zudem Hinweise auf das Kommunikationsverhalten aller Gesprächsteilnehmer geben. Die Regelungen sollten verbindliche Vorgaben für die technische Ausgestaltung von TK-Anlagen geben und den Umfang der zulässigen Datenverarbeitung festlegen:

- Es muß technisch möglich sein, daß Anrufer und Angerufene die Rufnummernanzeige fallweise abschalten können.
- Die automatische Speicherung der Rufnummern von externen Anrufern nach Beendigung des Telefongesprächs ist auszuschließen, soweit hierfür keine sachliche Notwendigkeit besteht.
- Die Weiterleitung eines Anrufs an einen anderen als den gewählten Anschluß sollte dem Anrufer so rechtzeitig signalisiert werden, daß dieser den Verbindungsaufbau abbrechen kann.
- Das Mithören und Mitsprechen weiterer Personen bei bestehenden Verbindungen sollte nur nach eindeutiger und rechtzeitiger Ankündigung möglich sein.
- Verbindungsdaten, einschließlich der angerufenen Telefonnummern, sollten nach Beendigung der Gespräche nur insoweit gespeichert werden, als dies für Abrechnungszwecke und zulässige Kontrollzwecke erforderlich ist. Die Nummern der Gesprächspartner von Arbeitnehmervertretungen, internen Beratungseinrichtungen und sonstigen auf Vertraulichkeit angewiesenen Stellen dürfen nicht registriert werden.
- Die TK-Anlagen müssen durch geeignete technische Maßnahmen gegen unberechtigte Veränderungen der Systemkonfiguration und unberechtigte Zugriffe auf Verbindungs- und Inhaltsdaten geschützt werden. Da TK-Anlagen geeignet sind, das Verhalten und die Leistung der Arbeitnehmer zu kontrollieren, und sie überdies häufig die Arbeitsplatzgestaltung beeinflussen, löst ihre Einführung in Betrieben und Behörden Mitbestimmungsrechte der Betriebsräte und überwiegend auch der Personalräte aus. Sie dürfen daher nur betrieben werden, wenn unter Beteiligung der Arbeitnehmervertretungen verbindlich festgelegt wurde, welche Leistungsmerkmale aktiviert und unter welchen Bedingungen sie genutzt werden, welche Daten gespeichert, wie und von wem sie ausgewertet werden. Die Nutzer der TK-Anlage sind über den Umfang der Datenverarbeitung umfassend zu unterrichten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, daß umgehend datenschutzrechtliche Regelungen für den Einsatz und die Nutzung von internen TK-Anlagen mit einer bereichsspezifischen Rechtsgrundlage für die Verarbeitung von Arbeitnehmerdaten geschaffen werden.

Anlage 8 (zu 1.8, 12.1)

Entschließung der 44. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Entwurf eines Gesetzes zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung — Gesundheits-Strukturgesetz 1993 (BR-Drucksache 560/92)

Die Bundesregierung will mit dem Gesundheits-Strukturgesetz dem Kostenanstieg in der gesetzlichen Krankenversicherung entgegenwirken. Dieses begrüßenswerte Ziel soll nach dem vorgelegten Gesetzentwurf u. a. auch durch eine verstärkte automatisierte Datenverarbeitung erreicht werden. Die damit verbundenen Eingriffe in die Persönlichkeitsrechte der Versicherten und in die sie schützende ärztliche Schweigepflicht müssen auf das unbedingt Notwendige beschränkt werden. Die Datenschutzkonferenz hält vor allem folgende Verbesserungen für notwendig:

- Der Gesetzentwurf sieht vor, daß die Krankenhäuser den Krankenkassen mehr Versichertendaten zur Verfügung stellen müssen als bisher. Es sollte deshalb eingehend geprüft werden, ob die Krankenkassen tatsächlich alle geforderten Angaben benötigen; die Aufgabenteilung zwischen Krankenkassen und Medizinischem Dienst muß aufrechterhalten bleiben.
- Für das Modellvorhaben zur Überprüfung des Krankenhausaufenthalts müssen die Erhebung, Verwendung und Löschung von Versichertendaten durch den Medizinischen Dienst präziser als bisher vorgesehen geregelt werden.
- Beim Einzug der Vergütung der Krankenhausärzte für Wahlleistungen durch Krankenhäuser sollte die Einschaltung privater Abrechnungsstellen ohne Einwilligung der Patienten nicht zugelassen werden, da dabei Abrechnungsdaten an Dritte offenbart werden. Die Daten sind gegen unbefugte Offenbarung und Beschlagnahme rechtlich besser geschützt, wenn sie — auch zur Abrechnung — im Krankenhaus verbleiben. Die Krankenhäuser sind zudem in der Lage, die Vergütung einzuziehen.
- Für die neu vorgesehenen Patienten-Erhebungsbogen zur Ermittlung des Bedarfs an Pflegepersonal im Krankenhaus sollte eine strikte Zweckbindung sowie eine frühestmögliche Löschungs- oder Anonymisierungspflicht festgelegt werden. Eine Überlassung der Patienten-Erhebungsbogen in der im Gesetzentwurf vorgesehenen Fassung an die Krankenkassen ist abzulehnen.

Anlage 9 (zu 1.8, 12.4)

Entschließung der 44. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zur Krankenversichertenkarten als Chipkarte

Die Konferenz der Datenschutzbeauftragten stellt fest, daß wegen der wachsenden Automatisierung bei allen Institutionen des Gesundheitswesens und der Erweiterung des Anteils maschinenlesbarer Datenträger eine Speicherung auf einer Chip-Karte als elektronische Krankenversicherungskarte auf die gesetzlich festgelegten Grunddaten beschränkt bleiben muß und nicht auf Gesundheitsdaten ausgedehnt werden darf. Eine technische Sicherung dieser Beschränkung ist zu gewährleisten.

Anlage 10 (zu 1.8, 5.1.3)

Entschließung der 44. Konferenz der Datenschutzbeauftragen des Bundes und der Länder vom 1./2. Oktober 1992 — gegen die Stimme Bayerns — zum „Lauschangriff"

Die Datenschutzbeauftragten des Bundes und der Länder erklären:

Nachdem erst vor kurzem mit dem Gesetz zur Bekämpfung der organisierten Kriminalität die Befugnisse der Strafverfolgungsbehörden erheblich erweitert worden sind und obwohl über den Erfolg dieser Maßnahmen noch keine Erfahrungen gesammelt werden konnten, wird gegenwärtig parteiübergreifend vielfach die Forderung erhoben, der Polizei in bestimmten Fällen das heimliche Abhören und Herstellen von Bild- und Tonaufzeichnungen in und aus Wohnungen (sog. „Lauschangriff") zu ermöglichen.

1. Das Grundgesetz gewährt jedem einen unantastbaren Bereich privater Lebensgestaltung, der der Einwirkung der öffentlichen Gewalt entzogen ist. Dem einzelnen muß um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein „Innenraum" verbleiben, in dem er „sich selbst besitzt" und „in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt" (BVerfGE 27,1 ff.). Jedem muß ein privates Refugium, ein persönlicher Bereich bleiben, der obrigkeitlicher Ausforschung — insbesondere heimlicher — entzogen ist. Dies gilt gegenüber Maßnahmen der Strafverfolgung vor allem deshalb, weil davon auch unverdächtige oder unschuldige Bürger betroffen sind. Auch strafprozessuale Maßnahmen dürfen nicht den Wesensgehalt eines Grundrechts, insbesondere nicht das Menschenbild des Grundgesetzes verletzen.
2. Die Datenschutzbeauftragten nehmen die Gefahren, die das organisierte Verbrechen für die Opfer und auch für die Demokratie und den Rechtsstaat heraufbeschwört, sehr ernst. Sie sind allerdings der Meinung, daß eine angemessene Abwägung zwischen der Verfolgung der organisierten Kriminalität und dem Schutz der Persönlichkeitsrechte der Bürger geboten und möglich ist und es eine Wahrheitserforschung um jeden Preis auch künftig im Strafprozeßrecht nicht geben darf. Daraus folgt, daß der Lauschangriff auf Privatwohnungen für Zwecke der Strafverfolgung auch in Zukunft nicht erlaubt werden darf.
3. Eine andere Frage ist, ob und unter welchen Voraussetzungen der Gesetzgeber für Räume, die allgemein zugänglich sind oder beruflichen oder geschäftlichen Tätigkeiten dienen (z. B. Hinterzimmer von Gaststätten, Spielcasinos, Saunaclubs, Bordelle), einen Lauschangriff zulassen kann. Hierfür sind Mindestvoraussetzungen ein eng begrenzter abschließender Straftatenkatalog, die Verwendung der gewonnenen Erkenntnisse ausschließlich zur Verfolgung dieser Straftaten, ein strikter Richtervorbehalt sowie die Wahrung besonderer Amts- und Berufsgeheimnisse.

Anlage 11 (zu 1.8, 19.2)

Entschließung der 45. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. Februar zur Richtlinie des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt (30/313/EWG)

Im Interesse eines wirksamen Umweltschutzes hat der Ministerrat der Europäischen Gemeinschaft die Umweltinformationsrichtlinie erlassen, die jedem Bürger ein Recht auf Zugang zu den bei Behörden vorhandenen Informationen über die Umwelt gewährt. Da es nicht gelungen ist, die Richtlinie innerhalb der vorgegebenen Frist bis Ende 1992 in deutsches Recht umzusetzen, herrscht gegenwärtig Rechtsunsicherheit bei Bürgern und Behörden über den Zugang zu Umweltinformationen.

Die Konferenz der Datenschutzbeauftragten sieht in der Gewährung eines freien Zugangs zu Umweltinformationen einen wesentlichen Beitrag zu größerer Transparenz des Verwaltungshandelns. Informationsfreiheit und Datenschutz bilden dabei keinen unlösbaren Gegensatz. Die Konferenz hält es für geboten, die Arbeit am Entwurf des Umweltinformationsgesetzes (UIG) zügig zum Abschluß zu bringen. Sie begrüßt entsprechende Initiativen auf Landesebene.

In den Gesetzen sind folgende datenschutzrechtliche Grundsätze zu berücksichtigen:

Soweit Umweltinformationen auf Personen beziehbar sind, ist das Grundrecht auf informationelle Selbstbestimmung zu beachten. Deshalb sind Informationen grundsätzlich in anonymisierter oder aggregierter Form zu geben. Wenn damit das Informationsinteresse nicht erfüllt werden kann, sind Eingriffe in das Persönlichkeitsrecht nur unter klaren gesetzlichen Voraussetzungen zulässig, welche die Rechte, insbesondere die Verfahrensrechte, der Betroffenen wahren.

Anlage 12 (zu 21.5)

Merkblatt der DBP Telekom: Hinweise zum Datenschutz für unsere Telefonkunden

1. Um Ihre vielfältigen Dienste und Dienstleistungen kundenbezogen und sachgemäß anbieten und erbringen zu können, ist die Deutsche Bundespost, wie viele andere Unternehmen auch, darauf angewiesen, Daten ihrer Kunden und der übrigen am Fernmeldeverkehr Beteiligten erheben, verarbeiten und nutzen zu dürfen. Regelungen hierzu enthält die TELEKOM-Datenschutzverordnung (Verordnung über den Datenschutz bei Dienstleistungen der Deutschen Bundespost Telekom — TDSV, BGBl. I, Nr. 19 vom 29. Juni 1991, S. 1390 ff.), deren Text Sie bei ihrem Fernmeldeamt oder jedem Telekomladen einsehen können.

2. *Bestandsdaten*

   In dem durch diese Verordnung vorgegebenen Rahmen erhebt, verarbeitet und nutzt die Deutsche Bundespost Telekom personenbezogene Daten ihrer Kunden, die für die Begründung und Änderung der Kundenverträge erforderlich sind (Bestandsdaten). Dazu gehören z. B. Name, Anschrift und Geburtsdatum. Das Geburtsdatum wird zur sicheren Unterscheidung namensgleicher oder -ähnlicher Kunden benötigt und für keine anderen Zwecke genutzt, insbesondere nicht an Dritte weitergegeben. Die Bestandsdaten werden in der Regel mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres gelöscht.

3. *Eintragung ins Telefonbuch*

   Die Deutsche Bundespost Telekom und die Deutsche Postreklame GmbH sind berechtigt, den unter Beteiligung ihrer Kunden festgelegten Eintrag in allen für Dienste der Telekom herausgegebenen Kundenverzeichnissen und in der Fernsprechauskunft zu verwenden. Außerdem darf die Deutsche Bundespost Telekom die Telefonbuch-Einträge ihrer Kunden an Dritte weitergeben, die ebenfalls Telefonbücher verlegen oder eine Auskunft über Telefonbuchdaten betreiben möchten. Kundenverzeichnisse sind zur Zeit das amtliche Telefonbuch, das Örtliche Telefonbuch, das Elektronische Telefonbuch, die CD-ROM und für geschäftlich genutzte Telefonanschlüsse die „Gelben Seiten". Bei der CD-ROM handelt es sich um ein mittels Computer lesbares elektronisches Telefonverzeichnis. Zum Nutzen aller Kunden sollten die Verzeichnisse so vollständig wie möglich sein. Dabei werden grundsätzlich Name, Vorname, ggf. Beruf, Anschrift und Rufnummer kostenfrei veröffentlicht. Die Kunden können aber jederzeit gegenüber ihrem Fernmeldeamt den Umfang der Eintragung beschränken oder der Veröffentlichung ganz widersprechen; dann unterbleibt insoweit die Veröffentlichung in allen Kundenverzeichnissen und in der Fernsprechauskunft, sowie die Weitergabe der Daten an Dritte, die Telefonbücher verlegen oder eine Auskunft betreiben.

4. *Verbindungsdaten*

   Bei Anrufen, die von Anschlüssen des dienstintegrierenden digitalen Netzes (ISDN) und des Mobilfunks (Funktelefonanschluß usw.) aus geführt werden, werden Verbindungsdaten wie die Rufnummern des anrufenden und des angerufenen Anschlusses, die in Anspruch genommene Dienstleistung, Beginn und Ende der Verbindung und bei Anschlüssen des Mobilfunks die Standortkennung erhoben und verarbeitet. Bei der Verwendung von Kundenkarten (z. B. Telefonieren in der Telefonzelle mit der „Telekarte") wird darüber hinaus die Kartennummer gespeichert. Keinesfalls aber werden die Nachrichteninhalte (z. B. Telefongespräche oder übermittelte Texte) gespeichert. Die Kunden der Telekom können wählen, ob die Verbindungsdaten nach Absendung der Fernmelderechnung

   — vollständig gelöscht oder

   — unter Verkürzung der Zielrufnummer um die letzten drei Ziffern weiterhin gespeichert werden sollen.

   Wir machen darauf aufmerksam, daß die Telekom von der Pflicht zur Vorlage der Verbindungsdaten zum Beweis der Richtigkeit der Rechnung befreit ist, wenn sie diese auf Wunsch der Kunden gelöscht hat.

   Sobald die Telekom ihren Kunden eine detaillierte Rechnung anbieten kann, die für jede gewählte Verbindung den Zeitpunkt, die Dauer und vollständige Zielrufnummer ausweist, und der Kunde diesen Einzelverbindungsnachweis wünscht, bleiben die Verbindungsdaten noch 80 Tage nach Absendung der Fernmelderechnung vollständig gespeichert. Danach werden auch sie — wie die verkürzten Verbindungsdaten — gelöscht.

   Über das Angebot des Einzelverbindungsnachweises werden wir Sie rechtzeitig unterrichten.

   Nur ausnahmsweise können Daten auch über einen längeren Zeitraum verarbeitet oder genutzt werden, so z. B. im Fall der Störungsbeseitigung oder des strafbaren Mißbrauchs von Fernmeldeanlagen (§ 7 TDSV).

5. *Entgeltdaten*

   Die Deutsche Bundespost Telekom erhebt und verarbeitet die zur ordnungsgemäßen Ermittlung und Abrechnung der Entgelte und zum Nachweis der Richtigkeit derselben erforderlichen Daten (Entgeltdaten). Dies sind — neben einem Teil der Verbindungsdaten — u. a. Tarifeinheiten und Zahlungsweisen.

6. *Beratung, Werbung und Marktforschung durch die Telekom*

   Die Deutsche Bundespost Telekom nutzt die Bestandsdaten ihrer Kunden zu Beratungs-, Werbungs- und Marktforschungszwecken, soweit es um die von ihr selbst angebotenen Produkte und Dienstleistungen geht. Die Kunden können dieser Nutzung — sofern nicht bereits mit dem Telefondienstauftrag geschehen — jederzeit durch eine Erklärung gegenüber dem Fernmeldeamt widersprechen. Der Widerspruch kann auch im Telekomladen abgegeben werden.

7. *Werbliche Nutzung der veröffentlichten Daten durch Dritte*

   Die in den Kundenverzeichnissen oder anderen öffentlichen Unterlagen eingetragenen Daten können nach den Vorschriften des Bundesdatenschutzgesetzes von jedermann für Werbezwecke genutzt werden. Wenn die Kunden der Telekom nicht möchten, daß ihre veröffentlichten Daten für werbliche Zwecke genutzt werden, können sie gegenüber einzelnen Firmen der werblichen Nutzung dieser Daten widersprechen.

   Die Kunden der Telekom können sich auch auf die beim Deutschen Direktmarketing-Verband geführte „Robinsonliste" setzen lassen, die von allen dem Verband angeschlossenen Werbeunternehmen respektiert wird.

   Die Adresse lautet:

   DDV-Robinsonliste, W-7257 Ditzingen
   Postfach 7257, Telefon: (07156) 951010.

Anlage 13 (zu 30.2)

Empfehlungen zur Paßwortgestaltung und zum Sicherheitsmanagement *)

I. Paßwortregeln

Grundsatz:

„Für den Benutzer leicht zu merken, für einen Fremden schwer zu erraten."

1. *Nirgends notieren! Niemandem mitteilen!*
2. *Nur dem Benutzer bekannt.*
3. Mindestlänge: 6 Stellen.
4. Vor- und Familiennamen nie allein verwenden, sondern:
5. Stets alphanumerisch gestalten (Buchstaben und Zahlen/Zeichen).
6. Keine Trivialpaßwörter (z. B. 4711, 12345 oder andere nebeneinanderliegende Tasten, gast usw.) verwenden; möglichst vom System automatisch abweisen lassen.
7. In angemessenen Zeitabständen (möglichst automatisch gesteuert) ändern; nicht zu oft!
8. Automatisch verhindern, daß (aus Bequemlichkeit) als neues wieder das alte Paßwort gewählt wird.
9. Für besonders wichtige Funktionen/sensible Daten: Zusatzpaßwort („4-Augen-Prinzip"). Oder: Zwei Personen kennen je das *halbe* Paßwort.
10. Paßwort des Systemverwalters — *nur* ihm bekannt — für Vertretungsfall versiegelt aufbewahren.

II. Sicherheitsmanagement

1. Jede Person erhält eine eigene Benutzerkennung („User"). Benutzerkennungen werden grundsätzlich nur für Bedienstete der Stelle eingerichtet; für Fremde (Wartung usw.) nur zur kontrollierten Inanspruchnahme.
2. Benutzerkennungen werden nur für den Zeitraum eingerichtet, in dem sie tatsächlich benötigt werden.
3. Die Datei der Paßwörter und Benutzerkennungen ist besonders zu schützen, i. d. R. durch kryptographische Verschlüsselung.
4. Automatische Begrenzung der Anzahl der Anmeldungs-Fehlversuche (maximal drei, danach: Sperrung der Benutzerkennung).
5. Protokollierung der Fehlversuche und Information des Systemverwalters und/oder Benutzers.
6. Anzeige der letzten korrekten Anmeldung zur Kontrolle durch den Berechtigten (Tag, Uhrzeit, Terminal usw.).
7. Zeitliche Begrenzung der Zugangsberechtigung, z. B. auf die Bürozeit.
8. Verhindern, daß Anmeldung mit Funktionstaste möglich („auto-log-in").
9. Automatisches Sperren oder Abmelden des Terminals/APC nach längerer Nichtbenutzung, z. B. nach 5 Minuten.
10. Bei Verbindung des Systems mit dem öffentlichen Wählnetz: Zusätzliche Sicherungsmaßnahmen (Rückrufautomatik usw.).

---

*) Mit Schreiben VI — 170/1 vom 11. Dezember 1991 an oberste Bundesbehörden

Anlage 14 (zu 30.4)

Hinweise zu Protokolldateien*)

1. Erforderlichkeit, Zweckbindung

Eine Erzeugung von Protokolldateien ist nur zulässig, wenn sie auch *erforder*lich sind, d. h. tatsächlich genutzt werden. Werden sie ausschließlich zu Zwekken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes der ADV-Anlage gespeichert, dürfen sie *nur* für diese Zwecke verwendet werden (§ 14 Abs. 4 BDSG).

2. Dateiverzeichnis, Registermeldung

Protokolldateien der genannten Art sind in das Verzeichnis der Dateien gem. § 18 Abs. 2 BDSG aufzunehmen. Wenn sie länger als drei Monate vorgehalten werden, müssen sie darüber hinaus dem Bundesbeauftragten für den Datenschutz zum Register gem. § 26 Abs. 5 BDSG gemeldet werden. Dateien gem. § 14 Abs. 4 BDSG brauchen nicht gemeldet zu werden.

3. Mitbestimmung

Im allgemeinen ist davon auszugehen, daß die Protokolldateien zur Verhaltens- und Leistungskontrolle geeignet sind. Es erscheint daher unerläßlich, den Personalrat oder Betriebsrat auf die Protokolldatei(en) hinzuweisen, damit dieser gegebenenfalls von seinen Mitbestimmungsrechten Gebrauch machen kann.

Die zulässigen Auswertungen der Protokolldateien sowie die Art ihrer Nutzung sollten unter Beteiligung des internen Datenschutzbeauftragten und des Personalrates oder Betriebsrates festgelegt werden. Tatsächliche Auswertungen zu Zwecken der Datenschutzkontrolle oder der Kontrolle der IT-Sicherheit sollten durch den Datenschutzbeauftragten bzw. IT-Sicherheitsbeauftragten unter Beteiligung des Personalrates erfolgen.

4. Vermeidung einer „Totalregistrierung"

Eine wahllose Registrierung *aller* Aktivitäten des Benutzers ist aus Sicht des Datenschutzes bedenklich. Zwar erfordert § 9 BDSG (Anl., Nr. 7 u. a.) Maßnahmen, damit nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zur welcher Zeit von wem in das System eingegeben wurden. Der Angemessenheitsgrundsatz des § 9 gestattet es jedoch, dahingehende Registrierungen in Protokolldateien auf *sensiblere* Aktivitäten (Benutzung bestimmter Programme, Dateien, Datenfelder) zu begrenzen. Es sollten daher alle systemseitig vorhandenen Möglichkeiten — durch Einstellen von Parametern oder Setzen von „Schaltern" — genutzt werden, damit wirklich nur Aktivitäten mit erhöhtem Schutzbedarf registriert werden. So reicht es aus, wenn nicht *jeder* Zugriff z. B. auf eine Personaldatei registriert wird, sondern nur diejenigen, die besonders sensible Datenfelder oder Programme betreffen. Auch eine solche Protokolldatei darf nicht zur Verhaltens- und Leistungskontrolle genutzt werden.

5. Löschung

Protokolldateien müssen nach angemessener Zeit (automatisch) gelöscht werden; eine Speicherdauer von maximal einem Jahr ist im allgemeinen als ausreichend anzusehen (siehe auch o. Nr. 2).

---

*) Mit Schreiben VI — 170/1 vom 11. Dezember 1991 an oberste Bundesbehörden

Anlage 15 (zu 30.8)

Hinweise zu automatisierten Abrufverfahren i. S. § 10 BDSG*)

1. Ein *automatisiertes Abrufverfahren* (§ 10 BDSG) ist ein Datenverarbeitungsverfahren, in dem Einzeldaten oder ganze Datenbestände durch Abruf an einen Dritten (§ 3 Abs. 9) übermittelt (§ 3 Abs. 5 Nr. 3) werden.

   Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt die abrufende Stelle.

   Von mehreren Stellen gemeinsam betriebene Dateien mit wechselseitiger Schreibbefugnis fallen nicht unter § 10.

2. Wesentlich für den *Abruf* ist das Moment der „Selbstbedienung". Werden Art und Umfang der zu übermittelnden Daten allein von der übermittelnden Stelle bestimmt und kann der Empfänger nur den Zeitpunkt festlegen, liegt daher kein Abruf im Sinne des § 10 vor, so etwa bei der regelmäßigen Übermittlung der Kfz-Zulassungsdaten von den Gemeinden an das Kraftfahrtbundesamt im automatisierten Verfahren.

   Ein Abruf kann der Abruf eines Datensatzes, des Teils eines Datensatzes oder mehrerer Datensätze (eines Datenbestandes) sein. Gegenstand eines Abrufs kann auch das Ergebnis einer Datenverarbeitung sein, z. B. des Vergleichs oder Abgleichs zweier Datenbestände.

3. Die speichernde Stelle und die abrufende(n) Stelle(n) legen die Einzelheiten des vereinbarten Verfahrens gemäß § 10 Abs. 2 S. 2 fest:

   — Anlaß und Zweck des Verfahrens,

   — abrufberechtigte Stellen („Datenempfänger"),

   — zum Abruf vorgesehene Daten,

   — getroffene Sicherungsmaßnahmen i. S. § 9 BDSG.

4. Das Abrufverfahren ist schriftlich zu *dokumentieren*. Die in § 10 Abs. 2 genannten Informationen sind in geeigneter Weise übersichtlich in einer eigenen Dokumentation zusammenzustellen. Dazu reicht die technische Entwicklungsdokumentation (Programmdokumentation) allein in der Regel nicht aus. Sie kann der Dokumentation jedoch ergänzend als Anlage beigefügt werden.

5. Ist an dem Verfahren — als speichernde oder abrufende Stelle — eine öffentliche Stelle des Bundes beteiligt, ist der *Bundesbeauftragte für den Datenschutz* über das Abrufverfahren zu unterrichten. Dabei sind ihm die gem. § 10 Abs. 2 S. 2 festgelegten oder festzulegenden Einzelheiten des Verfahrens (s. o. Nr. 3) mitzuteilen.

6. Die speichernde Stelle hat zu gewährleisten, daß die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann (§ 10 Abs. 4 S. 3). Dazu ist eine *Protokollierung* der Abrufe erforderlich, deren Umfang für das einzelne Abrufverfahren festzulegen ist. Zumindest für einen Teil der Abrufe werden Zeitpunkt und Inhalt (Anfragetext und Antworttext) sowie abrufende Stelle und abrufender Benutzer dokumentiert.

   Eine *Vollprotokollierung*, d. h. eine lückenlose Protokollierung aller Abrufe mit allen genannten Details, ist vom Gesetz nicht gefordert. Gleichwohl kann sie unter Umständen geboten sein. Solche Umstände können sich aus der Sensibilität der gespeicherten Daten, der Art des Übertragungsweges, aus dem Benutzerkreis oder aus allen drei Kriterien ergeben. Selbst wenn alle Anforderungen des § 9 nebst Anlage erfüllt sind, ist ein Eindringen über die on-line-Verbindung in den Datenbestand durch Hacker nicht auszuschließen. Zwar dient die Einrichtung geeigneter Stichprobenverfahren der Gewährleistung der Kontrolle (durch den Bundesbeauftragten oder die Aufsichtsbehörden), es ist aber vor allem Sache der speichernden Stelle zu überprüfen, ob unbefugt auf ihre gespeicherten Daten zugegriffen wird.

   Liegen keine besonderen Umstände vor, so erfolgt die *Protokollierung in Form einer Auswahl* (z. B. jeder dritte Abruf) oder ausschnittsweise, wobei sich die Ausschnitte auf Zeiträume, Benutzer oder Benutzergruppen, Datenarten oder Dateninhalte beziehen oder an definierte Ereignisse (z. B. Abrufhäufigkeit) anknüpfen können. Die Auswahl sollte flexibel und situationsangemessen sein. Eine statistisch gleichmäßige (repräsentative) Berücksichtigung des Gesamtaufkommens der Abrufe ist nicht geboten. Eine gezielte Auswahl nach bestimmten Kriterien, zu denen auch Zufallskriterien gehören können, wird meist wirkungsvoller sein. Von entscheidender Bedeutung für die Mißbrauchsprävention ist, daß die Art und Weise der Protokollierung für die Benutzer nicht vorhersehbar ist; für sie muß immer das Risiko einer Protokollierung und Nachprüfung bestehen.

   Die Protokolldaten müssen nicht in Papierform vorliegen; es reicht aus, wenn sie maschinenlesbar verfügbar sind.

   Eine allgemeine Aussage, wie lange die Protokolle aufzubewahren sind, ist nicht möglich. Im allgemeinen wird eine Aufbewahrungsdauer von einem Jahr angemessen sein.

   Für alle Protokolldateien gilt die besondere Zweckbindung des § 14 Abs. 4 BDSG.

7. Bei der *Auswertung der Protokolldaten* steht das Ziel im Vordergrund, unzulässige und „problematische" Abrufe zu erkennen, um geeignete Korrekturmaßnahmen einleiten zu können. Ebenso ist es Ziel der Auswertung, eine möglichst hohe Gewißheit zu erreichen, daß unzulässige Abrufe nicht stattfinden. Hierzu ist es notwendig, einzelne protokollierte Abrufe auf ihre Rechtmäßigkeit zu überprüfen, insbesondere an Hand der Unterlagen der abrufenden Stelle. Welche Fälle in die konkrete Überprüfung einbezogen werden, richtet sich nach dem Kontrollzweck. Eine für den gesamten protokollierten Bestand repräsentative Auswahl ist nicht geboten und für sich allein nicht der optimale Ansatz. Vielmehr ist es zweckmäßig, durch Auswertung des Protokollbestandes diejenigen Teilmengen einzukreisen, bei denen eine erhöhte Wahrscheinlichkeit kritischer Abrufsfälle besteht. Hierzu können Auswertungen nach Tageszeiten, nach abrufberechtigten Personen oder Stellen, nach regionalen Gesichtspunkten, nach Nutzungsfrequenz, nach verwendeten Abrufarten oder nach abgerufenen Datenarten in Betracht kommen. Erweisen sich bestimmte Teilmengen von Abrufen als besonders fehlerträchtig, ist es angezeigt, für diese eine intensivere Protokollierung und Auswertung vorzunehmen. Umgekehrt kann die Kontrolldichte für Bereiche zurückgenommen werden, für die sich erwiesen hat, daß keine Fehler (mehr) auftreten.

   Die Zwischen- und Endergebnisse der Auswertung unterliegen ebenso wie der Inhalt der Protokolldateien der besonderen Zweckbestimmung des § 14 Abs. 4.8. Es ist Aufgabe der speichernden Stelle, den einzelnen *Benutzer* (jede einzelne Person) der abrufenden Stelle zu identifizieren und zu authentisieren (Anl. zu § 9). Einzelheiten dieser und aller weiteren Maßnahmen zur Sicherheit des Verfahrens sind bei der Vereinbarung des Abrufverfahrens von der speichernden Stelle und der abrufenden Stelle festzulegen. Erforderlich sind solche Maßnahmen, die in angemessenem Verhältnis zu dem angestrebten Schutzzweck stehen (§ 9 Satz 2).

   Paßwörter sind in Abrufsystemen mit den üblichen Verfahrensweisen, etwa Kryptierung, zu schützen.

   Näheres zur Identifikation und Authentisierung enthält mein Rundschreiben an die obersten Bundesbehörden vom 11. Dezember 1991 — VI — 170/1 —, wiedergegeben im 14. Tätigkeitsbericht (Anl. 13).

9. Wegen der prinzipiellen Angreifbarkeit des *öffentlichen Wählnetzes*, insbesondere des Telefonnetzes, können bei besonders sensiblen Daten anstelle von Wählanschlüssen auch festgeschaltete Leitungen erforderlich sein.

10. Die Anforderungen des § 9 BDSG mit Anlage werden durch § 10 nicht eingeschränkt.

*) Mit Schreiben VI — 170/37 vom 23. Februar 1993 an oberste Bundesbehörden

Anlage 16 (zu 32.3)

Schweigepflichtentbindungsklauseln in Versicherungsverträgen

Berufsunfähigkeitsversicherung

Ich ermächtige den Versicherer, zur Nachprüfung und Verwertung der von mir über meine Gesundheitsverhältnisse gemachten Angaben alle Ärzte, Krankenhäuser und sonstigen Krankenanstalten, bei denen ich in Behandlung war oder sein werde sowie andere Personenversicherer über meine Gesundheitsverhältnisse bei Vertragsabschluß zu befragen; dies gilt für die Zeit vor der Antragsannahme und die nächsten zehn Jahre nach der Antragsannahme. Werden Leistungen wegen Berufsunfähigkeit beansprucht, darf der Versicherer die in Satz 1 genannten Personen und Einrichtungen, die Ärzte, die mich untersucht haben, sowie Behörden — mit Ausnahme von Sozialversicherungsträgern — auch über Ursache, Beginn, Art, Verlauf, Grad und voraussichtliche Dauer der Berufsunfähigkeit sowie über diejenigen Krankheiten, die zur Berufsunfähigkeit geführt haben, befragen.

Insoweit entbinde ich alle, die hiernach gefragt werden, von der Schweigepflicht auch über meinen Tod hinaus.

Pflegerentenversicherung

Ich ermächtige den Versicherer, zur Nachprüfung und Verwertung der von mir über meine Gesundheitsverhältnisse gemachten Angaben alle Ärzte, Krankenhäuser, sonstige Krankenanstalten sowie Alten- und Pflegeheime, bei denen ich in Behandlung war oder sein werde, andere Personenversicherer sowie alle Personen, die mit der Pflege betraut waren, über meine Gesundheitsverhältnisse zu befragen; dies gilt für die Zeit vor der Antragsannahme und die nächsten 10 Jahre nach der Antragsannahme. Werden Leistungen beansprucht, darf der Versicherer die in Satz 1 genannten Personen und Einrichtungen, die Ärzte, die mich untersucht haben, sowie Behörden — mit Ausnahme von Sozialversicherungsträgern — auch über Ursache, Beginn, Art, Verlauf, Pflegestufe und voraussichtliche Dauer des Pflegefalls sowie über diejenigen Krankenheiten, die zur Pflegebedürftigkeit oder zum Tode geführt haben, befragen.

Insoweit entbinde ich alle, die hiernach befragt werden, von der Schweigepflicht auch über meinen Tod hinaus.

Anlage 17 (zu 33.2)

Probleme des Fernmeldegeheimnisses und der Satellitenkommunikation

Bericht der Arbeitsgruppe Telekommunikation und Medien der Internationalen Datenschutzkonferenz

und

Gemeinsame Erklärung der 14. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 29. Oktober 1992

Bericht

Fernmeldegeheimnis

1. Jeder Bürger, der ein Telefon benutzt, hat grundsätzlich die legitime Erwartung, daß sein Telefongespräch von niemandem, insbesondere von keiner staatlichen Stelle, abgehört wird.

   Der Grundsatz der Vertraulichkeit von Telefongesprächen ist deshalb in den Verfassungen verschiedener Länder wie z. B. Österreichs, Deutschlands, Griechenlands, der Niederlande, Portugals und Spaniens verankert. Darüber hinaus garantiert die Europäische Menschenrechtskonvention das Recht jedes Einzelnen auf Achtung seiner Privatsphäre, seines Familienlebens, seiner Wohnung und seiner Korrespondenz. Dieser Artikel der Europäischen Menschenrechtskonvention ist vom Europäischen Menschenrechtsgerichtshof so ausgelegt worden, daß er auch das Fernmeldegeheimnis umfaßt.

   In vielen Ländern ist das Abhören von Telefongesprächen sogar ein Straftatbestand. Die bloße Behauptung, daß Telefone illegal abgehört worden seien, kann auch weitreichende politische Konsequenzen haben. So mußte kürzlich ein Minister der Republik Irland aufgrund derartiger Vorwürfe zurücktreten, um nur ein Beispiel zu geben.

2. Andererseits ist in den meisten Ländern anerkannt, daß es unter besonderen Voraussetzungen Ausnahmen vom Fernmeldegeheimnis geben muß. In Belgien, dem einzigen Land, in dem es bisher ein absolutes Verbot des Abhörens von Telefongesprächen gibt, bereitet die Regierung einen Gesetzentwurf für entsprechende Ausnahmen vor.

   Die Statistik zeigt, daß Telefongespräche für Zwecke der Strafverfolgung im Jahre 1990 in 2 449 Fällen in Deutschland und in 2 031 Fällen in den Niederlanden abgehört wurden (Quelle: Bundesministerium für Post und Telekommunikation; Niederländisches Justizministerium).

   Nach Artikel 8 Abs. 2 der Europäischen Menschenrechtskonvention ist der „Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts" (auf Achtung des Post- und Fernmeldegeheimnisses) „nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist". Dieser Katalog von Ausnahmen, die der nationale Gesetzgeber vorsehen kann, ist sehr weitreichend, und einige europäische Länder haben restriktive Vorschriften erlassen, die das Abhören von Telefongesprächen erlauben (vgl. auch Ziffer 2.4 des Entwurfs einer Empfehlung für den Schutz von personenbezogenen Daten im Bereich der Telekommunikationsdienste, mit besonderem Bezug zu Telefondiensten, angenommen vom Ausschuß für rechtliche Zusammenarbeit des Europarats, Juni 1992).

   Die Arbeitsgruppe hat die neueren Entwicklungen der Gesetzgebung in den einzelnen Ländern untersucht und dabei festgestellt, daß trotz einiger Zweifel hinsichtlich der Effektivität des Telefonabhörens als Mittel im Kampf gegen die „organisierte Kriminalität" dennoch eine wachsende Tendenz zu beobachten ist, die Unverletzlichkeit des Fernmeldegeheimnisses mit zusätzlichen Ausnahmen zu versehen. In Deutschland trat in diesem Jahr ein neues Gesetz in Kraft, das eine Verwaltungsbehörde ermächtigt, Telefongespräche abzuhören, um illegale Waffenexporte zu verhindern (sogar bevor Straftaten begangen werden). In vielen Ländern kann das Telefonabhören in Strafverfahren angeordnet werden, die spezielle schwere Straftaten wie Drogenhandel, Mord und terroristische Verbrechen betreffen.

   Allerdings wird das Abhören von Telefongesprächen neuerdings von Politikern auch als effektive Waffe im Kampf gegen Korruption und organisierte Kriminalität angesehen (Australien, Deutschland). Es ist bisher nicht gelungen, diese Kategorien von Straftatbeständen präzise zu beschreiben. Deshalb birgt jede Gesetzgebung, die mit derart ungenauen Tatbeständen arbeitet, die Gefahr, daß die Telefongespräche unverdächtiger Personen abgehört werden.

   In Österreich wird andererseits über einen Gesetzentwurf diskutiert, der sogar den Geheimdienst verpflichtet, eine richterliche Anordnung zu beantragen, bevor Telefongespräche rechtmäßig abgehört werden dürfen.

Die Notwendigkeit einer Rechtsgrundlage für jeden staatlichen Eingriff in das Fernmeldegeheimnis hat der Europäische Menschenrechtsgerichtshof sehr strikt ausgelegt. In seiner neueren Rechtsprechung betont der Gerichtshof, daß Abhören und andere Formen der Registrierung von Telefongesprächen einen schwerwiegenden Eingriff in das Privatleben und die Kommunikation darstellen und deshalb auf einer Rechtsvorschrift beruhen müssen, die besonders präzise formuliert ist. Der Gerichtshof hebt hervor, daß es entscheidend ist, klare, detaillierte Vorschriften in diesem Bereich zu haben, insbesondere weil die verfügbare Technologie sich ständig weiterentwickelt (Fall Kruslin, 7/1989/167/223, Ziffer 33). Aus diesem Grund (Mangel an Präzision) wurde festgestellt, daß die Vorschriften des französischen Rechts über das Abhören von Telefongesprächen, gegen die Europäische Menschenrechtskonvention verstießen. Zwischenzeitlich ist Frankreich dem Beispiel des Vereinigten Königreichs gefolgt und hat ein neues Abhörgesetz verabschiedet, um den Anforderungen des Europäischen Menschenrechtsgerichtshofs zu entsprechen.

Das deutsche Bundesverfassungsgericht hat vor kurzem entschieden, daß eine präzise Rechtsgrundlage notwendig ist, um Fangschaltungen vorzunehmen, auch wenn der Inhalt der belästigenden Anrufe nicht aufgezeichnet wird.

Man kann drei Verfahrensstadien unterscheiden, wenn staatliche Stellen Telefone überwachen wollen:

— die Entscheidung, Telefongespräche abzuhören;

— die Durchführung dieser Entscheidung und

— die Kontrolle dieser Überwachungsmaßnahme, nachdem sie beendet worden ist.

Die Entscheidung, Telefongespräche abzuhören, kann getroffen werden von einer Verwaltungsbehörde (im Vereinigten Königreich), von einem Untersuchungsrichter (in den meisten Ländern) oder von einer Verwaltungsbehörde bzw. einem Gericht, je nachdem zu welchem Zweck abgehört werden soll (Deutschland). Beauftragte für den Datenschutz und den Schutz der Privatsphäre sind an diesen Entscheidungen nicht beteiligt und haben keine Kompetenz, sie zu überwachen. Dies bezieht sich ebenso auf die Durchführung der Anordnung, Telefongespräche abzuhören.

Sobald allerdings die Abhörmaßnahme beendet worden ist, gibt es gute Gründe dafür, daß die Beauftragten für den Datenschutz und den Schutz der Privatsphäre die Befugnis erhalten, die Nutzung der Daten zu kontrollieren, die aus der Abhörmaßnahme stammen. In einigen Ländern wächst die Erkenntnis, daß Beauftragte für den Datenschutz und den Schutz der Privatsphäre eine wichtige Rolle in diesem Bereich zu spielen haben, obwohl sie bisher noch keine derartige Kompetenz haben mögen.

In den Niederlanden wird das Recht möglicherweise in naher Zukunft in der Weise geändert, daß die Ergebnisse einer Abhörmaßnahme in den Akten der Nachrichtendienste dokumentiert werden. Sobald dies geschieht, würden diese Akten der Kontrollkompetenz der Registratiekamer unterliegen.

In Deutschland kann der Bundesbeauftragte für den Datenschutz nicht in ein gerichtliches Verfahren eingreifen, das zu einer Abhöranordnung führt. Aber der Bundesminister für Post und Telekommunikation hat anerkannt, daß der Bundesbeauftragte für den Datenschutz zu kontrollieren hat, ob die Deutsche Bundespost TELEKOM die Abhöranordnung korrekt durchführt, welche Art personenbezogene Daten bei Durchführung der richterlichen Anordnung erhoben werden und für welchen Zweck sie genutzt werden. Es ist entscheidend, daß die Ergebnisse einer Abhörmaßnahme nur für den Zweck benutzt werden, für den die Daten ursprünglich erhoben wurden.

In mehreren Ländern wird das Recht geändert, um die Überwachung von Nachrichten zu ermöglichen, die mit anderen Telekommunikationsmitteln (Telefax, Telex, Datenübertragung etc.) übermittelt werden. Zum Teil wird diese Gesetzgebung sich auch auf private Netzbetreiber und Diensteanbieter erstrecken und sie zur Zusammenarbeit mit der Polizei verpflichten.

Man muß sich vergegenwärtigen, daß die Überwachung von Telekommunikationsverbindungen, insbesondere das Abhören von Telefongesprächen, kein gewöhnliches Überwachungsmittel ist, das automatisch gegen jeden eingesetzt werden kann, der bestimmte Verbrechen begeht oder die nationale Sicherheit bedroht. Es ist im Gegenteil in den meisten Ländern eine Ermittlungsmethode für Ausnahmesituationen und unterliegt zusätzlichen Bedingungen. In einer Reihe von Ländern kann die Überwachung von Telefongesprächen nur angeordnet werden, wenn jemand einer Straftat verdächtigt wird, zu deren Aufklärung die Abhörmaßnahme beitragen kann, und nur dann, wenn herkömmliche Ermittlungsmethoden unpraktikabel oder erfolglos sind.

Es ist entscheidend, daß die Person, deren Telefongespräche abgehört worden sind, von der verantwortlichen Behörde über die Abhörmaßnahme informiert wird, sobald dies möglich ist, ohne den Zweck der Ermittlungen zu gefährden.

Nur dann ist der Einzelne in der Lage, die Abhörmaßnahme durch einen Richter oder ein anderes unabhängiges Organ überprüfen zu lassen. Die Benachrichtigung des Betroffenen ist bisher allerdings nur in wenigen nationalen Rechtssystemen vorgesehen.

3. Das Recht des Bürgers, das Telefon zu benutzen, ohne registriert und beobachtet zu werden, schützt ihn nicht nur gegen die Aufzeichnung der Gesprächsinhalte, sondern auch gegen die Nutzung der technischen Daten, die vom Telekommunikationsnetz für andere als Abrechnungszwecke

erzeugt werden (Verbinddungsdaten wie Zeit, Dauer des Gesprächs und Rufnummer des Angerufenen). Allerdings gibt es von diesem Grundsatz noch weiterreichende Ausnahmen als vom Prinzip der Vertraulichkeit des Gesprächsinhalts. In Belgien und Deutschland können Verbindungsdaten aufgrund einer strafgerichtlichen Anordnung in jedem Strafverfahren genutzt werden, während das Abhören von Telefongesprächen im eigentlichen Sinn in vielen Ländern nur bei bestimmten Katalogstraftaten zulässig ist.

Auch in dieser Beziehung lassen sich in den verschiedenen Rechtssystemen unterschiedliche Tendenzen feststellen. In Australien hat der Attorney-General vor kurzem vorgeschlagen, den Begriff der Kommunikationsüberwachung neu zu definieren, so daß er das Mithören oder Aufzeichnen von Informationen umfaßt, die eine Person einer anderen über ein Telekommunikationssystem übermittelt, ohne daß beide Gesprächsteilnehmer davon wissen; die Registrierung von Verbindungsdaten sollte nicht mehr unter diesen Begriff fallen. Diesen Vorschlag hat der australische Beauftragte für den Schutz der Privatsphäre scharf kritisiert. Nach seiner Auffassung sollten Verbindungsdaten und Inhaltsdaten, die über ein Telefonnetz übermittelt werden, in der gleichen Weise geschützt werden. Aufgrund neuerer technischer Entwicklungen (insbesondere der Einrichtung von digitalen Telekommunikationsnetzen) werden Verbindungsdaten systematisch von den Netzbetreibern gespeichert und sind deshalb für eine gewisse Zeit auch für andere Zwecke wie Strafverfahren verfügbar. Es gibt keinen Grund für ein unterschiedliches Schutzniveau für Inhaltsdaten einerseits und Verbindungsdaten andererseits. Der Grundsatz der Vertraulichkeit von Telefongesprächen schützt sowohl deren Inhalt als auch deren nähere Umstände (Zeit, Dauer und die an ihnen beteiligten Personen).

Aus demselben Grund hat die deutsche Konferenz der Datenschutzbeauftragten den Bundestag aufgefordert, die alte Vorschrift aufzuheben, die die Nutzung von Verbindungsdaten für jedes Strafverfahren zuläßt. Wendet man diese Vorschrift auf digitale Netze an, so ist sie mit dem verfassungsrechtlich geschützten Fernmeldegeheimnis nicht mehr vereinbar.

4. Da die Gesetzgebung über die Telekommunikationsüberwachung gegenwärtig in vielen Ländern, die in der Arbeitsgruppe vertreten sind, geändert wird, kann dieser Bericht nur ein Zwischenbericht sein. Es ist notwendig, daß die Beauftragten für den Datenschutz und den Schutz der Privatsphäre die technische und rechtliche Entwicklung in diesem Bereich genau beobachten, um die Privatsphäre des Einzelnen gegen exzessive Überwachung zu schützen.

Satellitenkommunikation

Vor mehr als sechs Jahren verabschiedete die VII. Internationale Konferenz der Datenschutzbeauftragten in Luxemburg eine Entschließung über Datenschutz und Neue Medien, in der sie betonte, daß der „Einsatz von Satelliten zur Kommunikation" . . . „Im Hinblick auf die Datenintegrität und den Schutz vor unbefugtem Abhören ebenfalls Risiken" schafft.

Seitdem scheinen diese Risiken fast vergessen, obwohl es geradezu eine Revolution am Himmel gegeben hat, was die Kapazität der Satelliten angeht. Der Kapazitätszuwachs der europäischen Satelliten von 1989 bis 1993 wird bei 215 % liegen (vgl. EG-Kommission, Grünbuch zur Satellitenkommunikation, Tabelle 5. S. 57).

Satelliten können für eine Reihe von Zwecken eingesetzt werden, deren wichtigste die Verteilung von Fernsehprogrammen und die Telekommunikation sind. Es gibt andere Einsatzmöglichkeiten wie etwa die weltweite

— Positionsbestimmung und das Flottenmanagement,

— Fernmessen und Fernwirken,

— Fernerkundung.

1. *Telekommunikation*

Ein Satellitensystem besteht in der Regel aus mindestens zwei Erdfunktionen und dem Raumsegment. Informationen werden von einer leistungsstarken Erdfunkstation zum Satelliten gefunkt („Uplink", Aufwärtsstrecke; ein fester Punkt — zu — Punkt-Dienst). Sie werden dann über Transponder im Satelliten zurück zu einer anderen Erdfunkstation oder mehreren Erdfunkstationen übermittelt („Downlink", Abwärtsstrecke). Bei der Abwärtsstrecke sind verschiedene Dienstformen vorstellbar, wie z. B. ein fester (Punkt — zu — Punkt-Telekommunikations-) Dienst, ein Fernsehverteil-Punkt — zu — Mehrfachpunkt-Dienst, ein mobiler Dienst, bei dem Informationen zu beweglichen Empfangsstationen wie etwa Lastwagen mit kleinen Dachantennen gefunkt werden. Moderne Satelliten tragen bis zu 16 Transponden und jeder Transponder kann bis zu zwei Fernsehkanäle oder 1 700 Telefonsprachkanäle übertragen.

In Europa werden nur 2 bis 3 % der internationalen Telefongespräche über Satellit abgewickelt, während Satelliten eine weit größere Rolle bei transatlantischer und interkontinentaler Telekommunikation spielen, wo sie fast 60 % des Verkehrsaufkommens übernehmen. Satellitengestützte Kommunikationsnetze sind von großer Bedeutung für den Aufbau der Telefoninfrastruktur in Ost- und Zentraleuropa. Die Entwicklung von billigen Antennen mit einem Durchmesser von weniger als einem Meter, insbesondere VSATs (Very Small Aperture Terminals, auch Mikrostationen genannt) die schon in den Vereinigten Staaten weit verbreitet sind, erleichtert neue Punkt — zu Mehrfachpunkt-Dienste. Die Unterscheidung zwischen Individual- und Massenkommunikation verschwimmt immer mehr. Mikrostationen können reine Empfangs- oder interaktive Empfangs- und Sendeterminals sein. Diese technische Entwicklung führt zur Entstehung von weltweiten mobilen

„Overlay"-Telekommunikationsnetzen. Sie werden terrestrische Mobilfunknetze, die in dicht besiedelten Gebieten bestehen, ergänzen, allerdings nicht ersetzen. Satellitenkommunikation wird besondere Bedeutung in großen, dünn besiedelten Ländern wie Australien, Kanada und Rußland haben. Das Raumsegment eines Satellitensystems steht im Eigentum einer internationalen Organisation wie z. B. INTELSAT (International Telekommunications Satellite Organisation), EUTELSAT, INMARSAT (International Maritime Satellite Organisation), American Mobile Satellite Corporation (USA), TELESAT MOBILE (Kanada) oder AUSSAT (Australien). Dabei handelt es sich um kommerzielle Organisation auf der Grundlage von zwischenstaatlichen Verträgen, die selbst allerdings keine Völkerrechtssubjekte sind. Alle Unterzeichnerstaaten haben einen gewissen Kapitalanteil an der Organisation. Die Satellitenorganisationen verkaufen Kapazitäten im Raumsegment entweder selbst oder durch Diensteanbieter.

Neue Dienste vor allem für geschlossene Benutzergruppen umfassen:

a) INTELSAT Business Service (IBS), der Sprachübermittlung, Fax, Telex, Datenübertragung, elektronische Post und Videokonferenzen integriert,

b) INTELNET-Dienste, die auf Datenverteilung und Datensammlung beschränkt sind,

c) nationales oder weltweites satellitengestütztes Paging.

Geostationäre Telekommunikationssatelliten (also Satelliten, die sich in einer gleichzeitigen Umlaufbahn zur Erdoberfläche bewegen), die gegenwärtig in Betrieb sind, reflektieren lediglich die Daten, die zu ihnen heraufgefunkt werden, auf einer anderen Frequenz hinunter zu einer anderen Erdfunkstation.

Nicht-geostationäre Satelliten können Informationen von einem Punkt der Erdumlaufbahn zu einem anderen transportieren, was die Speicherung von Daten im Raumsegment über eine längere Zeit erforderlich machen würde, als für das bloße Reflektieren der Daten erforderlich ist. Ein deutscher Forschungssatellit, der gegenwärtig Wissenschaftlern in der Arktis dient, funktioniert auf diese Weise (wie ein Postbote).

Sobald Daten im Raumsegment verarbeitet werden, wachsen die klassischen Risiken für die informationelle Selbstbestimmung, die mit jeder Verarbeitung von personenbezogenen Daten verbunden sind. Die EG-Kommission hat erkannt, daß satellitengestützte Kommunikationen sowohl nationale wie auch EG-Gesetzgebung umgehen kann. Allerdings hat die Kommission bisher kein überzeugendes Konzept entwickelt, wie diesen Risiken zu begegnen ist.

2. *Positionsbestimmung und Flottenmanagement*

Satelliten werden zunehmend für Zwecke der Navigation nicht nur von Schiffen (die das INMARSAT-System nutzen), sondern auch von Lastwagen und sogar Einzelpersonen genutzt.

EUTELTRACS ist ein europäisches satellitengestütztes System für die mobile Landkommunikation zum Management von LKW-Flotten. Die Position eines Fahrers und seine Bewegungen mit dem LKW können von einer Zentralstelle zu jeder Zeit überprüft werden. Dies spart für das Unternehmen Zeit und Geld und könnte auch zur Vermeidung von Verkehrsstauungen beitragen, wenn die Zentralstelle den Fahrern alternative Routen vorschlagen kann, die weniger überfüllt sind.

Das Global-Positioning-System (GPS-globales Positionsbestimmungssystem) wurde vom Pentagon entwickelt und erfolgreich im Golfkrieg getestet. Es beruht auf gegenwärtig 16 Satelliten (Ende 1993 werden es 21 sein), von denen jeder die genaue Zeit und Position aussendet, die von jedem, der mit einem GPS-Empfänger ausgerüstet ist, empfangen werden kann. Der Empfänger wiederum berechnet seine genaue Position im Verhältnis zum Satelliten. Dieses System erlaubt z. B. einer Reederei, den Standort jedes ihrer Schiffe weltweit zu ermitteln und dann Informationen an das Schiff über INMARSAT zu übermitteln. Piloten und in naher Zukunft auch Fahrer können das System zusammen mit digitalen Landkarten benutzen, um ihren Weg in unbekannter Umgebung zu finden.

Gleichzeitig ist es offensichtlich, daß mit einem solchen System ein elektronisches Bewegungsprofil des einzelnen ohne dessen Einwilligung erzeugt werden kann.

3. *Fernmessen und Fernwirken*

Satellitengestützte Netze können auch genutzt werden, um Pipelines, Eisenbahnlinien, Stromleitungen und Ölquellen zu überwachen. Mit Hilfe der Fernmeßtechnik kann sogar die Temperatur in einem Kühlwagen kontrolliert und angepaßt werden. Zugleich würde dies auch eine verstärkte Überwachung der Arbeitnehmer bedeuten.

4. *Fernerkundung*

Fernerkundung ist eine ältere (ursprünglich militärische) Einsatzform von Satelliten, durch die Bodenschätze, Wolkenbildungen (für die Wettervorhersage) Umweltverschmutzung und sogar die Routen von Zugvögeln vom Himmel aus beobachtet werden können.

Im Jahre 1991 startete die European Space Agency (ESA) einen modernen Satelliten (ERS-I), um Umweltveränderungen zu erkunden. Dieser Satellit verfügt über ein Radarsystem (SAR-Synethetic Aperture-Radar), das in der Lage ist, sogar nachts oder durch eine geschlossene Wolkendecke Fotografien der Erdoberfläche zu machen. Dieser Satellit speichert bestimmte Daten, bis er eine Position erreicht, von der aus er sie zu der nächsten Erdfunkstation abstrahlen kann.

Fernerkundungssatelliten, die von den alliierten Streitkräften im Golfkrieg eingesetzt wurden, waren in der Lage, Objekte (z. B. Panzer) zu erkennen, die zwischen 1 und 5 Metern Kanten-

länge hatten. Es ist sehr wahrscheinlich, daß Satellitentechnologie, die von den Militärs entwickelt wurde, mit einer gewissen zeitlichen Verzögerung auch für den zivilen Einsatz verfügbar sein wird.

Die EG-Kommission plant, über Satellit zu kontrollieren, ob Landwirte eine geringere Menge einer bestimmten Getreideart anbauen, als die, für die sie Gemeinschaftszuschüsse erhalten. Die Technik wird bald verfügbar sein, z. B. mit Hilfe eines Satelliten die Schlagzeilen einer Zeitung zu lesen, die jemand an einer Bushaltestelle liest.

5. Die unbestrittenen Vorteile der Satellitentechnologie werden begleitet von offensichtlichen Risiken für die Privatsphäre, sobald der einzelne ins Blickfeld des Satelliten gerät. Die Beauftragten für den Datenschutz und den Schutz der Privatsphäre sollten sich deshalb für internationale Abkommen einsetzen, die regeln,

   — in welchem Ausmaß personenbezogene Daten im Weltall verarbeitet werden dürfen,

   — wer der verantwortliche Datenverarbeiter ist, wenn personenbezogene Daten im Raumsegment gespeichert werden, und wer für die Datensicherheit verantwortlich ist,

   — daß besondere technische Maßnahmen ergriffen werden müssen, z. B. sollten Verschlüsselungstechniken (die bereits im militärischen Bereich angewandt werden) für die zivile Nutzung ohne zusätzliche Kosten angeboten werden.

Der internationale Normungsprozeß für weltweite Mobilkommunikation über Satellit berücksichtigt den Datenschutz noch immer nicht hinreichend.

Gemeinsame Erklärung

Die Beauftragten für den Datenschutz und den Schutz der Privatsphäre, die sich zu ihrer XIV. Internationalen Konferenz in Sydney getroffen haben,

— begrüßen den Bericht der Arbeitsgruppe Telekommunikation und Medien,

— heben die Bedeutung der beschriebenen Probleme im Bereich des Fernmeldegeheimnisses und der Satellitenkommunikation hervor und

— stimmen darin überein, daß die technische und rechtliche Entwicklung im Bereich des Fernmeldegeheimnisses sorgfältig beobachtet werden muß, um die Privatsphäre des einzelnen vor exzessiver Überwachung zu schützen.

Anlage 18 (zu 1.7)

Übersicht über durchgeführte Kontrollen, Beratungen und Informationsbesuche

Auswärtiges Amt

Bundesministerium des Innern einschließlich Außenstelle Berlin

Bundesministerium der Justiz

Bundesministerium für Wirtschaft

Bundesministerium für Ernährung, Landwirtschaft und Forsten

Bundesministerium für Arbeit und Sozialordnung

Bundesministerium der Verteidigung einschließlich Außenstelle

Bundesministerium für Familie und Senioren

Bundesministerium für Frauen und Jugend

Bundesministerium für Gesundheit

Bundesministerium für Verkehr einschließlich Außenstelle

Bundesministerium für Post und Telekommunikation

Bundesministerium für Forschung und Technologie

Bundesministerium für Bildung und Wissenschaft

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung

Deutscher Bundestag — Verwaltung

Bundesrat — Verwaltung

Bundesnachrichtendienst

Verwaltungs- und Abwicklungsstelle des Auswärtigen Amtes, Berlin

eine Botschaft

Statistisches Bundesamt — Außenstelle Berlin —

Bundesverwaltungsamt

Bundesarchiv in Koblenz und Außenstellen in Berlin und Potsdam

Bundesamt für die Anerkennung ausländischer Flüchtlinge

Bundesamt für Verfassungsschutz

Bundeskriminalamt

Bundesamt für den Zivilschutz

Grenzschutzdirektion

Bundesamt für die Sicherheit in der Informationstechnik

Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR einschließlich einiger Archive

Deutsches Patentamt

Zollkriminalinstitut

eine Oberfinanzdirektion in den neuen Bundesländern

zwei Hauptzollämter

Treuhandanstalt

Physikalisch-Technische Bundesanstalt

Bundesanstalt für Arbeit

Militärischer Abschirmdienst

Korps und Territorialkommando in den neuen Bundesländern

Wehrbereichsverwaltung in den neuen Bundesländern

Bundesamt für den Zivildienst

Kraftfahrt-Bundesamt

Luftfahrt-Bundesamt

Wasser- und Schiffahrtsdirektion Südwest

Bundesamt für Strahlenschutz

Deutsche Bundespost Postdienst

Deutsche Bundespost Telekom, Generaldirektion

mehrere Oberpostdirektionen

Bundesdruckerei

mehrere Fernmeldeämter

ein Grenzschutzamt

eine Grenzschutzstelle

Bundesversicherungsanstalt für Angestellte

eine Betriebskrankenkasse

Techniker Krankenkasse

Bundesknappschaft

vier Berufsgenossenschaften

Berufsgenossenschaftlicher Arbeitsmedizinischer Dienst

Datenstelle der Rentenversicherungsträger (VDR)

Zentralstelle für Arbeitsvermittlung in Frankfurt

eine Ausländerbehörde im Beitrittsgebiet

eine Zentrale Ausländerbehörde für Asylangelegenheiten im Beitrittsgebiet

Zentrales Einwohnerregister für das Beitrittsgebiet

Gemeinsames Statistikamt der neuen Länder

zwei Finanzämter in den neuen Bundesländern

sieben Arbeitsämter

ein Kreiswehrersatzamt

ein Jägerbataillon

ein Instandsetzungsbataillon

zwei Zivildienstgruppen

eine Kfz-Zulassungsstelle und eine Führerscheinstelle in den neuen Bundesländern

Suchdienst des Deutschen Roten Kreuzes

Das Nationale Krebsregister der ehemaligen DDR

Wismut GmbH

Anlage 19 (zu 1.7)

Wichtige Themen und die Art ihrer Bearbeitung

Thema	Art der Erledigung
Datenschutzordnung des Deutschen Bundestages und entsprechende Ergänzung des Bundesdatenschutzgesetzes	Schriftliche Stellungnahme gegenüber dem Vorsitzenden des Ausschusses für Wahlprüfung, Immunität und Geschäftsordnung des Deutschen Bundestages sowie Anhörung durch die Berichterstatter des Ausschusses
Gesetz zur Änderung des Außenwirtschaftsgesetzes, des Strafgesetzbuches und anderer Gesetze	Schriftliche Stellungnahme gegenüber Chef BK, BMI, BMJ und BMWi sowie gegenüber dem Innenausschuß, dem Rechtsausschuß und dem Ausschuß für Wirtschaft des Deutschen Bundestages
Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG)	Beratung und schriftliche Stellungnahmen gegenüber dem BMI und dem BMJ sowie gegenüber dem Innenausschuß und dem Rechtsausschuß des Deutschen Bundestages namentlich zur Frage der Zulassung des sogenannten Lauschangriffes
Entwurf eines Gesetzes zu dem Schengener Durchführungsübereinkommen vom 19. Juni 1990	Beratung und schriftliche Stellungnahmen gegenüber dem BMI und gegenüber dem Innenausschuß des Deutschen Bundestages
Allgemeine Verwaltungsvorschrift über die Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Bundesverwaltung (Dienstanschlußvorschriften — DAV —)	Schriftliche Stellungnahme gegenüber dem BMF und dem Innenausschuß des Deutschen Bundestages
Wehrstammkarten der ehemaligen NVA	Schriftliche Stellungnahme gegenüber dem BMVG sowie gegenüber dem Vorsitzenden des Innenausschusses des Deutschen Bundestages
Errichtung der „Stiftung Archiv der Parteien und Massenorganisationen der DDR" und Gesetz zur Änderung des Bundesarchivgesetzes	Beratung und schriftliche Stellungnahme gegenüber dem BMI und dem Innenausschuß des Deutschen Bundestages
Gesetz zur Änderung des Finanzverwaltungsgesetzes und anderer Gesetze	Schriftliche Stellungnahme gegenüber dem BMF und dem Finanzausschuß des Deutschen Bundestages
Zentrales Verkehrsinformationssystem (ZEVIS)	Mitwirkung an dem vom Bundesministerium für Verkehr vorbereiteten ZEVIS-Bericht der Bundesregierung an den Deutschen Bundestag
Neuntes Gesetz zur Änderung dienstrechtlicher Vorschriften	Besprechungen, Beratungen und schriftliche Stellungnahmen gegenüber dem BMI; schriftliche Stellungnahme an den Innenausschuß des Deutschen Bundestages
Vorschriften zur ärztlichen Beurteilung der Polizeidiensttauglichkeit	Besprechung und Beratung mit dem BMI und den Datenschutzbeauftragten der Länder sowie schriftliche Stellungnahme gegenüber dem BMI
Erlaß über die Führung der ärztlichen Aufzeichnungen im BGS	Besprechung, Beratung und schriftliche Stellungnahme gegenüber dem BMI
Arbeitnehmerdatenschutz	Beratungen und Besprechungen mit den Datenschutzbeauftragten der Länder, Schriftwechsel mit dem Bundesministerium für Arbeit und Sozialordnung, Vortrag im Ausschuß für Arbeit und Sozialordnung des Deutschen Bundestages
Regelungen zur Überprüfung der Verfassungstreue für Bewerber aus den neuen Bundesländern	Beratungen und Besprechungen mit den Datenschutzbeauftragten der Länder; schriftliche Stellungnahmen gegenüber dem BMI, Behörden, Personalvertretungen und betroffenen Bürgern

Thema	Art der Erledigung
Übermittlung von Daten aus der Verkehrsunfallstatistik an die Bundesanstalt für Straßenwesen (BASt)	Beratung und schriftliche Stellungnahme gegenüber dem BMI, dem BMV, der BASt und dem Statistischen Bundesamt
Entwurf eines Bevölkerungsstatistikgesetzes	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Informationsaustausch zwischen dem ZKA und den Nachrichtendiensten	Beratung und schriftliche Stellungnahme gegenüber Chef BK, BMI und BMF
Entwurf eines Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes — Sicherheitsüberprüfungsgesetz — SÜG —	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Referentenentwurf zur Änderung des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten — Bundeskriminalamtgesetz — BKAG —	Beratung des BMI
Verkartungspläne für mehrere Abteilungen des BfV	Beratung und schriftliche Stellungnahmen gegenüber BMI/BfV
Errichtungsanordnungen für Dateien des BfV	Schriftliche Stellungnahmen gegenüber BMI/BfV
Dienstvorschriften beim BfV	Schriftliche Stellungnahmen gegenüber BMI/BfV
Übermittlung von Kfz-Sachfahndungsbestandsdaten durch das BKA an den HUK-Verband und an Kfz-Hersteller	Beratung und schriftliche Stellungnahmen gegenüber BMI/BKA
Einführung eines automatisierten Fingerabdruckidentifizierungssystems beim BKA (AFIS)	Beratung des BMI/BKA
Errichtungsanordnung für Spurendokumentationssysteme beim BKA	Schriftliche Stellungnahmen gegenüber BMI/BKA
Geheimschutzanweisung für den Bundesgrenzschutz	Schriftliche Stellungnahmen gegenüber BMI
Dienstanweisung gemäß § 17 Abs. 2 Satz 2 BVerfSchG	Schriftliche Stellungnahme gegenüber dem BMI
EUROPOL	Beratung und schriftliche Stellungnahme gegenüber BMI
Regelung über die Einrichtung von IT-Sicherheitsbeauftragten	Beratung des BMI
Vorbereitung eines Ausländerzentralregistergesetzes sowie entsprechender datenverarbeitungstechnischer Maßnahmen	Beratung und schriftliche Empfehlungen gegenüber dem BMI und dem Bundesverwaltungsamt
Durchführung des Asylverfahrensgesetzes	Schriftliche Empfehlungen gegenüber dem BMI und dem Bundesamt für die Anerkennung ausländischer Flüchtlinge
Vorbereitung von Verwaltungsvorschriften zum Ausländergesetz	Empfehlungen gegenüber dem BMI
Verwendung der Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR	Schriftliche Empfehlungen gegenüber dem Bundesbeauftragen für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) und gegenüber dem BMI, insbesondere zur Verwendung der PKZ
Verwendung von Altdaten des früheren Bundesministeriums für innerdeutsche Beziehungen (BMB) und des ehemaligen Ministeriums des Innern der DDR	Beratung und schriftliche Empfehlungen gegenüber dem BMI und dem Bundesarchiv
Durchführung des Aussiedleraufnahmeverfahrens	Beratung und schriftliche Empfehlung gegenüber dem BMI und dem Bundesverwaltungsamt

Thema	Art der Erledigung
Datenverarbeitung durch den Suchdienst des Deutschen Roten Kreuzes	Schriftliche Empfehlungen gegenüber dem BMI, dem Bundesverwaltungsamt und dem DRK
Entwurf eines Gewinnaufspürungsgesetzes	Schriftliche Empfehlungen gegenüber dem BMI
Regierungsentwurf einer Insolvenzordnung	Schriftliche Stellungnahme gegenüber dem BMJ
Regierungsentwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen	Beratung und schriftliche Stellungnahmen gegenüber dem BMJ
Entwurf einer gesetzlichen Regelung zum genetischen Fingerabdruck	Schriftliche Stellungnahme gegenüber dem BMJ
Maßnahmen zur Verstärkung des Persönlichkeitsschutzes im Strafverfahren	Schriftliche Empfehlungen gegenüber dem BMJ
Schutz von in der früheren DDR amtlich bekanntgewordenen Privatgeheimnissen	Schriftliche Empfehlungen gegenüber dem BMJ
Vorbereitung eines Gesetzes zur Änderung des Jugendgerichtsgesetzes	Schriftliche Empfehlungen gegenüber dem BMJ
Vorbereitung eines Gesetzes zur Änderung des Strafvollzugsgesetzes	Schriftliche Empfehlungen gegenüber dem BMJ
Vorbereitung eines Jugendvollzugsgesetzes	Schriftliche Empfehlungen gegenüber dem BMJ
Justizstatistik-Informationssystem	Beratung gegenüber dem BMJ
Entwurf eines Strafverfolgungsstatistikgesetzes	Beratung und schriftliche Stellungnahme gegenüber dem BMJ
Gesetz zur Änderung der Abgabenordnung (AOÄG 1994)	Beratung und schriftliche Stellungnahme gegenüber dem BMF
Zollrechtsänderungsgesetz	Schriftliche Stellungnahme gegenüber dem BMF
EG-Zollinformationnssystem	Beratung und schriftliche Stellungnahme gegenüber dem BMF
Verordnung über den automatisierten Abruf von Steuerdaten des Bundesamtes für Finanzen, der Finanzämter und Gemeinden	Schriftliche Stellungnahmen gegenüber dem BMF
Arbeitsentwurf für ein ZKA-Gesetz	Schriftliche Stellungnahme gegenüber BMF
Entwurf eines Gesetzes zur Änderung des Gesetzes über das Schornsteinfegerwesen	Schriftliche Stellungnahme gegenüber dem BMWi
Entwurf eines Gesetzes zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften	Beratung und schriftliche Stellungnahme gegenüber dem BMWi
Entwurf eines Gesetzes zur Änderung der Wirtschaftsprüferordnung	Schriftliche Stellungnahme gegenüber dem BMWi
Gesetz zur Errichtung des Bundesausfuhramtes	Beratung und schriftliche Stellungnahme gegenüber dem BMWi
Integriertes Verwaltungs- und Kontrollsystem der EG — InVeKos —	Beratung und schriftliche Stellungnahme gegenüber dem BML
Verordnung über die Anforderungen in der Meisterprüfung für den Beruf Landwirt/Landwirtin	Beratung und schriftliche Stellungnahme gegenüber dem BML
Agrarstatistikgesetz	Beratung und schriftliche Stellungnahme gegenüber dem BML
Zweites Gesetz zur Änderung des Sozialgesetzbuches	Beratung und schriftliche Stellungnahmen gegenüber dem BMA, dem BMG und dem BMFJ
Arbeitsschutzrahmengesetz	Beratung und schriftliche Stellungnahme gegenüber dem BMA
Agrarsozialreformgesetz	Beratung und schriftliche Stellungnahme gegenüber dem BMA

Thema	Art der Erledigung
Gesetz zur Änderung von Fördervoraussetzungen im Arbeitsförderungsgesetz und in anderen Gesetzen	Beratung und schriftliche Stellungnahme gegenüber dem BMA
Pflegeversicherungsgesetz	Beratung und schriftliche Stellungnahme gegenüber dem BMA
Entwurf eines Zweiten Gesetzes zur Änderung des Wehrpflichtgesetzes	Schriftliche Stellungnahme gegenüber dem BMVg
Entwurf einer Verordnung über die Führung der Personalakten der Soldaten	Schriftliche Stellungnahme gegenüber dem BMVg
Errichtungsanordnungen für Dateien des MAD	Schriftliche Stellungnahme gegenüber dem BMVg/ MAD
Zweites Gleichberechtigungsgesetz	Beratung und schriftliche Stellungnahme gegenüber dem BMFJ
Erstes SGB VIII-Änderungsgesetz	Beratung und schriftliche Stellungnahme gegenüber dem BMFJ
Gesetz über die Einführung eines freiwilligen ökologischen Jahres	Beratung und schriftliche Stellungnahme gegenüber dem BMFJ
Gesetz über die Einführung eines freiwilligen sozialen Jahres	Beratung und schriftliche Stellungnahme gegenüber dem BMFJ
Gesundheitsstrukturgesetz	Beratung und schriftliche Stellungnahme gegenüber dem BMG und dem Gesundheitsausschuß des Deutschen Bundestages
Erprobungsregelung zur Beitragsrückzahlung und begleitendes Forschungsvorhaben gemäß § 287 Abs. 1 i. V. m. §§ 65, 68 SGB V	Beratung und schriftliche Stellungnahmen gegenüber dem BMG, dem BKK-Bundesverband und der BKK Hoesch
Krankenversichertenkarten	Beratung und schriftliche Stellungnahme gegenüber dem BMG sowie den Spitzenverbänden der Krankenkassen und den Kassenärztlichen Bundesvereinigungen
Nationales Krebsregister der ehemaligen DDR	Beratung und schriftliche Stellungnahme gegenüber dem BMG
Entwurf eines Bundeskrebsregistergesetzes	Beratung und schriftliche Stellungnahme gegenüber dem BMG
Entwurf eines Gesetzes zur Aufhebung der Tarife im Güterverkehr	Beratung und schriftliche Stellungnahme gegenüber dem BMV
Entwurf einer Verordnung zur Zuverlässigkeitsüberprüfung von auf Flughäfen Beschäftigten nach § 29d LuftVG	Beratung und schriftliche Stellungnahme gegenüber dem BMV
Entwurf eines Umweltinformationsgesetzes	Beratung gegenüber dem BMU
Verordnung über den Datenschutz bei Dienstleistungen der Deutschen Bundespost Telekom (Telekom-Datenschutzverordnung — TDSV —)	Beratung und schriftliche Stellungnahme gegenüber dem BMPT und dem Poststrukturrat, Mitwirkung in Ressortbesprechungen
Entscheidung des Bundesverfassungsgerichtes zur Fangschaltung und zur Zählvergleichseinrichtung	Beratung des BMPT bei der Erörterung der rechtlichen Konsequenzen
Fehlsubventionen in Wohnungsbau	Schriftliche Stellungnahme gegenüber dem BMBau
Datenspeicher Wohnungspolitik der ehemaligen DDR	Schriftliche Stellungnahme gegenüber dem BMBau
Einzelverbindungsnachweis für Telekom-Kunden; Umsetzung der Sondervorschriften zugunsten der Telefon-Seelsorge und anderer	Schriftliche Stellungnahme gegenüber der Generaldirektion der Deutschen Bundespost Telekom, Besprechung mit Vertretern der Kirchen
Information der Telekomkunden über die Verarbeitung ihrer personenbezogenen Daten sowie ihrer Rechte nach datenschutzrechtlichen Vorschriften	Beratung der Generaldirektion der Telekom bei der Gestaltung von Merkblättern und Vordrucken
Einsatz von Zählvergleichseinrichtungen durch die Telekom	Beratungen der Generaldirektion Telekom für die Verfahrensgestaltung bei Rechnungsbeschwerden

Thema	Art der Erledigung
APC-Einsatz bei der Deutschen Bundespost Telekom	Beratung der Generaldirektion bei der Erstellung einer unternehmenseinheitlichen Regelung
Einführung einer Kundennummer für Telekom-Kunden	Beratung der Generaldirektion Telekom
Forschungsvorhaben gemäß § 287 Abs. 1 i. V. m. §§ 67, 68 SGB V	Beratung und schriftliche Stellungnahme gegenüber der Hamburgischen Zimmererkrankenkasse
Forschungsvorhaben gemäß § 287 SGB V	Beratung undd schriftliche Stellungnahme gegenüber der VW-Betriebskrankenkasse
Personaldatenverarbeitung einschließlich Beihilfeangelegenheiten	Beratungen und schriftliche Stellungnahmen gegenüber Behörden und Personalvertretungen

Anlage 20

Der Bundesbeauftragte
für den Datenschutz

Dr. Einwag

Leitender Beamter

Dir Dr. Jacob

Zentrale Aufgaben	**OARn Schumacher** Presse und Öffentlichkeitsarbeit
	OAR Czepluch Personal-, Haushalts- und Organisationsangelegenheiten, Innerer Dienst, Fortbildungsangelegenheiten
Referat I	**MinR Dr. Dammann** Grundsatzangelegenheiten, Internationales, nicht-öffentlicher Bereich, Meldewesen
Referat II	**MinR Dr. Au** Rechtswesen, Finanzen, Verteidigung
Referat III	**MinR Spickschen** Sozialwesen, Personalwesen
Referat IV	**MinR Dr. Schmidt** Wirtschaft und Verkehr, Forschung, Statistik, Archivwesen, Post, Umweltangelegenheiten
Referat V	**MinR Dr. von Pommer-Esche** Polizei, Nachrichtendienste
Referat VI	**RegDir Alke** Informationstechnik
Referat VII	**MinR Ottermann** Allgemeine innere Verwaltung, Strafrecht, Aufarbeitung der MfS-Unterlagen

Riemenschneiderstr. 11
5300 Bonn 2
ab 01.07.1993: 53175 Bonn

Postfach 20 01 12
5300 Bonn 1
ab 01.07.1993: 53131 Bonn

Telefon (02 28) 8 19 95-0

Telefax (02 28) 8 19 95-50

Telex 228 3771=BfD

Sachregister

Abgabenordnung 54f., 58
Abhören von Funksendungen 123
Abhören von Telefongesprächen 29, 198ff.
→ s. Telefonüberwachung
AFIS 11, 35, 132
Agrarförderung 12, 60f.
Agrarsozialreformgesetz 82
Akteneinsicht 78
Allfinanzkonzept 157
Altdaten der ehemaligen DDR 19
Anonymisierung 60, 125f.
Anspruchs- und Anwartschafts-Überführungsgesetz 25, 26f.
APIS 135ff.
Arbeitnehmerdatenschutzgesetz 62, 182
Arbeitsförderungsgesetz 10, 77
Arbeitslosengeld 83, 86
Arbeitsplatzcomputer → s. Personalcomputer
Arbeitsvermittlung 84, 85, 87, 88f.
Ärztliche Gutachten und Atteste 73ff., 87f., 97
Ärztliche Untersuchungen 73ff., 86f., 101f.
Assessment-Center 69f.
Asylverfahren 10, 35, 145
Ausländergesetz 36
Ausländerzentralregister (AZR) 33ff., 152
Auslandsvertretungen 15, 44f.
Außenwirtschaftskontrolle 10, 58f., 139
Aussiedleraufnahme 41f., 43
Auswärtiges Amt 15, 43f., 68
Automatisiertes Abrufverfahren 34, 58f., 76, 106, 152, 154, 195

Bankeinzugsverfahren 116f.
Bankgeheimnis 55
Bausoldat 28
Beihilfe 62ff.
Berufsgenossenschaft 22f., 26, 97ff.
Bestandsdaten 191
Betriebsärztlicher Dienst 73
Beurteilung 68, 69
Bevölkerungsstatistik 127
Bewerber 66ff., 88f.
Biometrie 138f.
Bundesamt für Sicherheit in der Informationstechnik (BSI) 147f., 149, 151
Bundesamt für den Zivildienst 27, 28, 101ff.
Bundesamt für Finanzen 55, 56
Bundesamt für Verfassungsschutz 141ff.
Bundesanstalt für Arbeit 10, 83ff., 91
Bundesanstalt für Arbeitsmedizin 25f.
Bundesanstalt für gesamtdeutsche Aufgaben 40
Bundesarchiv 19, 20, 21, 30f., 40f.
Bundesaufsichtsamt für das Versicherungswesen 60
Bundesausfuhramt 10, 58f.
Bundesbahn 151
Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) 21, 30, 36ff.
Bundeskriminalamt 13, 48, 68, 107, 129f., 132ff., 160
Bundesminister für Innerdeutsche Beziehungen (BMB) 40
Bundesministerium für Verteidigung 27ff., 100f.
Bundesnachrichtendienst (BND) 146
Bundesversicherungsanstalt für Angestellte (BfA) 26f., 78, 79, 84, 96f.
Bundesverwaltungsamt (BVA) 34f., 41, 44, 152
Bundeswehr 100f.
Bundeszentralregister 41, 51, 138, 160

Chipkarte 148
Confounder-Daten 26

DALEB 11
Daktyloskopie 132
Dateiverzeichnis 17, 194
Datenlöschung 18f., 105, 133f., 147, 194
Datennetze 150f.
Datensicherung 147ff.
Deutsche Bundesbahn → s. Bundesbahn
Deutscher Bundestag 32f., 154, 155
Deutsches Rotes Kreuz 42f.
Dienstanschlußvorschriften 65ff.
Diskretionszone 44, 162
Disziplinarverfahren 69, 71f.
DNA-Analyse → s. Genomanalyse
Drittschuldner 162
Düsseldorfer Kreis 153, 155f.

EG-Datenschutz-Richtlinie 57, 159
Eingaben 14, 43f.
Einigungsvertrag 13, 18ff., 20, 21, 23, 25, 27, 28, 38, 50, 154f.
Einzelverbindungsnachweis (EVN) 118f., 191
electronic cash 157
Erbschaftsteuer- und Schenkungsteuergesetz 58
Europa 130ff.
Europäische Gemeinschaft 11, 12, 55ff., 113f., 126, 140f., 157ff.
Europäische Informationssysteme 157ff.
Europarat 158f.
EUROPOL 130f.

Fahrerlaubnisregister → s. Führerschein
Fahrzeugbrief und -schein 108
Fahrzeugdaten 106ff.
Familienzusammenführung 40, 42
Fangschaltung 117
Fernmeldegeheimnis 117, 123, 133, 139f., 158
Finanzbehörden 58
Flughafen 11, 139
Flugunfalluntersuchung 111f.
Freistellungsauftrag → s. Zinsabschlaggesetz
Führerschein 109f., 161
Funktelefon 11, 121, 123, 191

Gefahrguttransport 112
Gefangenenkartei 40f.
Geldwäschegesetz → s. Gewinnaufspürungsgesetz
Genetischer Fingerabdruck 49
Genomanalyse 104f.
Genomanalyse im Strafverfahren 49f.
Gesellschaftliches Arbeitsvermögen der DDR 21
Gesundheitsdaten 21f., 79
Gesundheitsstrukturgesetz 10, 89f.
Gesundheitsunterlagen 24ff.
Gewalttäter Sport 133
Gewerbeordnung 59
Gewinnaufspürungsgesetz 10, 46f.
Grenzkontrolle 137, 138f.
Grenzschutz 137f.
Grunderwerbsteuergesetz 58

Häftlingsfreikauf 40
Handwerksordnung 59
Heimatortskartei 41
Hooligandatei 133

inoffizieller Mitarbeiter 39
INPOL 129, 132, 137

Insolvenzordnung 54
Internationale Datenschutzkonferenz 17, 158, 198
ISDN 11, 118, 123f., 191
IT-Sicherheitsbeauftragter 151

Jugendgerichtshilfe 51f.
Justizakten 36, 37
Justizmitteilungsgesetz 53

Kaderakte 23ff.
Kfz-Fahndung 132
Kirche 155
Konkurrentenklage 70f.
Konkursverfahren 54
Kontrollmitteilung 58
Kontrollrecht des BfD 18, 20, 42, 45, 153, 159f.
Kraftfahrt-Bundesamt 106ff., 152, 161
Krankenversichertenkarte 92f., 148
Krebsregister 15, 19, 29, 103f.
Kreditwirtschaft 157
Kreiswehrersatzamt 27, 28f.
Kriegsdienstverweigerer 28, 101f.
Kriegsgerichtsakten 31
Kriminalaktennachweis 134f.
Kryptographische Verschlüsselung 44, 107, 123, 148, 149, 151, 193, 196

Landesdatenschutzbeauftragter 14, 16, 55, 133
Landwirt 60, 61
Lauschangriff 13, 45f., 47f.
Leistungsmißbrauch 81, 83f.
Luftaufsicht 111
Luftfahrt 110f.
Luftverkehrsrecht 15, 110f.

Melderegister 20f.
Militärischer Abschirmdienst (MAD) 147
Militärisches Zwischenarchiv Potsdam 30f.
Ministerium für Staatssicherheit 23f.
Mithören von Telefongesprächen 30, 123
Mobilfunk → s. Funktelefon

Nachsendungsantrag 114f.
NADIS 146
Nationale Volksarmee 16, 27f.

online → s. automatisiertes Abrufverfahren
Ordnungswidrigkeit 108f., 112
Organisierte Kriminalität 10, 45ff., 48, 131, 132, 198

Paßwort 124f., 148f., 151, 193
Patientengeheimnis 73ff., 76, 89f., 156
Personalakten 23ff., 31, 62f., 68, 69, 70ff., 100ff.
Personalcomputer (PC) 15, 17, 45, 85, 122, 129, 148, 149, 150, 151f., 161
Personaldatenverarbeitung 61f., 64
Personalfragebogen 23, 66ff.
Personalvertretung 65, 66, 68, 70
Personenkennzahl 20f., 25f., 27, 28, 39
Pfändungs- und Überweisungsbeschlüsse 162
Planfeststellungsverfahren 105f.
Polizeiliche Zusammenarbeit 130f., 133
Postbank 116f., 161
Postdienst 114ff.
Postfachinhaber 115f.
Postreklame 120, 154, 191
Poststrukturgesetz 118
Privatdetektei 156
Privatgeheimnis 51
Protokolldatei 149, 154, 194, 195f.

Rasterfahndung 45f., 48f.
Rauschgiftkriminalität 45f., 131
Regierungskriminalität 40
Registermeldung 17f.
Rehabilitierung 41, 50f.
Rentenversicherung 11
Robinsonliste 120, 192

Satellitenkommunikation 200
Schadenersatzanspruch 33
Schengener Durchführungsübereinkommen (SDÜ) 45, 130, 158, 159
Schengener Informationssystem (SIS) 12, 44f., 130, 159
SCHUFA 116, 157
Schuldnerverzeichnis 162
Schweigepflichtentbindungsklauseln 156f., 197
SED-Unrechtsbereinigungsgesetz 41, 50f.
Sicherheitsüberprüfung 138, 141ff., 161
Sozialdatenschutz 25f., 75ff.
Sozialdienst 72
Sozialgeheimnis 55, 75f., 98
Sozialhilfe 11
Sozialversicherungsausweis 82
Staatsschutz 135ff.
Staatssicherheitsdienst 36ff.
Stasi-Unterlagen 36ff.
Statistik 12, 27, 126ff., 162
Statistikgeheimnis 126f., 128
Steuergeheimnis 54, 55
Strafregister der DDR 41
Strafverfahrensänderungsgesetz 47, 48f.
Strafverfolgungsstatistik 129
Strafvollzugsgesetz 52
Suchdienst des DRK 42f.

Telefonbuch 119f., 191
Telefondatenverarbeitung 64ff., 125
Telefonrechnung 120f.
Telefonseelsorge 118f.
Telefonüberwachung 121f., 133, 139, 158, 198
Telefonverbindungsdaten → s. Verbindungsdaten
Telekarte 118, 191
Telekommunikation 117ff., 200
TK-Anlage 123
Treuhandanstalt 25, 31f.

Umsatzsteuer 56
Umweltinformationssystem 113
Umweltrichtlinie (EG) 113f.
Umweltstatistik 128f.
Unfallversicherung 97ff.
UNIX 148
Unterhaltspflicht 86

Verbindungsdaten 121, 123f.
Verdeckter Ermittler 45f., 48f.
Verfassungsschutz 141f., 161
Verfassungstreue 22ff., 68, 141ff., 161
Vergleichsverfahren 54
Verkehrszentralregister 109, 112
Vermögensgesetz 55
Versicherungswirtschaft 156f., 157
Verwertungsverbot 47, 50
Visum 34f., 44

Wartung 152
Wehrdienst 28
Wehrersatzwesen 101
Wehrpflichtige 27, 100f.
Wehrstammkarte 16, 27f.
Werbung 91, 92, 108, 120, 161, 192
Widerspruchsrecht 59, 153
Wirtschaftsprüfer 59
Wismut GmbH 21ff., 25, 26
Wohnungsstatistik 128

Zählvergleichseinrichtung (ZVE) 16, 117, 120f., 125
Zentrales Einwohnerregister (ZER) 20f., 39
Zeugnisverweigerungsrecht 80
ZEVIS 106f., 109, 152
Zinsabschlaggesetz 10, 55
Zivildienst 28, 101ff.
Zollinformationssystem der EG (CIS) 12, 57, 140f.
Zollkriminalamt (ZKA) 59, 140, 141
Zoll- und Agrarregelungen 12, 57
Zollverwaltungsgesetz 55f.
Zweieranschluß 30

Abkürzungsverzeichnis

1. SED-UnBerG	Erstes Gesetz zur Bereinigung von SED-Unrecht (Erstes SED-Unrechtsbereinigungsgesetz)
AA	Auswärtiges Amt
AAÜG	Anspruchs- und Anwartschaftsüberführungsgesetz
ADV	Automatisierte Datenverarbeitung
AFG	Arbeitsförderungsgesetz
AFIS	Automatisiertes Fingerabdruck-Identifizierungssystem
AO	Abgabenordnung
AOÄG	Gesetz zur Änderung der Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
APC	Arbeitsplatzcomputer
APIS	Arbeitsdatei PIOS innere Sicherheit
ASRG	Agrarsozialreformgesetz
AsylVfG	Asylverfahrensgesetz
AtomG	Atomgesetz
AuslG	Ausländergesetz
AWV	Arbeitsgemeinschaft für wirtschaftliche Verwaltung
AZR	Ausländerzentralregister
BA	Bundesanstalt für Arbeit
BAD	Berufsgenossenschaftlicher Arbeitsmedizinischer Dienst
BAfAM	Bundesanstalt für Arbeitsmedizin
BAFl	Bundesamt für die Anerkennung ausländischer Flüchtlinge
BAG	Bundesarbeitsgericht; auch: Bundesamt für Güterverkehr
BArchivG	Bundesarchivgesetz
BAZ	Bundesamt für den Zivildienst
BBG	Bundesbeamtengesetz
BDO	Bundesdisziplinarordnung
BDSG	Bundesdatenschutzgesetz
BeamtVG	Beamtenversorgungsgesetz
BfA	Bundesversicherungsanstalt für Angestellte
BfD	Bundesbeauftragter für den Datenschutz
BfGA	Bundesanstalt für gesamtdeutsche Aufgaben
BfV	Bundesamt für Verfassungsschutz
BG	Berufsgenossenschaft
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGSG	Bundesgrenzschutzgesetz
BKA	Bundeskriminalamt
BKA-AN	BKA-Aktennachweisdatei
BKA-VNP	BKA-Versorgungsnachweisdatei Personen
BKK	Betriebskrankenkasse
BMA	Bundesministerium für Arbeit und Sozialordnung
BMB	Bundesministerium für innerdeutsche Beziehungen
BMBau	Bundesministerium für Raumordnung, Bauwesen und Städtebau
BMF	Bundesministerium der Finanzen
BMFT	Bundesministerium für Forschung und Technologie
BMFJ	Bundesministerium für Frauen und Jugend
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BML	Bundesministerium für Ernährung, Landwirtschaft und Forsten
BMPT	Bundesministerium für Post und Telekommunikation
BMU	Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit
BMV	Bundesministerium für Verkehr
BMVg	Bundesministerium der Verteidigung
BMWi	Bundesministerium für Wirtschaft
BND	Bundesnachrichtendienst

BPersVG	Bundespersonalvertretungsgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStatG	Bundesstatistikgesetz
BStU	Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BR-Drs.	Bundesrats-Drucksache
BT-Drs.	Bundestags-Drucksache
Btx	Bildschirmtext
BVA	Bundesverwaltungsamt
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung
BVerfSchG	Bundesverfassungsschutzgesetz
BVerwG	Bundesverwaltungsgericht
BVerwGE	Bundesverwaltungsgerichtsentscheidung
BVFG	Bundesvertriebenengesetz
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
BZV	befristeter Zählvergleich
CIS	Zollinformationssystem der EG-Mitgliedstaaten
coArb	computerunterstützte Arbeitsverwaltung
CPU	Zentraleinheit eines Rechners (Central Processing Unit)
DAV	Dienstanschlußvorschriften
DB	Deutsche Bundesbahn
DBP	Deutsche Bundespost
DDR	Deutsche Demokratische Republik
DEVO/DÜVO	Datenerfassungsverordnung/Datenübermittlungsverordnung
DNA	Desoxyribonuclein acid (acid = Säure)
DRK	Deutsches Rotes Kreuz
DV/dv	Datenverarbeitung
DVAT	Datenverschlüsselung auf AT-Rechner
EDU	Europäische Drogeneinheit
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
EIS	Europäisches Informationssystem
EStG	Einkommensteuergesetz
EUROPOL	Zentrales Europäisches Kriminalpolizeiamt
EUROSTAT	Statistisches Amt der Europäischen Gemeinschaft
EVN	Einzelverbindungsnachweis
EWG	Europäische Wirtschaftsgemeinschaft
FAA	US-Amerikanisches Luftfahrt-Bundesamt (Federal Aviation Administration)
FIN	Fahrzeug-Identifizierungsnummer
FRV	Fahrzeugregisterverordnung
FTZ	Forschungs- und Technologiezentrum der Telekom
GBl. DDR	Gesetzblatt der DDR
GG	Grundgesetz
GGO	Gemeinsame Geschäftsordnung der Bundesministerien
GMBl	Gemeinsames Ministerialblatt
GUS	Gemeinschaft unabhängiger Staaten
GVG	Gerichtsverfassungsgesetz
HUK-Verband	Verband der Haftpflichtversicherer, Autoversicherer und Rechtsschutzversicherer e. V.
HVBG	Hauptverband der gewerblichen Berufsgenossenschaften
IAO	Internationale Arbeitsorganisation
ICAO	Abkommen über die internationale Zivilluftfahrt vom 7. Dezember 1944 (Convention on International Civil Aviation)
IHK	Industrie- und Handelskammer
IKK	Innungskrankenkasse
IM	Inoffizieller Mitarbeiter der Stasi
INPOL	Informationssystem der Polizei
InVeKoS	Integriertes Verwaltungs- und Kontrollsystem
ISDN	Integrated Services Digital Network

IT	Informationstechnik
ITG	Informationstechnische Gesellschaft
JGG	Jugendgerichtsgesetz
JUSTIS	Justiz-Informationssystem
JZ	Juristenzeitung
KAN	Kriminalaktennachweisdatei
KBA	Kraftfahrt-Bundesamt
KBV	Kassenärztliche Bundesvereinigung
KDVG	Kriegsdienstverweigerungsgesetz
KG	Kindergeld
KJHG	Kinder- und Jugendhilfegesetz
KKH	Kaufmännische Krankenkasse Hannover
KOBRA	Kontrolle bei den Ausfuhren
KoKo	kommerzielle Koordinierung
KSZE	Konferenz für Sicherheit und Zusammenarbeit in Europa
KVK	Krankenversicherungskarte
LBA	Luftfahrt-Bundesamt
LuftVG	Luftverkehrsgesetz
LVA	Landesversicherungsanstalt
MAD	Militärischer Abschirmdienst
MdI	Ministerium des Innern (der ehemaligen DDR)
MfS	Ministerium für Staatssicherheit/Amt für nationale Sicherheit (der ehemaligen DDR)
MOSTA	militärischer Oberstaatsanwalt (der ehemaligen DDR)
MRRG	Melderechtsrahmengesetz
MTA	Manteltarifvertrag für Angestellte
NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenzeitschrift
NVA	Nationale Volksarmee
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZA	Neue Zeitschrift für Arbeitsrecht
ODIN	Organisationsdienst für nachgehende Untersuchungen
OFD	Oberfinanzdirektion
OrgKG	Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität
PARLAKOM	Parlamentskommunikationssystem
PC	Personalcomputer
PD-DSV	Postdienst-Datenschutzverordnung
PIOS	Auskunftssystem über Personen, Institutionen, Objekte und Sachen
PIN	persönliche Identifikationsnummer
PK	Personenkennziffer
PKZ	Personenkennzahl
PTB	Physikalisch-Technische Bundesanstalt
RDV	Recht der Datenverarbeitung (Zeitschrift)
RVO	Reichsversicherungsordnung
SAEG	Statistisches Amt der Europäischen Gemeinschaft
SAP	Sozialamt der Deutschen Bundespost
SDAG	Sowjetisch-Deutsche Aktiengesellschaft
SED	Sozialistische Einheitspartei Deutschlands
SEDOC	Europäisches System zur Übermittlung von Stellen und Bewerberangeboten im internationalen Ausgleich
SG	Soldatengesetz
SGB I	Sozialgesetzbuch Erstes Buch
SGB IV	Sozialgesetzbuch Viertes Buch
SGB V	Sozialgesetzbuch Fünftes Buch (Gesundheitsreformgesetz)
SGB VI	Sozialgesetzbuch Sechstes Buch (Rentenversicherung)
SGB VIII	Sozialgesetzbuch Achtes Buch
SGB X	Sozialgesetzbuch Zehntes Buch
SIS	Schengener Informationssystem
SPUDOK	Spurendokumentationssystem
Stasi	Staatssicherheitsdienst

StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StUG	Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz)
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrs-Zulassungs-Ordnung
SZS	Staatliche Zentralverwaltung für Statistik (der ehemaligen DDR)
TB	Tätigkeitsbericht *)
TDSV	Telekom-Datenschutzverordnung
THA	Treuhandanstalt
TK-Anlagen	Telekommunikationsanlagen
TKO	Telekommunikationsordnung
TREVI	Terrorisme, Radicalisme, Extremisme, Violence International
TÜ	Telefonüberwachung
UStG	Umsatzsteuergesetz
UVV	Unfallverhütungsvorschriften
VAP	Versorgungsanstalt der Deutschen Bundespost
VDR	Verband Deutscher Rentenversicherungsträger
VMBl	Ministerialblatt des Bundesministeriums der Verteidigung
VSA	Verschlußsachenanweisung
VwGO	Verwaltungsgerichtsordnung
VZR	Verkehrszentralregister
WSD	Wasser- und Schiffahrtsdirektion
ZAP	Zentrale ADV-Prüfung der Bundesverbände der AOK, BKK und IKK
ZAV	Zentralstelle für Arbeitsvermittlung
ZDG	Zivildienstgesetz
ZEBWis	Zentrale Erfassungs- und Betreuungsstelle Wismut
ZER	Zentrales Einwohnerregister
ZEVIS	Zentrales Verkehrsinformationssystem
ZKI	Zollkriminalinstitut
ZKA	Zentrales Kriminalamt
ZollVG	Zollverwaltungsgesetz
ZPO	Zivilprozeßordnung
ZSKI	Zentralstelle für Kriminalistische Informationsverarbeitung
ZVE	Zählvergleichseinrichtungen

*) Erster Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 8/2460
Zweiter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 8/3570
Dritter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/93
Vierter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/1243
Fünfter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/2386
Sechster Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/877
Siebenter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/2777
Achter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/4690
Neunter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/6816
Zehnter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 11/1693
Elfter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 11/3932
Zwölfter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 11/6458
Dreizehnter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 12/553

Druck: Bonner Universitäts-Buchdruckerei, 5300 Bonn
Alleinvertrieb: Verlag Dr. Hans Heger, Postfach 20 13 63, Herderstraße 56, 5300 Bonn 2, Telefon 02 28/36 35 51, Telefax 02 28/36 12 75
ISSN 0722-8333