LANDTAG RHEINLAND-PFALZ
12. Wahlperiode

Drucksache 12/7589
16. 11. 1995

Unterrichtung

durch den Landesbeauftragten für den Datenschutz

Fünfzehnter Tätigkeitsbericht nach § 29 Abs. 2 Landesdatenschutzgesetz – LDSG – für die Zeit vom 1. Oktober 1993 bis 30. September 1995

Inhaltsverzeichnis

		Seite
1.	Vorbemerkung	10
2.	Novellierung des Landesdatenschutzgesetzes	10
3.	Datenschutz in Europa	11
3.1	Europäische Datenschutzrichtlinie	11
3.1.1	Die Säulen der Europäischen Union	11
3.1.1.1	Gemeinschaftsrecht	12
3.1.1.2	Die anderen Bereiche	12
3.1.1.3	Künftige Probleme	12
3.1.2	Umsetzungsbedarf	12
3.1.2.1	Sensible Daten	12
3.1.2.2	Verarbeitung personenbezogener Daten durch die Medien	13
3.1.2.3	Widerspruchsrecht	13
3.1.2.4	Verbot automatisierter Persönlichkeitsbewertung	13
3.1.2.5	Pflicht zur Meldung bei der Kontrollstelle	13
3.1.2.6	Grenzüberschreitende Datenübermittlung	13
3.1.2.7	Struktur der Kontrollstelle	14
3.2	Sonstige Projekte und Aktionen auf EU-Ebene mit Bezug zur Datenschutzrichtlinie	15
4.	Meldewesen	15
4.1	Novellierung des Meldegesetzes	15
4.2	Novellierung der Meldedatenübermittlungsverordnung (MeldDÜVO)	15
4.3	Meldedatenübermittlung zum Zwecke der Einleitung von Ermittlungen durch das Finanzamt	16
4.4	Meldedatenübermittlung an den Ausländerbeirat	16
4.5	Meldedatenübermittlung an den Internationalen Suchdienst Arolsen (ISD)	16
4.6	Auskunft trotz Sperrung von Meldedaten	17
4.7	Namensverwechslungen	17
4.8	Widerspruch gegen die Veröffentlichung von Ehejubiläumsdaten	18
5.	Polizei	18
5.1	BND hört mit	18
5.2	Entwurf eines Gesetzes über das Bundeskriminalamt	19
5.3	Zusammenarbeit mit französischen Polizeibehörden	19
5.4	Novellierung des Polizei- und Ordnungsbehördengesetzes	20
5.5	Hooligan-Listen an US-Behörden zur Fußball-WM?	21

Dem Präsidenten des Landtags mit Schreiben vom 14. November 1995 zugeleitet. Der Bericht wurde in der Sitzung der Kommission beim Landesbeauftragten für den Datenschutz am 24. Oktober 1995 nach § 26 Abs. 3 Satz 4 LDSG vorberaten.

Druck: Landtag Rheinland-Pfalz, 15. Januar 1996

		Seite
5.6	Örtliche Überprüfungen bei der Polizei	21
5.7	Drohbriefe nach unzulässiger Abfrage	22
5.8	Polizeiliche Datensammlung zur Kontakterleichterung	22
5.9	Verkehrsunfallaufnahme-Richtlinie	23
5.10	Blutalkohol	23
5.11	Übermittlungen von Informationen über Drogenkonsum an Führerscheinstellen	23
5.12	„Geisterautos" und „Schrottfrisierungen"	24
5.13	Welchem Zweck dient das Kfz-Kennzeichen auf dem Verwarnungsblock?	24
5.14	Keine Fahndung im Personalausweisregister nach Verwarnungssündern	25
5.15	Geplante Änderungen beim polizeilichen Dokumentationssystem (POLDOK) und beim kriminalpolizeilichen Meldedienst (KPMD)	25
5.16	In welchen polizeilichen Dateien können personenbezogene Daten gespeichert sein?	26
5.17	Speicherungsdauer ausländerrechtlicher Verstöße in INPOL	26
5.18	Auswertung von Fingerabdrücken auch im Ausländer- und Asylbestand des BKA	27
6.	**Verfassungsschutz**	27
6.1	Überprüfungen der Verfassungsschutzbehörde	27
6.2	Sicherheitsüberprüfungen gesetzlich regeln	27
6.3	Novellierung des Verfassungsschutzgesetzes	28
6.4	NADIS-Identifizierungsmerkmale zur Aktenauffindung	29
6.5	Keine Auswertung von Wahlunterstützungslisten durch den Verfassungsschutz	29
7.	**Justiz**	29
7.1	Kompetenzkonflikte: MAJA – die Entwicklung von Justizautomation unter Ausschluß des LfD?	29
7.2	Gesetzliche Defizite	31
7.2.1	Dateienregelungen im Strafverfahren, Ergänzung der Strafprozeßordnung	31
7.2.2	Aufbewahrungsfristen – eine angemessene Regelung ist überfällig	32
7.3	Bundes-SISY – der entscheidende Schlag gegen Ladendiebe oder eine überflüssige und zu umfassende Zentraldatei?	32
7.4	Geschäftsstellenautomation der Staatsanwaltschaften, CUST und GAST	32
7.5	Telefonabhörmaßnahmen	33
7.5.1	Örtliche Feststellungen bei einer Staatsanwaltschaft des Landes	33
7.5.2	Sonstige Beanstandungen	34
7.5.3	Vorschläge für eine datenschutzgerechtere Ausgestaltung der Überwachung des Fernmeldeverkehrs	35
7.6	Auskunftsansprüche gegen die Strafverfolgungsbehörden?	37
7.7	Darf ein Strafurteil an eine ausländische Vormundschaftsbehörde übersandt werden?	38
7.8	Datenschutz für Opfer und Zeugen	39
7.9	Die private Nutzung dienstlicher DV-Geräte durch Justizbedienstete oder: Wie weit darf die Dienstbehörde dem Bediensteten unbemerkt ins Private folgen?	41
7.10	Strafvollzug	42
7.10.1	Das Strafvollzugsgesetz läßt die Datenschutzfragen noch immer ungeregelt	42
7.10.2	Anstaltsöffentlicher Ausruf mit Nennung des Anlasses	42
7.10.3	Dürfen Standesamtsbücher in der JVA gebunden werden?	42
8.	**Schulen, Hochschulen, Wissenschaft**	43
8.1	Zentrale Vorgaben für die automatisierte DV in Schulen fehlen	43
8.2	Schulverwaltungsprogramm COSIS/ISCO	43
8.3	Verfahren zur Lernmittelfreiheit im Schuljahr 1994/1995	43
8.3.1	Rechtsänderungen durch die Landesverordnung vom 8. April 1994, Gestaltung der Antragsunterlagen	43
8.3.2	Verfahren bei staatlich anerkannten Privatschulen	44
8.4	Dürfen die Schulen den BAföG-Ämtern die Schulabbrecher melden?	44
8.5	Die Berufung eines neuen Schulleiters unter Beteiligung der Presse	44
8.6	Das neue Universitätsgesetz	45
8.6.1	Lehrberichte	45
8.6.2	Datenerhebungsbefugnisse und weitere Regelungen zur Datenverarbeitung durch Frauenbeauftragte und Ausschüsse für Frauenfragen	45
8.6.3	Bereichsspezifische Regelung der Verarbeitung personenbezogener Studentendaten	45

		Seite
8.7	Datenschutz in Netzen: Wer ist bei der Betreibung eines Netzes durch die verfaßte Studentenschaft verantwortlich?	46
8.8	Krebsregister	46
8.9	Datenschutzfragen beim Kirchenaustritt	47
9.	**Umweltschutz**	47
9.1	Umweltinformation im Verwaltungsverfahren – von der EU-Richtlinie zum Umweltinformationsgesetz	47
9.2	Altablagerungs- und Altstandortkataster	48
9.3	Sonderabfallentsorgung in Rheinland-Pfalz	48
9.4	Daten aus dem Ablagerungs- und Verdachtsflächenkataster	49
9.5	Auslagerung von Tätigkeiten an ein privates Unternehmen	50
9.6	Öffentlichkeit und Erörterungstermin im abfallrechtlichen Planfeststellungsverfahren	50
9.7	Erfassungsblatt zum Zwecke der Veranlagung von Weinbaubetrieben zur Schmutzfrachtgebühr	51
10.	**Gesundheitswesen**	52
10.1	Statistik und wissenschaftliche Forschung mit medizinischen Daten	52
10.1.1	Meldungen und Statistik nach dem Bundesseuchengesetz	52
10.1.2	Verwendung von Leichenschauscheinen für wissenschaftliche Zwecke	52
10.1.3	Erfassungsprogramm für angeborene Fehlbildungen bei Neugeborenen (Mainzer Modell)	52
10.2	Öffentlicher Gesundheitsdienst	53
10.2.1	Landesgesetz über den öffentlichen Gesundheitsdienst	53
10.2.2	Was hat der Stuhlgang eines Polizeibeamten mit seinem verstauchten Finger zu tun?	54
10.2.3	Tonbandaufzeichnungen bei Prüfungsgesprächen	55
10.2.4	Unterrichtung von Straßenverkehrsbehörden durch die Gesundheitsämter	55
10.2.5	Übermittlung von Gesundheitsdaten durch die Gesundheitsämter an Sozialleistungsträger	56
10.3	Übersendung von Arztbriefen durch Krankenhausärzte	56
10.4	Die Befreiung vom ärztlichen Notfalldienst – ein Datenschutzproblem	57
10.5	Der „schusselige" Zahnarzt	58
10.6	Verwendung von Disketten mit Patientendaten für die Fehleranalyse	58
10.7	Aufbewahrung von Patientenunterlagen	59
10.8	Datenschutz bei der Einführung und Verwendung einer Patientenchipkarte in Neuwied/Rhein	59
11.	**Sozialdatenschutz**	60
11.1	Krankenkassen, Kassenärztliche Vereinigungen	60
11.1.1	Rechtsfragen bei der Anwendung von Vorschriften des SGB V	60
11.1.2	Eingeschränkter Zugriff auf Versichertendaten bei landesweiten oder überregionalen gesetzlichen Krankenkassen	61
11.1.3	Vorlage eines polizeilichen Führungszeugnisses für die Zulassung als Kassenarzt	61
11.1.4	Bekanntgabe von Patientendaten durch den Prüfarzt einer Kassenärztlichen Vereinigung	62
11.1.5	Diagnoseangaben auf Hilfsmittelverordnungen	62
11.2	Sozialhilfe, Kinder- und Jugendhilfe	62
11.2.1	Offenbarung von Sozialdaten gegenüber den Rechnungsprüfungsausschüssen von Ortsgemeinden	62
11.2.2	Übermittlung von Kfz-Zulassungsdaten an Sozialämter	63
11.2.3	Steuerliche Erfassung der ausgezahlten Mieten für Asylbegehrende und andere Sozialleistungsempfänger	64
11.2.4	Übermittlung von Sozialdaten an Heimträger	64
11.2.5	Sozialhilfe; Rechtswahrungsanzeige	64
11.2.6	Sozialdatenschutz im gerichtlichen Verfahren	65
11.2.7	Sozialhilfestatistik	65
11.2.8	Beratung und Unterstützung bei der Ausübung der Personensorge	65
11.2.9	Datenübermittlung von Jugendämtern an Polizeibehörden	66
11.3	Datenschutz bei Adoptionen	66
11.3.1	Einladung zur Mütterberatung	66
11.3.2	Verwendung eines Motivationserfassungsbogens bei der Adoptionsvermittlung	67
11.3.3	Überprüfung des Kindergeldanspruchs bei Adoptiveltern	67
11.4	Festsetzung von Elternbeiträgen zu den Kosten von Kindertagesstätten	67
11.5	Mitarbeiterinnen in Frauenhäusern haben Verschwiegenheitspflichten zu beachten	68
11.6	Archivierung von Akten einer Beratungsstelle für Kinder, Jugendliche und Erwachsene	68
11.7	Abrechnung der Kosten für die Schwangerenberatung	69

		Seite
11.8	Hilfe bei Schwangerschaftsabbrüchen	69
11.9	Versorgungsverwaltung; Auskunftsansprüche eines Sozialleistungsempfängers gegen einen ärztlichen Gutachter	70
12.	**Ausländerrecht**	70
12.1	ASYLCARD u. a.	70
12.2	Ausländerzentralregistergesetz (AZRG)	71
12.3	Auf Dauer keine Verwaltungsvorschrift zum Ausländergesetz?	71
12.4	Übermittlung der Auslandsadresse durch die Ausländerbehörde	71
12.5	Zwangsweise Vorführung Abzuschiebender beim Konsulat	72
12.6	Ausländerbeiratswahlen	73
13.	**Finanzverwaltung**	74
13.1	Datenschutzrechtliche Ergänzung der Abgabenordnung	74
13.2	Die Steuerdaten-Abrufverordnung: erforderlich, aber inhaltlich umstritten	74
13.3	Dürfen die Ortsbürgermeister Listen mit Daten von Gewerbesteuerzahlern und Hundesteuerpflichtigen erhalten?	74
13.4	Was darf das Finanzamt den Sozialämtern mitteilen?	75
13.5	Weitergabe von Steuerdaten durch das Finanzamt an die IHK zur Berechnung der Kammerbeiträge	75
14.	**Wirtschaft und Verkehr**	75
14.1	Überlassung von Zweitschriften der Gaststättenkonzessionen an die GEMA	75
14.2	Auskunftserteilung an Private aus dem Gewerberegister	76
14.3	Bereichsspezifische Übermittlungsregelung im Schornsteinfegergesetz	77
14.4	Datenübermittlungen im Rahmen der Fremdenverkehrswerbung	77
14.5	Musterentwurf zur Durchführung der §§ 14, 15 und 55 c der Gewerbeordnung (GewO)	78
14.6	Automatische Gebührenerhebung auf Autobahnen	78
14.7	Die Grunderwerbsverzeichnisse im Planfeststellungsverfahren	80
14.8	Neukonzeption des automatisierten Ordnungswidrigkeitenverfahrens	81
15.	**Landwirtschaft, Weinbau und Forsten**	82
15.1	Müssen Öko-Landwirte gegenüber privaten Kontrollstellen die Betriebsdaten offenbaren?	82
15.2	Datenverarbeitung im Zusammenhang mit der Agrarförderung	83
16.	**Statistik**	83
16.1	Mikrozensus 1995	83
16.1.1	Zufallsauswahl und Geheimhaltung	83
16.1.2	Gestaltung der Erhebungsvordrucke	84
16.1.3	Inhalt des Ankündigungsschreibens	84
16.2	EG-Statistikverordnung	84
16.3	Verdiensterhebungen in Industrie und Handel	85
17.	**Personaldatenverarbeitung**	85
17.1	Telefonanlagen und Mitbestimmung	85
17.1.1	Dürfen die Nummern aller Dienstgespräche vollständig gespeichert werden?	85
17.1.2	In welchem Umfang dürfen Telefondaten über im Dienst geführte private Gespräche gespeichert werden?	85
17.1.3	Wie lange dürfen Gesprächsdaten bei privaten Telefongesprächen gespeichert werden?	85
17.1.4	Dürfen Gesprächsdaten der vom Personalrat geführten Telefonate aufgezeichnet werden?	86
17.1.5	Gibt es technische Vorrichtungen, die dem Gesprächsteilnehmer deutlich machen, daß sein Partner die Konferenzschaltung oder das Freisprechen eingeschaltet hat?	86
17.1.6	Gibt es Bereiche, z. B. bei Arbeitsplätzen mit Publikumsverkehr, in denen auf die Möglichkeit des Freisprechens und der Konferenzschaltung ganz verzichtet werden muß?	86
17.1.7	Ist es zulässig, Störungen per Fernwartung beheben zu lassen?	86
17.1.8	Darf die Änderung von Kurzwahlnummern und die Vergabe der Geheimnummern über die Fernwartung erfolgen?	87
17.1.9	Dürfen die Privatgespräche aus der Hausmeisterwohnung nummernmäßig erfaßt werden?	87
17.2	Zeiterfassung	87
17.3	Personalverwaltungssystem AUP beim Landesamt für Jugend und Soziales und beim Landesversorgungsamt	87

		Seite
17.4	Vernichtete Vorgänge im Inhaltsverzeichnis einer Personalakte – Bewerbungsunterlagen in Personalakten	88
17.5	IT-Heimarbeitsplätze, Telearbeit	88
17.6	Mitbestimmung bei Nebentätigkeitsgenehmigungen	88
17.7	Stammdatenspeicherung bei Personalvertretungen; Weitergabe von Personalstammdaten aus der Personalverwaltung an die Personalvertretung	89
17.8	Dienstordnungsverfahren: dienstliche Stellung und Befugnisse des Vorermittlungsführers	90
17.9	Einsichtsrecht des Landesrechnungshofes in Personalakten der Landeszentrale für private Rundfunkveranstalter (LPR)	91
17.10	Nutzung von Personaldaten für Werbezwecke	92
17.11	Nutzung von Bewerberdaten zu Werbezwecken durch einen Bediensteten	93
17.12	Das Landesgleichstellungsgesetz	93
18.	**Datenschutz im kommunalen Bereich**	94
18.1	Tonaufzeichnungen in Ratssitzungen	94
18.2	Zusammenarbeit der Handwerkskammern mit Mandatsträgern in den Gemeinderäten	95
18.3	Weitergabe der Tagesordnung des Kreisrechtsausschusses an die örtliche Presse	95
18.4	Aktenweitergabe an die nach dem Waffengesetz zuständige Erlaubnisbehörde	96
18.5	Datenschutz im Vollstreckungswesen	96
18.6	Kommunale Datenerhebung zu Planungszwecken (§ 32 LDSG); Umfrage zur Neuorganisation des Schulzweckverbandes	96
19.	**Medien**	97
19.1	Multimedia am Start	97
19.2	Der Rundfunkbegriff im Wandel	97
19.3	Änderung des Rundfunkstaatsvertrages im Hinblick auf Reality-TV	98
19.4	Gerichtsfernsehen	99
19.5	Medienarchive	99
20.	**Telekommunikation**	99
20.1	Europäische Richtlinie zum Datenschutz im ISDN	99
20.2	Postreform II – Rechtsgrundlagen in Bewegung	100
20.3	Neuorganisation der Informationstechnik in Rheinland-Pfalz	101
20.4	Entwurf eines Gesetzes über die Errichtung des Daten- und Informationszentrums Rheinland-Pfalz (DIZ)	103
20.5	Gefahren beim täglichen Umgang mit Telefon und Anrufbeantworter	104
21.	**Technischer und organisatorischer Datenschutz**	104
21.1	Ergebnisse der Kontroll- und Beratungstätigkeit	104
21.2	Technisch-organisatorische Datenschutzfragen in einzelnen Verfahren	105
21.2.1	Automatisierte Vorgangsverwaltung der Polizei (Hamburger COMVOR-Verfahren)	105
21.2.2	Einsatz von Personalcomputern bei der Kommunalwahl 1994	106
21.2.3	Elektronische Post im Landesdatennetz (BKS-LRZ)	107
21.2.4	Haushaltsaufstellungs- (HAVWin) und Haushaltsbewirtschaftungsverfahren (IRMA)	108
21.2.5	Lohn- und Gehaltsabrechnung für die Zivilbeschäftigten der alliierten Streitkräfte Berlin	109
21.2.6	Verschlüsselung beim Datenaustausch zwischen den Allgemeinen Ortskrankenkassen und Arbeitgebern	109
21.2.7	EWKOM	110
21.3	Landesdaten- und Kommunikationsnetz Rheinland-Pfalz (LDKN)	111
21.4	Arbeitsgruppe „Verfahrensübergreifende Sicherheitskonzepte“ (IT-Grundschutz)	113
21.5	Absicherung der Zugänge zu öffentlichen Kommunikationsnetzen	114
21.6	Wartung/Fernwartung und Datenverarbeitung im Auftrag	115
21.6.1	Allgemeine Einordnung	115
21.6.2	Anforderungen bei der Durchführung der Wartung/Fernwartung	116
21.7	Computerviren auf Versanddisketten	116
21.8	Protokollierung und Dokumentation	117
21.9	Dienstanweisungen	119
22.	**Öffentlich-rechtliche Wettbewerbsunternehmen, Sparkassen**	119
22.1	Wahlfreiheit für Sparkassenkunden, welche Filiale auf ihre Kontendaten zugreifen kann	119
22.2	Geldwäschegesetz	120

Seite

22.2.1 Speicherung in staatsanwaltschaftlichen Dateien ... 120
22.2.2 Wann darf der Personalausweis fotokopiert werden? ... 120
22.3 Installation von Video-Kameras im Außenbereich ... 120
22.4 Telefonische Datenübermittlungen über den Kontostand durch eine Sparkasse ... 121
22.5 Kontoauszüge in Sichtfenster-Briefumschlägen ... 122

23. Sonstiges ... 122
23.1 Die korrekte Adressierung als Datenschutzproblem ... 122
23.1.1 Nutzung der Dienstanschrift für ein Schreiben in Personalangelegenheiten ... 122
23.1.2 Der Weg von Verurteilungsmitteilungen an das Wahlamt ... 123
23.2 Gibt es ein Einsichtsrecht des beleidigenden Bürgers in behördliche Aufzeichnungen über sein Fehlverhalten? ... 123
23.3 Ermittlungsbefugnisse, Datenübermittlungen und Auskunftserteilung an den Betroffenen durch Kreishandwerkerschaften bei der Verfolgung der Schwarzarbeit ... 124
23.4 Mahnung per Postnachnahmeauftrag ... 125
23.5 Aufzeichnung von Telefonaten in Rettungsleitstellen ... 126
23.6 Katasterwesen – Auszug aus dem Veränderungsnachweis und Eigentümernachweis ... 126
23.7 Datenschutzbürokratie ... 127
23.8 Das Datenschutzregister ... 127

24. Schlußbemerkung ... 128

Anlagen

		Seite
1	Entschließung „Kartengestützte Zahlungssysteme im öffentlichen Nahverkehr“	129
2	Entschließung „Gefährdung der Vertraulichkeit der Funkkommunikation von Sicherheitsbehörden und Rettungsdiensten“	130
3	Entschließung „Regelmäßige Datenübermittlung an die öffentlich-rechtlichen Rundfunkanstalten und die Gebühreneinzugszentrale (GEZ)“	131
4	Entschließung „Gewährleistung des Datenschutzes bei Mobilkommunikation“	132
5	Entschließung „Integriertes Verwaltungs- und Kontrollsystem (InVeKoS)“	133
6	Entschließung „Datenschutz bei der Privatisierung der Deutschen Bundespost Telekom und bei der europaweiten Liberalisierung des Telefonnetzes und anderer Telekommunikationsdienste“	134
7	Entschließung „Chipkarten im Gesundheitswesen“	135
8	Entschließung „Informationsverarbeitung im Strafverfahren“	137
9	Entschließung „Neuordnung des Postwesens und der Telekommunikation“	139
10	Entschließung „Ausländerzentralregister“	140
11	Entschließung „EG-Statistikverordnung“	141
12	Entschließung „Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen“	143
13	Entschließung „Fehlende bereichsspezifische gesetzliche Regelungen bei der Justiz“	144
14	Entschließung „Datenschutzrechtliche Anforderungen an ein Übereinkommen der Mitgliedstaaten der Europäischen Union über die Errichtung eines europäischen Polizeiamtes (EUROPOL)“	145
15	Entschließung „Verbrechensbekämpfungsgesetz, zur Trennung von Polizei und Nachrichtendiensten“	146
16	Entschließung „Geänderter Vorschlag für eine Europäische Richtlinie zum Datenschutz im ISDN und in Mobilfunknetzen“	147
17	Entschließung „Eingeschränkter Zugriff auf Versichertendaten bei landesweiten oder überregionalen gesetzlichen Krankenkassen“	148
18	Entschließung „Entwurf eines Gesetzes über das Bundeskriminalamt“	149
19	Entschließung „Automatische Erhebung von Straßennutzungsgebühren“	150
20	Entschließung „Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich“	151
21	Entschließung „Anforderungen an den Persönlichkeitsschutz im Medienbereich“	152
22	Entschließung „Sozialgesetzbuch VII“	154
23	Entschließung „Datenschutz bei Wahlen“	156
24	Entschließung „Datenschutz bei elektronischen Mitteilungssystemen“	157
25	Entschließung „Maßhalten beim vorbeugenden personellen Sabotageschutz“	159
26	Entschließung „Entwurf einer Telekommunikations- und Informationsdienstunternehmen-Datenschutzverordnung (TIDSDV) des Bundesministeriums für Post und Telekommunikation“	160

Abkürzungen

ADV	Automatisierte Datenverarbeitung
AFIS	Automatisiertes Fingerabdruck-Identifizierungssystem
AG	Amtsgericht
AGBSHG	Ausführungsgesetz Bundessozialhilfegesetz
AGVwGO	Ausführungsgesetz zur Verwaltungsgerichtsordnung
AO	Abgabenordnung
APIS	Arbeitsdatei PIOS – Innere Sicherheit
AZRG	Ausländerzentralregistergesetz
AsylVerfG	Asylverfahrensgesetz
AuslG	Ausländergesetz
BBG	Bundesbeamtengesetz
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Datenschutz
BFH	Bundesfinanzhof
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BHO	Bundeshaushaltsordnung
BKA	Bundeskriminalamt
BND	Bundesnachrichtendienst
BRRG	Beamtenrechtsrahmengesetz
BSHG	Bundessozialhilfegesetz
BVerfGE	Bundesverfassungsgerichtsentscheidungen
BZRG	Bundeszentralregistergesetz
BAföG	Bundesausbildungsförderungsgesetz
COSIS	Computerunterstütztes offenes Schulinformationssystem
CUST	Computerunterstützung der Staatsanwaltschaft
Datex-J	Bildschirmtextdienst der Deutschen Telekom
Datex-P	Paketorientierter Datenübertragungsdienst der Deutschen Telekom
DÖV	Die öffentliche Verwaltung
DSK	Datenschutzkommission
DuD	Datenschutz und Datensicherheit
ED	Erkennungsdienst
EGV	Vertrag über die Europ. Gemeinschaft
ELIAS	Einsatzleit-, Informations- und Auskunftssystem
EStG	Einkommensteuergesetz
EWGV	Vertrag zur Gründung der Europäischen Wirtschaftsgemeinschaft
EWOIS	Einwohnerinformationssystem
GAST	Geschäftsstellenautomation der Staatsanwaltschaften
GEMA	Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte
GG	Grundgesetz
GStB	Gemeinde- und Städtebund
GVG	Gerichtsverfassungsgesetz
GWG	Geldwäschegesetz
GemO	Gemeindeordnung
GewO	Gewerbeordnung
IHK	Industrie- und Handelskammer
INPOL	Polizeiliches Informationssystem
ISCO	Zusammenfassung der Programme ISIS und COSIS
ISD	Internationaler Suchdienst Arolsen
ISDN	Integrated Services Digital Network
ISIS	Internes Schulinformationssystem
JVA	Justizvollzugsanstalt
KAG	Kommunalabgabengesetz
KAVO	Kommunalabgabenverordnung
KPMD	Kriminalpolizeilicher Meldedienst
KV	Kassenärztliche Vereinigung
KpS	Kriminalpolizeiliche Sammlungen
LAbfWAG	Landesabfallwirtschafts- und Altlastengesetz
LBG	Landesbeamtengesetz
LDSG	Landesdatenschutzgesetz 1994
LDatG	Landesdatenschutzgesetz 1978
LHO	Landeshaushaltsordnung
LKA	Landeskriminalamt
LKG	Landeskrankenhausgesetz
LPersVG	Landespersonalvertretungsgesetz
LRG	Landesrundfunkgesetz
LVwVGDVO	Durchführungsverordnung zum Landesverwaltungsvollstreckungsgesetz
LfD	Landesbeauftragter für den Datenschutz
LfUG	Landesamt für Umwelt und Gewerbeaufsicht
MAJA	Mainzer Automatisierte Justizanwendungen
MG	Meldegesetz
MeldDÜVO	Meldedatenübermittlungsverordnung
MiStra	Mitteilungen in Strafsachen
NJW	Neue Juristische Wochenschrift
NVwZ	Neue Verwaltungszeitung
ÖGdG	Gesetz über den öffentlichen Gesundheitsdienst
OLG	Oberlandesgericht
ONP	Open Network Provision
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz
PC	Personalcomputer
PIOS	Personen, Institutionen, Objekte, Sachen
POG	Polizei- und Ordnungsbehördengesetz
POLADIS	Automatisierte Vorgangsverwaltung der Polizei
POLDOK	Polizeiliches Hinweis- und Spurendokumentationssystem
PVG	Polizeiverwaltungsgesetz
RdNr.	Randnummer
RiStBV	Richtlinie für das Straf- und Bußgeldverfahren
SDÜ	Schengener Durchführungsübereinkommen
SGB I	Sozialgesetzbuch – Erstes Buch –
SGB V	Sozialgesetzbuch – Fünftes Buch –
SGB VIII	Sozialgesetzbuch – Achtes Buch –

SGB X	Sozialgesetzbuch – Zehntes Buch –
SIS	Schengener Informationssystem
SISY	Staatsanwaltschaftliches Informationssystem
StDAV	Steuerdaten-Abrufverordnung
StPO	Strafprozeßordnung
StVÄG	Strafverfahrensänderungsgesetz
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrs-Zulassungsordnung
TÜ	Telefonüberwachung
Tb.	Tätigkeitsbericht
Tz.	Textziffer
UIG	Umweltinformationsgesetz
UrhWahrnG	Urheberrechtswahrnehmungsgesetz
VGH	Verwaltungsgerichtshof
VO	Verordnung
VV	Verwaltungsvorschrift
VwVfG	Verwaltungsverfahrensgesetz
WaffVwV	Allgemeine Verwaltungsvorschrift zum Waffengesetz
ZRHO	Rechtshilfeordnung für Zivilsachen

Tätigkeitsberichte der Datenschutzkommission und des Landesbeauftragten für den Datenschutz

1. Tätigkeitsbericht	Drucksache 7/3342	vom	17. Oktober	1974
2. Tätigkeitsbericht	Drucksache 8/350	vom	1. Oktober	1975
3. Tätigkeitsbericht	Drucksache 8/1444	vom	1. Oktober	1976
4. Tätigkeitsbericht	Drucksache 8/2470	vom	10. Oktober	1977
5. Tätigkeitsbericht	Drucksache 8/3492	vom	12. Oktober	1978
6. Tätigkeitsbericht	Drucksache 9/253	vom	15. Oktober	1979
7. Tätigkeitsbericht	Drucksache 9/970	vom	15. Oktober	1980
8. Tätigkeitsbericht	Drucksache 9/1869	vom	28. Oktober	1981
9. Tätigkeitsbericht	Drucksache 10/270	vom	26. Oktober	1983
10. Tätigkeitsbericht	Drucksache 10/1922	vom	8. November	1985
11. Tätigkeitsbericht	Drucksache 11/710	vom	11. November	1987
12. Tätigkeitsbericht	Drucksache 11/3427	vom	21. Dezember	1989
13. Tätigkeitsbericht	Drucksache 12/800	vom	16. Dezember	1991
14. Tätigkeitsbericht	Drucksache 12/3858	vom	12. November	1993

1. Vorbemerkung

Für den Bürger wird es angesichts des Vordringens der Informationstechnik in allen Lebensbereichen immer schwerer, sein Recht auf informationelle Selbstbestimmung zu wahren; denn er ist kaum noch in der Lage, die Informationsflüsse im öffentlichen und privaten Bereich nachzuvollziehen.

Für die Datenverarbeitung im privaten Sektor ist in den letzten Jahren der zunehmende Einsatz von Karten als Datenspeicher der verschiedensten Art und mit den unterschiedlichsten Funktionen (z. B. Krankenversichertenkarten, Patientenkarten, Kreditkarten) kennzeichnend. Aber nicht nur dies, sondern auch der zunehmende Einsatz mobiler Telefone mit der dadurch bedingten ständigen Speicherung von Bewegungsdaten der Telefonteilnehmer sowie die Entwicklungen im Bereich der Mail-Boxen und sonstiger Telekommunikationsdienste (Internet, Online-Datenbanken etc.) führen dazu, daß an verschiedenen Stellen umfangreiche Datensammlungen über das Verhalten von Bürgern entstehen, die aber leicht in eine zentrale Verarbeitung übergeführt werden können. Diese Datensammlungen lassen sich durch private Stellen unter den verschiedensten Gesichtspunkten, etwa zu Werbezwecken, auswerten. Aber auch staatliche Stellen haben zum Zweck der Strafverfolgung und der Steuererhebung derzeit rechtlich umfassende Zugriffsmöglichkeiten auf solche Datensammlungen.

Im staatlichen Bereich ist das Interesse der Öffentlichkeit zu Unrecht allein auf die Ausweitung der Ermittlungsbefugnisse von Polizei und Staatsanwaltschaft konzentriert. Die datenschutzrechtlich relevante Entwicklung wird mehr noch dadurch gekennzeichnet, daß neue zentrale Datensammlungen entstehen wie das bundesweite Register der Ermittlungsverfahren (staatsanwaltschaftliches Informationssystem SISY) oder auf landesweiter Ebene das automatisierte Liegenschaftskataster und die verschiedensten Dateien im Besteuerungsbereich. Durch die Vernetzung dezentraler Datenbestände entsteht zunehmend die Möglichkeit zentraler Auswertungen. Als Beispiel kann etwa die landwirtschaftliche Betriebsdatenbank genannt werden. Ferner sind die rechtlichen Voraussetzungen geschaffen worden, um auch die automatisiert geführten Grundbücher zu vernetzen.

Damit ist zwar nicht das eingetreten, was der Datenschutz in seinen Anfangszeiten befürchtet hat: das Entstehen eines zentralen umfassenden Datenbestandes in einem riesigen Rechenzentrum. Im Ergebnis ist die gegenwärtig absehbare Entwicklung allerdings ebenso bedrohlich: Der Umfang der automatisiert gespeicherten Daten wird durch den Einsatz der automatisierten Verfahren in allen Lebensbereichen ständig gesteigert.

Aus datenschutzrechtlicher Sicht ist das einzige Mittel, um hier Fehlentwicklungen und Mißbräuchen vorzubeugen, daß der Gesetzgeber angemessene Schranken zieht und daß auf der Ebene des Vollzugs dem technischen und organisatorischen Datenschutz der angemessene Stellenwert beigemessen wird. Beide Bereiche entsprechen derzeit noch nicht den Vorstellungen des Landesbeauftragten für den Datenschutz. Beispielsweise sei auf die Diskussion zu SISY und zur Gesundheitschipkarte verwiesen. Wenn hier auch primär der Bundesgesetzgeber gefordert ist, um einen angemessenen Interessenausgleich zwischen dem Persönlichkeitsrecht der Bürger und dem Effizienzinteresse des Staates zu schaffen, so sind doch auch auf der Ebene der Verwaltung und damit im Landesbereich vermeidbare Defizite festzustellen. Deren Beseitigung ist das primäre Anliegen des Landesbeauftragten für den Datenschutz (LfD). Der vorliegende 15. Tätigkeitsbericht gibt hierfür eine Fülle von Anregungen.

2. Novellierung des Landesdatenschutzgesetzes

Am 23. Juni 1994 hat der Landtag das neue Landesdatenschutzgesetz (LDSG) als zweite umfassende Novellierung nach dem ersten Gesetz (LDatG) vom Januar 1974 verabschiedet. Rheinland-Pfalz war seinerzeit das zweite Land mit einem allgemeinen Datenschutzgesetz und einer eigenen unabhängigen Kontrollinstanz. Die Datenschutzkommission (DSK) als Vorgängerin des Landesdatenschutzbeauftragten hatte bereits mehrfach eine Neufassung des inzwischen novellierten Gesetzes aus dem Jahre 1978 gefordert, jedoch kam es im Blick auf das dann im Jahre 1990 verabschiedete neue Bundesdatenschutzgesetz (BDSG) auch in der 11. Wahlperiode nicht mehr dazu. Entgegen der Argumentation der DSK war das Bundesgesetz bewußt abgewartet worden, obwohl in verschiedenen wesentlichen Punkten unterschiedliche gesetzgeberische Absichten bestanden, so zum Beispiel in der allgemeinen Ausdehnung der Kontrollkompetenzen des Datenschutzbeauftragten auf Akten.

Schon im April 1989 hatte die DSK in einem Schreiben an den damaligen Innenminister eine detaillierte und begründete Aufstellung der wesentlichen Grundsätze vorgelegt, die nach ihrer Auffassung unverzichtbare Bestandteile eines LDSG sein sollten, das den Anforderungen des Bundesverfassungsgerichts entspricht und das das Recht des Bürgers auf informationelle Selbstbestimmung angemessen und in zeitgemäßer Form verwirklicht.

Die Hauptforderungen waren u. a. die volle Einbeziehung der in Akten verarbeiteten personenbezogenen Daten, eine größere Transparenz, die Einbeziehung der Erhebung, eine konsequente Zweckbindung, eine präzisere Ausgestaltung der Kontrollbefugnisse sowie eine ausgewogene Regelung der Datenverarbeitung für wissenschaftliche Zwecke unter Berücksichtigung der vorhandenen Erfahrungen in der Praxis. Im Kern waren diese Punkte bereits im ersten Referentenentwurf des Ministeriums des Innern und für Sport berücksichtigt.

Im Verfahren der Entwurfsvorbereitung war der LfD zu einem frühen Zeitpunkt und umfassend beteiligt, so daß es möglich war, weitere Überlegungen einzubringen und zu diskutieren. Dabei fand die Mehrzahl der Vorstellungen des LfD Eingang in den Entwurf der Landesregierung.

Zu den auch im weiteren Verfahren nicht berücksichtigten Empfehlungen gehören u. a. der Wunsch, die Einschränkung des Nutzungsbegriffs in § 3 Abs. 2 Satz 2 Ziffer 3 aufzuheben. Der LfD hätte die Nutzungsregelung lieber weiterhin als Auffangvorschrift für Verarbeitungsformen angesehen, die nicht unter Erhebung, Speicherung usw. fallen. Der Entwurf schränkte demgegenüber diesen wichtigen Auffangtatbestand so ein, daß er nur auf Tätigkeiten innerhalb der datenverarbeitenden Stelle anwendbar ist. Damit entsteht in der Praxis eine Lücke für Fälle, in denen öffentliche Stellen außerhalb ihres Bereiches tätig werden.

Von verschiedenen vorgeschlagenen flankierenden Maßnahmen zu dem in § 7 geregelten automatisierten Übermittlungsverfahren konnte nur das vorherige Anhörungsrecht des LfD erreicht werden.

Im Laufe der Ausschußberatungen konnten im Einvernehmen mit dem Ministerium des Innern und für Sport weitere Verbesserungen eingefügt werden. Besonders hervorzuheben sind hierbei Verstärkungen der Rechte des LfD bei personalwirksamen Maßnahmen sowie bei den Kontrollmöglichkeiten. Im Regierungsentwurf noch vorgesehene Hemmnisse für das Auskunftsrecht der Bürger in Gestalt von besonderen Zustimmungsrechten beteiligter Behörden wie Staatsanwaltschaft, Finanzbehörden und Verfassungsschutz konnten so ebenfalls wegfallen. Insbesondere erwiesen sich hierbei die in der Anhörung vor dem Innenausschuß vorgebrachten Überlegungen insgesamt als hilfreich, wenn auch die pauschalierte Totalkritik des Sprechers der Deutschen Vereinigung für Datenschutz e. V. an dem gesamten Gesetzentwurf so nicht akzeptiert werden kann.

Ein erheblicher Anteil an allen erreichten Verbesserungen fällt der Unterstützung und intensiven Begleitung durch die Kommission bei dem Landesbeauftragten für den Datenschutz zu.

Insgesamt stärkt das neue Landesdatenschutzgesetz (LDSG) das Recht der Bürger auf informationelle Selbstbestimmung, wie es das Bundesverfassungsgericht in seinem Volkszählungsurteil vorgesehen und ausgestaltet hat. Zusammenfassend sind besonders hervorzuheben die ausdrückliche Einbeziehung der Akten in den Geltungsbereich des Gesetzes, die Verbesserung der Rechtsposition des Bürgers auf Auskunft über die zu seiner Person gespeicherten Daten und die Pflicht der Behörden des Landes und der Kommunen, behördliche Datenschutzbeauftragte zu bestellen.

3. Datenschutz in Europa

3.1 Europäische Datenschutzrichtlinie

Seitens der Datenschutzbeauftragten wurde immer wieder darauf hingewiesen, daß es auch auf der Ebene der Europäischen Union (EU) eines handlungsfähigen und unabhängigen Datenschutzes bedarf; denn die Globalisierung der Informationstechnologien und ihre Verbindung mit Ton- und Bildübermittlung wird zu einer enormen Zunahme des grenzüberschreitenden Austauschs von personenbezogenen Daten führen. Die technische Möglichkeit solch immenser Datenflüsse indiziert aber keineswegs ihre rechtliche Zulässigkeit. So beschränken fast alle Mitgliedstaaten zum Schutz der Privatsphäre die Verarbeitung, also die Erhebung, Speicherung, Nutzung und Übermittlung personenbezogener Daten. Die Unterschiedlichkeit dieser Regelungen in den einzelnen Mitgliedstaaten schafft potentielle Hindernisse für den grenzüberschreitenden Verkehr personenbezogener Daten in der Europäischen Union. Die Mitgliedstaaten haben auch unterschiedliche bereichsspezifische Regeln entwickelt, denen eine entsprechend differenzierte Rechtsprechung korrespondiert. In allen Fällen, in denen unterschiedliche inländische Regeln über den Datenschutz Geltung beanspruchen, rückt der inländische Verbotsanspruch den grenzüberschreitenden Datenverkehr in eine Grauzone der Rechtsunsicherheit, die seine Entwicklung und Akzeptanz behindert. In Deutschland hat das Bundesverfassungsgericht die grundrechtliche Verankerung des Rechts auf informationelle Selbstbestimmung im Volkszählungsurteil ausdrücklich anerkannt. Hinzu kommt, daß die Akzeptanz der Möglichkeiten der „Informationsautobahn" und der neuen Dienste, die sie transportiert, mit davon abhängen wird, ob es gelingt, gleichzeitig ausreichende Garantien für die Privatheit des einzelnen vorzusehen. Mithin war die Harmonisierung der Vorschriften zum Datenschutz notwendig, um die Grundlage für eine europäische „Datenverkehrsordnung" zu schaffen.

Der Rat der Europäischen Union hat am 24. Juli 1995 die Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Warenverkehr erlassen. Damit beginnt nach deren Artikel 32 Abs. 1 die Dreijahresfrist zu laufen, innerhalb derer die Mitgliedstaaten der Europäischen Union die erforderlichen richtlinienkonformen Rechts- und Verwaltungsvorschriften zu erlassen haben. Mit der Richtlinie ist das Fundament eines notwendigen Mindeststandards im Bereich des Datenschutzes gelegt worden.

3.1.1 Die Säulen der Europäischen Union

Für das Verständnis des Regelungsgehalts der Richtlinie ist es wichtig, sich die „drei Säulen" als Grundlage der Europäischen Union nach dem Vertragswerk von Maastricht vor Augen zu führen:

- der frühere EWG-Vertrag (jetzt: EG-Vertrag) mitsamt seiner Erweiterung um die Wirtschafts- und Währungsunion (WWU) und weitere Materien, z. B. Sozialpolitik, Kultur, Gesundheitswesen, transeuropäische Netze, Umweltschutz, Forschung und technologische Entwicklung (erste Säule);

- die künftige gemeinsame Außen- und Sicherheitspolitik (GASP) der Union, die sich an einem im Vertrag festgelegten Zielbündel orientiert und gemeinsame Aktionen ermöglichen und verfolgen soll (zweite Säule);
- die Zusammenarbeit in der Innen- und Rechtspolitik, die eine Reihe von Materien, u. a. Asylpolitik, Einwanderungspolitik und polizeiliche Zusammenarbeit bei Drogen- und Terrorismusbekämpfung umfaßt (dritte Säule).

3.1.1.1 Gemeinschaftsrecht

Die erste Säule unterscheidet sich von den anderen beiden dadurch, daß die Mitgliedstaaten in den einschlägigen Bereichen Hoheitsrechte an die Gemeinschaft übertragen haben. Zentrale Aufgabe der Gemeinschaft ist hier die Schaffung eines Binnenmarktes zwischen den Mitgliedstaaten. In diesem Zusammenhang wurden die vier Grundfreiheiten eingeführt: nämlich der freie Warenverkehr, der freie Personenverkehr, der freie Dienstleistungsverkehr und der freie Kapitalverkehr. Die Gemeinschaft wird tätig, soweit es erforderlich ist, um Hemmnisse abzubauen, die diesen Freiheiten entgegenstehen. Hinzu kommt, daß bereits seit Inkrafttreten des EWGV in vier Bereichen eine gemeinsame Politik vorgesehen wurde: so in der Verkehrspolitik, der Agrarpolitik, der Handelspolitik und der Wettbewerbspolitik. In diesen Bereichen ist die Zuständigkeit der Mitgliedstaaten auf die Gemeinschaft übertragen worden. Später wurden weitere Politikbereiche aufgenommen, wobei die Mitgliedstaaten allerdings der Gemeinschaft nur begrenzte Kompetenzen zugewiesen haben. Ihre Ausübung unterliegt dem Prinzip der Subsidiarität, das in Artikel 3 b EG-Vertrag (EGV) verankert ist. Danach wird die Gemeinschaft in den Bereichen, die nicht in ihre ausschließliche Zuständigkeit fallen, nur tätig, sofern und soweit die Ziele der in Betracht gezogenen Maßnahmen auf der Ebene der Mitgliedstaaten nicht ausreichend erreicht werden können und daher wegen ihres Umfangs oder ihrer Wirkungen besser auf Gemeinschaftsebene angestrebt werden. Hierzu gehören insbesondere das Gesundheitswesen, die Sozialpolitik, die Kulturpolitik, die Forschung und die Entwicklungspolitik.

Der Datenschutz bildet keinen eigenen Politikbereich. Maßnahmen der Gemeinschaft im Bereich des Datenschutzes stützen sich auf die Auffangnorm des Artikel 100 a EGV im Hinblick auf die Verwirklichung des Binnenmarktes oder stehen im Zusammenhang mit den Gemeinschaftspolitiken.

3.1.1.2 Die anderen Bereiche

Nicht unter das Gemeinschaftsrecht fallen die Bereiche der zweiten und dritten Säule. Folgerichtig ausgeschlossen wurde daher in Artikel 3 Abs. 2, erster Spiegelstrich, die Verarbeitung personenbezogener Daten im Zusammenhang mit Tätigkeiten, die nicht in den Anwendungsbereich des Gemeinschaftsrechts einzuordnen sind. Hierzu zählen die Tätigkeiten, die in den Titeln V und VI des Vertrages über die Europäische Union genannt sind. Diese Titel gehören nicht zum Gemeinschaftsrecht, sondern dem „Unionsrecht" an und betreffen die Gemeinsame Außen- und Sicherheitspolitik (zweite Säule) sowie die Zusammenarbeit der Mitgliedstaaten in den Bereichen Inneres und Justiz (dritte Säule). Hier bleibt die Zusammenarbeit zwischen den Mitgliedstaaten intergouvernemental. Gerade dieser – ausgeschlossene – Bereich berührt vielfach Datenschutzbelange.

3.1.1.3 Künftige Probleme

Die Gefahr, daß der Datenschutz europaweit in den von der Richtlinie nicht erfaßten Bereichen zurückbleibt, ist nach Einschätzung des LfD durchaus vorhanden. Es darf für das Schutzniveau grundsätzlich jedoch nicht darauf ankommen, welche „Säule" betroffen ist; denn das informationelle Selbstbestimmungsrecht ist unteilbar. Datenschutz ist die klassische Querschnittsmaterie, die sämtliche Bereiche der modernen Informationsgesellschaft betrifft; er sollte sich grundsätzlich nicht an den „Säulen" orientieren.

3.1.2 Umsetzungsbedarf

Für den deutschen Datenschutz ergeben sich unterschiedliche Konsequenzen für die öffentliche Verwaltung und die Privatwirtschaft. Im öffentlichen Bereich sind bereits umfassende Regelungen vorhanden. Für den Bereich der Privatwirtschaft ergeben sich indessen eine Reihe von Verschärfungen. So gilt die Richtlinie beispielsweise nicht nur für elektronisch gespeicherte Daten. Auch strukturierte Karteikartensammlungen mit personenbezogenen Daten fallen in ihren Anwendungsbereich. Das BDSG greift hier bislang nur, wenn die Informationen zur Übermittlung an Dritte bestimmt sind. Die neue Regelung wird zu einem wesentlich erhöhten Verwaltungsaufwand führen. Alle datenschutzrechtlichen Pflichten müssen künftig für solche Sammlungen beachtet werden.

Nachfolgend werden einzelne Regelungen angesprochen, die aus der Sicht des LfD für das Datenschutzrecht im öffentlichen Bereich bedeutsam sind:

3.1.2.1 Sensible Daten

In Artikel 8 wird die „Verarbeitung besonderer Kategorien personenbezogener Daten" geregelt. Besonders sensible Daten, etwa über religiöse oder philosophische Überzeugungen, über rassische oder ethnische Herkunft, politische Meinungen,

Gewerkschaftszugehörigkeit sowie Gesundheit oder Sexualleben genießen einen besonderen, über das deutsche Datenschutzrecht hinausgehenden Schutz vor Nutzung oder Weitergabe. Auch die Vorschriften des LDSG bleiben dahinter zurück. Bei der Umsetzung wird zu berücksichtigen sein, daß Artikel 8 aber auch eine Reihe von Ausnahmen vorsieht. Insbesondere zu nennen sind hier die Möglichkeit der Einwilligung der betroffenen Personen sowie die Verarbeitung personenbezogener Daten im Gesundheitswesen und auf dem Gebiet des Arbeitsrechts.

Fernerhin können gem. Artikel 8 Abs. 4 vorbehaltlich angemessener Schutzbestimmungen aus Gründen eines wichtigen öffentlichen Interesses weitere Ausnahmen vorgesehen werden. Den Erwägungsgründen der Richtlinie ist zu entnehmen, daß in diesen Bereich z. B. die Datenverarbeitung in der wissenschaftlichen Forschung, der öffentlichen Statistik sowie auf dem Gebiet der sozialen Sicherheit fällt.

3.1.2.2 Verarbeitung personenbezogener Daten durch die Medien

Nach Artikel 9 sehen die Mitgliedstaaten für die Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, Abweichungen und Ausnahmen von den Kapiteln II (allgemeine Rechtmäßigkeitsvoraussetzungen), IV (Drittlandtransfer) und VI (Kontrollstellen) nur insofern vor, als sich dies als notwendig erweist, um das Recht auf Privatsphäre mit den für die Meinungsäußerungsfreiheit geltenden Vorschriften in Einklang zu bringen. Es obliegt deshalb den Mitgliedstaaten, in Abwägung zwischen den Grundrechten Ausnahmen und Einschränkungen festzulegen, die beispielsweise bezüglich der Datenübermittlung in Drittländer oder hinsichtlich der Zuständigkeit der Kontrollstelle erforderlich sind. Mithin könnte für den Bereich der privatrechtlich organisierten Medien eine Selbstkontrolle der Datenverarbeitung durch interne Datenschutzbeauftragte eingeführt werden, z. B. im Wege einer Änderung der entsprechenden Bestimmungen des Landesrundfunkgesetzes (LRG). In § 42 BDSG ist dies übrigens für den öffentlich-rechtlichen Rundfunk des Bundes bereits vorgesehen. Danach bestellen die Rundfunkanstalten des Bundesrechts jeweils einen Beauftragten für den Datenschutz, der an die Stelle des Bundesbeauftragten für den Datenschutz tritt.

3.1.2.3 Widerspruchsrecht

Gemäß Artikel 14 werden die Mitgliedstaaten ein Widerspruchsrecht der betroffenen Person einführen, auch für den Fall einer rechtmäßigen Datenverarbeitung, jedoch unter anderem mit der Maßgabe, daß besondere Umstände vorliegen müssen und das schutzwürdige Interesse der betroffenen Person im Verhältnis zu dem des Verantwortlichen der Verarbeitung überwiegt. Umsetzungsbedarf ist dann vorhanden, wenn in besonderen Situationen neben dem Recht der betroffenen Person, z. B. auf Auskunft, ein zusätzliches Widerspruchsrecht für erforderlich gehalten werden kann. Eine solche Vorgehensweise ist dem deutschen Recht nicht fremd. Hinzuweisen ist in diesem Zusammenhang auf die Regelungen in § 7 Nr. 5 Melderechtsrahmengesetz, § 76 Abs. 2 Nr. 1 SGB X und § 3 Abs. 2 Krebsregistergesetz.

3.1.2.4 Verbot automatisierter Persönlichkeitsbewertung

Artikel 15 ist einer Vorschrift aus dem französischen Datenschutzrecht nachgebildet, wonach automatisierte Einzelentscheidungen einer Beschränkung unterliegen, wenn sie nachteilig für den Betroffenen sind. Hier könnte Umsetzungsbedarf für den Schulbereich vorhanden sein, daß beispielsweise Regelungen getroffen werden für die Arbeit mit „Lehrer-PC" im Hinblick auf Textbausteine als wiederkehrende Formulierungen bei Zensuren. Mit der Regelung in Artikel 15 soll verhindert werden, daß Entscheidungen aufgrund von Persönlichkeitsprofilen getroffen werden, ohne daß eine Person den Sachverhalt erneut überprüft hat. Eine Parallele findet sich auch bereits im deutschen Recht in § 90 g Abs. 4 Bundesbeamtengesetz (BBG), wonach beamtenrechtliche Entscheidungen nicht ausschließlich auf Informationen und Erkenntnisse gestützt werden dürfen, die unmittelbar durch automatisierte Verarbeitung personenbezogener Daten gewonnen werden.

3.1.2.5 Pflicht zur Meldung bei der Kontrollstelle

Nach Artikel 18 können die Mitgliedstaaten von umfassenden Meldepflichten absehen, wenn sie statt dessen zur wirksamen Vorabkontrolle die Einrichtung eines Datenschutzbeauftragten gewährleisten. Die Option für den behördlichen Datenschutzbeauftragten (vgl. § 11 LDSG) bietet somit die Alternative zu umfassenden Meldepflichten (vgl. § 27 LDSG).

3.1.2.6 Grenzüberschreitende Datenübermittlung

Aufgrund der in Artikel 25 und 26 vorhandenen Regelungen im Hinblick auf die Übermittlung personenbezogener Daten in Drittländer ist Umsetzungsbedarf bei § 17 LDSG vorhanden. Was die Datenübermittlung an ausländische sowie an über- und zwischenstaatliche Stellen anbelangt, ist nunmehr zwischen den Stellen im EU-Ausland, also den Staaten der Europäischen Union, und jenen in Drittstaaten zu unterscheiden. Soweit Gemeinschaftsrecht betroffen ist, sind innerhalb der EU künftig datenschutzrechtliche Schranken zwischen den Mitgliedstaaten überflüssig, weil von einem einheitlich hohen Schutzniveau ausgegangen wird. Für Datenübertragungen in Staaten außerhalb der Europäischen Union sieht die Richtlinie dagegen ein grundsätzliches Verbot vor, wenn beim Empfänger für den konkreten Fall kein angemessenes Schutzniveau vorliegt, wobei auch zahlreiche Ausnahmen vorgesehen sind.

In Artikel 25 ist das Verfahren festgelegt, das eine bestimmte Haltung der Mitgliedstaaten herbeiführen soll. Die Mitgliedstaaten und die Kommission konsultieren sich untereinander, wenn Zweifel an der Angemessenheit des Schutzniveaus in einem Drittstaat bestehen. Es ist vorgesehen, daß ein Ausschuß, der sich aus Vertretern der Regierungen zusammensetzt, aufgrund bestimmter Vorgaben (wie sie in Artikel 25 Abs. 2 niedergelegt sind) klärt, ob das Schutzniveau ausreichend ist. Das Ausschußverfahren ist in Artikel 25 Abs. 4 geregelt. Wenn das Schutzniveau nicht ausreichend ist, sorgen die Mitgliedstaaten dafür, daß keine Übermittlung personenbezogener Daten in dieses Land erfolgt, wobei die Kommission im Wege von Verhandlungen versuchen kann, zwischen der Gemeinschaft und den betreffenden Drittländern auf dem Verhandlungswege Abhilfe zu schaffen.

3.1.2.7 Struktur der Kontrollstelle

Artikel 28 bestimmt, daß die Mitgliedstaaten eine oder mehrere Kontrollstellen einrichten müssen, welche die ihnen zugewiesenen Datenschutzaufgaben in völliger Unabhängigkeit wahrnehmen. Vorgesehen sind eine Anhörungspflicht bei der Ausarbeitung von datenschutzrelevanten Verwaltungsmaßnahmen und -vorschriften, Informationsbeschaffungsbefugnisse und mehrere Alternativen von Einwirkungsbefugnissen. Zwischen Schutz des subjektiven Rechts auf informationelle Selbstbestimmung und Datenschutz im privaten Sektor wird nicht unterschieden. Artikel 28 läßt Raum für die Einrichtung völlig unabhängiger Kontrollstellen gegenüber der staatlichen Exekutive und der parlamentarischen Kontrolle unterliegenden Aufsichtsbehörden neben internen Datenschutzbeauftragten für den nichtöffentlichen Sektor.

Keine Konsequenzen sind daraus zu ziehen, daß die Richtlinie nicht zwischen öffentlichem und privatem Bereich unterscheidet. Grundsätzlich ist aber festzustellen, daß die Richtlinie generell eine stärkere Homogenisierung der Datenschutzanforderungen in beiden Bereichen anstrebt. Eine Zusammenlegung öffentlicher und privater Aufsichts- und Kontrollstellen wird von der Richtlinie aber nicht gefordert.

Gleichwohl ist gegenwärtig eine Diskussion im Gange, ob es nicht besser wäre, die Datenschutzkontrolle im privaten Sektor bei den Landesbeauftragten für den Datenschutz anzusiedeln, wie es bereits in Bremen, Hamburg, Niedersachsen und seit dem 1. August 1995 auch in Berlin der Fall ist. Gegen eine „einheitliche" Datenschutzkontrolle hat der LfD u. a. in einem Beitrag für die Zeitschrift DuD (Heft 8/95, S. 446 f.) Bedenken erhoben. Dort weist er darauf hin, daß die „Stellung der Landesbeauftragten für den Datenschutz, soweit sie für die Kontrolle des Rechts auf informationelle Selbstbestimmung gegenüber dem Staate zuständig sind, wie die Kontrolle der Rechnungshöfe ausgestaltet ist, weil sie wie die Rechnungshöfe nur Kontroll-, aber keine Exekutivbefugnisse besitzen. Sie kontrollieren die Exekutive sowie Parlamente und Gerichte, soweit diese Verwaltungstätigkeit ausüben. Im Schema der verfassungsrechtlich gebotenen Gewaltenteilung sind sie bei keiner der drei Gewalten anzusiedeln, weil sie weder legeferieren, exekutieren noch judizieren, sondern kontrollieren. Ihre Unabhängigkeit auch gegenüber den Parlamenten ist nur deshalb zu rechtfertigen. Hätten sie Exekutivbefugnisse, müßten sie insoweit parlamentarisch verantwortlich und gerichtlich überprüfbar sein, was in den vier Ländern mit einheitlicher Datenschutzkontrolle auch hinsichtlich des privaten Sektors verfassungsrechtlich notwendig der Fall ist. Schutzgut der Datenschutzbeauftragten der Länder im öffentlichen Sektor ist das Menschenrecht auf informationelle Selbstbestimmung. Träger dieses Rechts sind nur natürliche Personen als Privatrechtssubjekte, nicht dagegen Amtsträger in Ausübung ihres Amtes, auch nicht Beliehene. Adressat ist der Staat, die öffentliche Hand, meist auch dann, wenn sie in privatrechtlichen Formen tätig wird, da sich der Staat bekanntlich nicht durch die Flucht in das Privatrecht der Grundrechtsbindung entziehen kann. Im nichtöffentlich-rechtlichen Sektor handelt es sich beim Datenschutz um Normen, deren Einhaltung zunächst von den Privatrechtssubjekten selbst durchgesetzt werden muß, denen aber eine staatliche Aufsicht – vergleichbar der staatlichen Rechtsaufsicht über den Rundfunk, der Kartell- oder Bankenaufsicht – zur Seite steht, um notfalls Mißstände zwangsweise abzustellen. Eine staatliche datenschutzrechtliche Totalkontrolle im privaten Sektor kommt jedenfalls nicht in Betracht, auch wenn das Persönlichkeitsrecht tatsächlich im privaten Bereich mehr gefährdet sein sollte als das Grundrecht im öffentlichen. Bei manchen anderen Grundrechten ist eine Gefährdung durch den Staat auch weniger offensichtlich, als es Gefahren aus dem gesellschaftlichen Raum sind. Eine Drittwirkung des Rechts auf informationelle Selbstbestimmung ist jedenfalls solange nicht zu begründen, solange sie nicht wie die Koalitionsfreiheit ausdrücklich verfassungsrechtlich vorgesehen ist. Deshalb wird auch in den vier Ländern mit einheitlicher Datenschutzkontrolle sehr wohl zwischen Grundrechtsschutz einerseits und Datenschutz im privaten Sektor andererseits unterschieden, auch wenn dieselben Amtsträger für beide Sektoren zuständig sind. Daß vor allem im technisch-organisatorischen Datenschutz dieselben Probleme sowohl im öffentlichen wie im nichtöffentlichen Sektor auftreten, spricht jedenfalls nicht für eine Vermischung und Verwischung von Grundrechtsschutz einerseits und Datenschutz im privatrechtlichen Sektor andererseits. Eine Kooperation der beteiligten Kontrollbehörden beim technisch-organisatorischen Datenschutz ist insoweit möglich und existiert im übrigen auch bereits. Einer noch besseren gegenseitigen Information steht nichts im Wege."

Diese Probleme hat der LfD am Ende der letzten Legislaturperiode des Europäischen Parlaments auch mit dem damaligen Berichterstatter der Richtlinie, Herrn Geoffrey Hoon, erörtert. Es hat sich herausgestellt, daß die anderen Mitgliedstaaten das deutsche System, insbesondere die Aufteilung der Kontrolle im öffentlichen Bereich nach Bundes- und Länderzuständigkeit sowie die davon getrennte Aufsicht im privaten Bereich, nur sehr schwer nachvollziehen können. Nach dem Treffen konnte jedoch der Eindruck mitgenommen werden, daß es wichtig war, auf dieser Ebene die Gründe für das deutsche Modell zu erläutern. Letztlich ist es der deutschen Seite ja auch gelungen, was den Status und die Befugnisse der Kontrollstelle anbelangt, entsprechend offene Formulierungen durchzusetzen, die den deutschen Forderungen Rechnung tragen.

Jedenfalls ist die im ursprünglichen Entwurf vorgesehene und im 14. Tätigkeitsbericht, Tz. 3, kritisierte Regelung obsolet, wonach für die Kontrollbehörde sowohl ein unabhängiger Status als auch die Verleihung exekutiver Befugnisse vorzusehen war. Danach kann das bewährte deutsche Beauftragtenmodell im öffentlichen Bereich fortgeführt werden; denn ein Umsetzungsbedarf in nationales Recht im Hinblick auf die Einrichtung und Befugnisse der Kontrollbehörde besteht nicht.

3.2 Sonstige Projekte und Aktionen auf EU-Ebene mit Bezug zur Datenschutzrichtlinie

Die Beratungen des geänderten Vorschlags der geplanten ISDN-Richtlinie (vgl. dazu auch Tz. 20.1) wurden aufgrund eines Beschlusses der Rats-Arbeitsgruppe Fernmeldewesen so lange vertagt, bis die Datenschutzrichtlinie endgültig angenommen ist.

Mit Nachdruck wird an der Richtlinie zum offenen Netzzugang (ONP-Richtlinie – Open Network Provision) gearbeitet. Die Grundsätze für den offenen Netzzugang sind insbesondere darauf ausgerichtet, die Öffnung von Netzen zu ermöglichen und die Zugangsbedingungen zu Telekommunikationsinfrastrukturen in allen Mitgliedstaaten der EU zu harmonisieren. Der offene Netzzugang ist folglich unmittelbar an den Aufbau eines transeuropäischen Dienstleistungsmarktes gebunden, indem er die Verbindung von Dienstleistungserbringern und traditionellen Betreibern in den einzelnen EU-Mitgliedstaaten nach gemeinsamen Prinzipien ermöglicht. Er stellt von daher eine der Stützen der europäischen Telekommunikationspolitik dar. Die diesbezüglichen Verhandlungen finden aber gleichsam auf der „Überholspur" statt, da die ONP-Richtlinie vielfach auf die ISDN-Richtlinie verweist, wobei die Beratungen dazu seit Juli 1994 nicht fortgeführt wurden bis zur endgültigen Annahme der Datenschutzrichtlinie.

Schließlich ist auf den sog. Bangemann-Bericht vom 26. Mai 1994 hinzuweisen, der für die Tagung des Europäischen Rates am 24. Juni 1994 in Korfu erstellt wurde. Er behandelt u. a. auch den Schutz der Privatsphäre in einem Europa auf dem Weg in die Informationsgesellschaft.

4. Meldewesen

4.1 Novellierung des Meldegesetzes

Nach der Änderung des Melderechtsrahmengesetzes durch Gesetz vom 11. März 1994 (BGBl. I S. 529) besteht für den Landesgesetzgeber die Verpflichtung, das Meldegesetz innerhalb einer Zweijahresfrist anzupassen. Ein im Ministerium des Innern und für Sport erarbeiteter Referentenentwurf wurde dem LfD zur Stellungnahme zugeleitet. Folgende beabsichtigte Änderungen sind besonders datenschutzrelevant:

- Mit der Erweiterung der Hotelmeldepflicht um eine Ausweispflicht für Ausländer wird eine Vorgabe des Schengener Durchführungsübereinkommens zur Schaffung von Ausgleichsmaßnahmen für den Abbau der Binnengrenzkontrollen umgesetzt.
- Die Nutzung der von den Krankenhäusern und ähnlichen Einrichtungen nach § 28 MG geführten Verzeichnisse wird auf solche Fälle beschränkt, in denen die Auskunftserteilung zur Abwehr einer erheblichen und gegenwärtigen Gefahr, zur Verfolgung von Straftaten oder zur Aufklärung des Schicksals von Vermißten und Unfallopfern im Einzelfall erforderlich ist. Das bisherige Einsichtsrecht der Polizei in die Verzeichnisse wird durch eine Pflicht zur Auskunftserteilung an die Polizei und an andere Behörden zur Erfüllung der vorgenannten Aufgaben ersetzt.
- Die rechtliche Möglichkeit zur Erteilung von Melderegisterauskünften an Parteien usw. für Wahlwerbezwecke wird auf die Ausländerbeiratswahlen ausgedehnt. Zugleich wird ein Widerspruchsrecht für die Betroffenen und eine Pflicht der Übermittlungsempfänger zur Löschung der Daten innerhalb eines Monats nach der Wahl eingeführt.

Auf Empfehlung des LfD soll ergänzend klargestellt werden, daß die Weitergabe von Meldedaten innerhalb der Verwaltungseinheit, der die Meldebehörde angehört, im automatisierten Verfahren nur beim Vorliegen der Voraussetzungen nach § 7 LDSG zulässig ist.

Das Ministerium des Innern und für Sport sagte ferner zu, daß das Bereithalten von Daten zum Abruf durch andere Meldebehörden, das unter dem Verordnungsvorbehalt des § 31 Abs. 5 MG steht, im Rahmen einer Änderung der Meldedaten-Übermittlungsverordnung geregelt wird.

4.2 Novellierung der Meldedaten-Übermittlungsverordnung (MeldDÜVO)

Im 14. Tätigkeitsbericht stellte der LfD unter Tz. 4.1 seine Initiativen im Zusammenhang mit der Novellierung der MeldDÜVO dar. Schwerpunkte waren die regelmäßige Datenübermittlung innerhalb der Verwaltungseinheit, der die Meldebehörde angehört – hier forderte der LfD eine inhaltliche Beschränkung und die Verweisung auf die formalen Anforderungen des § 7 LDSG – und das Verfahren der regelmäßigen Datenübermittlung – hier wurde gefordert, die regelmäßige Datenübermittlung mit dem Ziel der Weiterverarbeitung unter einen ausdrücklichen Zulassungsvorbehalt zu stellen –.

Mit Bedauern mußte der LfD feststellen, daß diese wesentlichen Anliegen bei der Novellierung nicht berücksichtigt wurden; eine grundsätzliche Überarbeitung mit dem Ziel, in der Vergangenheit aufgetretene Streitpunkte auszuräumen, unterblieb. Der LfD wird diese Forderungen, soweit sie nicht durch die Änderungen des Meldegesetzes (vgl. Tz. 4.1) obsolet werden, bei einer Novellierung der Rechtsverordnung erneut zur Diskussion stellen.

4.3 Meldedatenübermittlung zum Zwecke der Einleitung von Ermittlungen durch das Finanzamt

Die Förderung des Wohneigentums ist nach § 10 e Abs. 6 a EStG nur noch in solchen Fällen möglich, in denen neuerbaute Wohnungen (Einfamilienhäuser, Wohnungen in Zwei- und Mehrfamilienhäusern) vor dem 1. Januar 1995 fertiggestellt wurden. Ein Finanzamt beabsichtigte, diesbezüglich Ermittlungen durchzuführen, und bat das Einwohnermeldeamt einer Verbandsgemeinde, die Anschriften von Bürgern mitzuteilen, die sich in dem Zeitraum vom 15. Dezember bis einschließlich 31. Dezember 1994 oder nach dem 31. Dezember 1994 mit Rückwirkung vor diesem Zeitpunkt an- oder umgemeldet haben und die eine neuerbaute Wohnung, deren Eigentümer sie sind, oder ein eigenes, neu errichtetes Einfamilienhaus bezogen haben könnten.

Der LfD wurde von der um Amtshilfe ersuchten Verbandsgemeinde um eine Stellungnahme gebeten.

Er ging in dieser Stellungnahme davon aus, daß die Amtshilfe von der Verbandsgemeinde grundsätzlich geleistet werden kann. Die Anschrift sowie der Tag des Ein- und Auszugs sind im Melderegister gespeichert, und die Verbandsgemeinde ist wohl auch in der Lage, Neubauten oder zumindest Neubaugebiete festzustellen und diese Feststellung einer Melderegisterrecherche zugrunde zu legen.

§ 31 Abs. 1 MG läßt die Übermittlung von Meldedaten an andere Behörden zu, wenn dies zur rechtmäßigen Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist. An dieser Voraussetzung fehlte es indessen, denn es war davon auszugehen, daß nicht nur solche Daten übermittelt werden, die für die Ermittlungen des Finanzamtes relevant sind, sondern, vermutlich in einem weitaus größeren Umfange, auch Daten von Einwohnern, die ihren steuerlichen Verpflichtungen ordnungsmäßig nachgekommen oder aus anderen Gründen nicht betroffen waren. Insoweit war eine Datenübermittlung aber nicht erforderlich.

Auch die Sonderregelung des § 31 Abs. 3 Nr. 5 steht unter dem Vorbehalt der Erforderlichkeit zur Aufgabenerfüllung; im übrigen privilegiert sie Finanzämter nur, soweit sie strafverfolgend tätig sind.

Eine auf den Einzelfall bezogene Prüfung der Erforderlichkeit einer Meldedatenübermittlung an Finanzämter entfällt nur beim Bereithalten von Daten zum Abruf nach § 11 MeldDÜVO. Eine derartige Datenübermittlung, die nach Schaffung der technischen Voraussetzungen selbstverständlich zulässig wäre, stand freilich nicht in Rede.

Der LfD hielt es für unbedenklich, einem Auskunftsersuchen des Finanzamtes zu entsprechen, wenn die Einwohner, auf die sich das Auskunftsersuchen bezieht, einzeln oder listenmäßig zusammengefaßt vom Finanzamt genannt werden.

Das Finanzamt erkannte die Rechtsauffassung des LfD an und reduzierte das Amtshilfeersuchen auf Einzel- oder Listenanfragen.

4.4 Meldedatenübermittlung an den Ausländerbeirat

Nach der Konstituierung der im Oktober 1994 gewählten Ausländerbeiräte fragten mehrere Städte und Gemeinden an, ob dem Wunsch um Übermittlung von Meldedaten an die Vorsitzenden entsprochen werden könne. Die Adreßdaten, Geburtsdaten und Angaben zur Nationalität sollten für konkrete Hilfs- und Beratungsangebote genutzt werden.

Der LfD wies darauf hin, daß es in entsprechender Anwendung von § 47 Abs. 1 Nr. 2 GemO die Aufgabe des Bürgermeisters ist, die Beschlüsse des Ausländerbeirats auszuführen. Im konkreten Fall bedeutet dies, daß die Adressierung von Sendungen mit Informationen und Hilfsangeboten durch die Verwaltung erfolgt. Hierfür können Meldedaten genutzt und im Rahmen des § 31 MG vom Meldeamt an die innerhalb der Verwaltung zuständige Stelle weitergegeben werden. Eine Weitergabe der Meldedaten an den Vorsitzenden des Ausländerbeirats kommt nicht in Betracht, weil diesem keine Aufgabe obliegt, zu deren Erfüllung die Datenübermittlung erforderlich ist (§ 31 Abs. 1 MG).

4.5 Meldedatenübermittlung an den Internationalen Suchdienst Arolsen (ISD)

Im 14. Tätigkeitsbericht, Tz. 4.5, berichtete der LfD über Probleme bei der Meldedatenübermittlung an den ISD, der sich im Rahmen seiner Aufgabenstellung um die Erlangung von personenbezogenen Unterlagen aus der Kriegszeit und unmittelbar danach bemüht.

Beim ISD handelt es sich um eine zwischenstaatliche Einrichtung und nicht um eine deutsche Behörde. Seine Aufgaben bestehen darin, personenbezogene Informationen über die Verfolgten während der nationalsozialistischen Herrschaft zu sammeln. Diese Informationssammlungen werden genutzt, um Auskünfte über Vermißte zu erteilen und Bestätigungen über Haft, Zwangsarbeit oder Verschleppung auszustellen. Die Bestätigungen werden von den Auskunftsberechtigten – ehemalige Verfolgte, ihren nächsten Familienangehörigen und Rechtsnachfolgern sowie von Organisationen und Wiedergutmachungsbehörden, die im Interesse der Verfolgten anfragen – benötigt, um Ansprüche auf Rente oder Entschädigung geltend machen zu können. Damit erfüllt der ISD eine von der Bundesrepublik Deutschland im Deutschlandvertrag aus dem Jahre 1955 übernommene völkerrechtliche Verpflichtung gegenüber den drei westlichen Siegermächten aus dem Zweiten Weltkrieg.

Eine Anwendung des § 33 MG auf Auskunftsersuchen des Internationalen Suchdienstes ist ausgeschlossen, denn diese Vorschrift regelt nur die Datenübermittlung an den Kirchlichen Suchdienst mit Sitz in München.

Es ist indessen davon auszugehen, daß sich Auskunftsersuchen des ISD in aller Regel auf Archivdaten beziehen. Dies ist dann der Fall, wenn Melderegisterkarten in kommunale Archive übernommen wurden. Der Zugriff auf diese Melderegisterkarten ist dann nach den Nutzungsbestimmungen des Landesarchivgesetzes zu beurteilen. Der LfD stimmte der Auffassung des Ministeriums des Innern und für Sport zu, daß keine datenschutzrechtlichen Bedenken zu erheben sind, wenn dem ISD auf Ersuchen Kopien von Karteikarten der Personen überlassen werden, auf die sich dessen Arbeit bezieht.

4.6 Auskunft trotz Sperrung von Meldedaten

Ein früherer Einwohner einer rheinland-pfälzischen Stadt war in eine norddeutsche Stadt umgezogen. Auf seinen Antrag wurden dort die Meldedaten gesperrt, weil Tatsachen die Annahme rechtfertigten, daß aus der Erteilung einer Melderegisterauskunft eine Gefahr für Leben und Gesundheit erwachsen könnte. Das früher in Rheinland-Pfalz zuständige Meldeamt wurde über die Auskunftssperre informiert, lehnte es aber ab, gleichfalls einen Sperrvermerk einzutragen, und übermittelte die aktuelle Anschrift auf Anfrage an eine Kreditauskunftei. Begründung: Die Voraussetzungen für die Eintragung einer Auskunftssperre hätten in der norddeutschen Stadt ebensowenig bestanden wie in Rheinland-Pfalz, wo ein entsprechender Antrag schon früher abgelehnt worden sei. Man fühle sich an eine andernorts getroffene Entscheidung, die zudem in der Sache fehlerhaft sei, nicht gebunden.

Diese Begründung ließ unberücksichtigt, daß Normadressat für die Vorschriften über die Erteilung von Melderegisterauskünften die „zuständige" Meldebehörde ist. Dies ist grundsätzlich die Meldebehörde, in deren Zuständigkeitsbereich der Betroffene seinen Wohnsitz hat. Lediglich für den Geltungsbereich des MG läßt Nummer 28.1 der Verwaltungsvorschrift des Ministeriums des Innern und für Sport vom 30. September 1988 zu, daß die für eine frühere Wohnung zuständige Meldebehörde auch die ihr bekanntgewordene aktuelle Anschrift mitteilen darf. Für Fälle, in denen eine Auskunftssperre nach § 34 Abs. 5 MG – wegen Gefahr für Leben, Gesundheit usw. – eingetragen ist, bestimmt die VV ausdrücklich, daß das Auskunftsersuchen an die zuständige Behörde weiterzuleiten ist. Der für eine frühere Wohnung zuständigen Meldebehörde steht es auch dann nicht zu, eine Melderegisterauskunft zu erteilen, wenn sie die von der zuständigen Meldebehörde verfügte Auskunftssperre für unberechtigt hält.

Die Meldedatenübermittlung an die Kreditauskunftei wurde nach § 25 Abs. 1 LDSG als Verstoß gegen melderechtliche Vorschriften beanstandet.

4.7 Namensverwechslungen

Nach wie vor kommt es bei der Erteilung von Melderegisterauskünften zu Namensverwechslungen. Diese bilden ein ernstes Problem sowohl für den Empfänger einer unrichtigen Auskunft, der Zeit und Kosten in unwirksame Maßnahmen investiert, wie auch in noch stärkerem Maße für die Betroffenen. In einem dem LfD durch eine Eingabe erneut bekannt wordenen Fall führte eine unrichtige Melderegisterauskunft zu einem Vollstreckungsversuch des Gerichtsvollziehers. Zu Recht wies der Betroffene darauf hin, daß sein guter Ruf als Geschäftsinhaber durch solche Maßnahmen Schaden nehmen könne.

Die Recherchen des LfD ergaben, daß das Meldeamt bei der Auskunftserteilung über alle Maßen leichtfertig gehandelt hatte. Da die anfragende Stelle – eine Bank – kein Geburtsdatum, sondern nur einen Vornamen und Nachnamen und den vermuteten Wohnort angegeben hatte, wurden auch nur diese Daten für die Melderegisterabfrage verwendet. Das Ergebnis war zunächst negativ, aber mit einem anderen als dem von der Bank angegebenen Vornamen fand sich eine Eintragung, die dann für die Melderegisterauskunft verwandt wurde. Diese Fehlleistung entspricht in ihrer Auswirkung anderen Verwechslungsfällen, über die im 11. Tätigkeitsbericht unter Tz. 6.1.2 und im 13. Tätigkeitsbericht unter Tz. 4.6 berichtet wurde. Es ist generell noch immer zu beklagen, daß die Meldebehörden das Geburtsdatum nicht in der gebotenen Weise bei der Melderegisterrecherche als Identifikationsmerkmal verwenden und die Melderegisterauskunft verweigern oder zumindest mit einem Vorbehalt versehen, wenn das Geburtsdatum von der anfragenden Stelle nicht benannt werden kann. Trotz fehlenden Geburtsdatums auch noch den Vornamen als Identifikationsmerkmal zu ignorieren, kann nur als grob fahrlässig bezeichnet werden.

4.8 Widerspruch gegen die Veröffentlichung von Ehejubiläumsdaten

Nach § 35 Abs. 3 MG darf eine Auskunft über Ehejubiläen von Einwohnern nur erteilt werden, wenn der Betroffene nicht widersprochen hat. Hierauf ist bei der Anmeldung sowie mindestens einmal jährlich durch öffentliche Bekanntmachung hinzuweisen.

Eine Prüfung der Bekanntmachungspraxis ergab, daß mehrere Verbandsgemeinden die gesetzlichen Bestimmungen besonders eng auslegten: Sie waren nur dann bereit, einen Widerspruch bei der Auskunftserteilung zu berücksichtigen, wenn das Widerspruchsrecht von den Ehegatten gemeinsam ausgeübt wurde. Fehlte eine Unterschrift auf dem Antrag auf Eintragung eines Widerspruchs in das Melderegister, so sahen sich die Meldebehörden nicht gehindert, die örtliche Presse über Ehejubiläen zu informieren.

Das Ministerium des Innern und für Sport stimmte der Rechtsauffassung des LfD zu, daß die Meldebehörden an einer Auskunftserteilung über Ehejubiläen auch dann gehindert sind, wenn nur ein Ehegatte widerspricht. Die Verbandsgemeinden wurden hierüber informiert.

5. Polizei

5.1 BND hört mit

Wer ein Auslandsgespräch führt und dabei Begriffe verwendet, die auch von Rauschgift- und illegalen Waffenhändlern sowie Geldwäschern als Tarnbezeichnungen gewählt werden, muß damit rechnen, daß der Gesprächsinhalt vom BND aufgezeichnet und daraufhin ausgewertet wird, ob sich z. B. hinter dem Ausdruck „Petersilie" ein reger Kokainhandel oder nur die Mitteilung des neuesten Kochrezeptes verbirgt. Ein unabhängiger Richter muß den Aufzeichnungen und Auswertungen nicht zugestimmt haben. Die Voraussetzungen sind mehr technischer Natur: Das Gespräch muß über eine Richtfunkstrecke oder über Satellit geschickt worden sein und der verfängliche Ausdruck muß sich als Suchbegriff auf einer Wortbank befinden, die der BND bei der Überwachung dieses Fernmeldeverkehrs verwendet. Da die Verbindungsdaten ebenfalls aufgezeichnet werden, sind alle Gesprächsteilnehmer jederzeit identifizierbar.

Nach Schätzungen des Bundesbeauftragten für den Datenschutz sind 99,9 v. H. der Abgehörten „nicht beschuldbar", meinen mit „Petersilie" also wirklich das Küchenkraut. Da sie nicht zu den vermutlich 0,1 v. H. gehören, deren Gesprächsinhalte an die Strafverfolgungsbehörden weitergeleitet werden sollen, erfahren sie fast nie, daß andere ihre vertraulichen Gespräche „ausgewertet" haben. Durch diese Unkenntnis wird der mit der Aufzeichnung und Auswertung des Telefonats verbundene Eingriff in das durch das Grundgesetz geschützte Fernmeldegeheimnis aber nicht geringer.

Die täglich in sehr hoher Zahl erfolgenden Eingriffe finden auf legaler Grundlage statt. Das Verbrechensbekämpfungsgesetz vom 28. Oktober 1994 sieht entsprechende Beschränkungen für eine Reihe von „Gefahrenbereichen" vor, zu denen die unbefugte Einfuhr nicht geringer Mengen von Rauschgift, im Ausland begangene Geldfälschungen und damit im Zusammenhang stehende Geldwäsche gehören. Für diese Beschränkungen darf der BND Suchbegriffe verwenden, die zur Aufklärung der genannten Sachverhalte geeignet erscheinen. Als wesentliche Abgrenzung zur klassischen Telefonüberwachung soll ein Verbot dienen, demzufolge die Suchbegriffe keine Identifizierungsmerkmale enthalten dürfen, die zu einer gezielten Erfassung bestimmter Fernmeldeanschlüsse im Inland führen (§ 3 des Gesetzes zu Artikel 10 Grundgesetz, geändert durch Artikel 13 Nr. 3 Verbrechensbekämpfungsgesetz).

Noch während des Gesetzgebungsverfahrens hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Beschluß vom 26./27. September 1994) Bedenken angemeldet und u. a. gefordert, daß geheimdienstliche Informationsmacht und polizeiliche Exekutivbefugnisse strikt getrennt werden müßten. Die durch das Trennungsgebot gezogene Linie dürfe nicht weiter verwischt werden.

Inzwischen liegt dem Bundesverfassungsgericht die Verfassungsbeschwerde eines Hochschullehrers aus Hamburg vor. Das Bundesverfassungsgericht wird zu entscheiden haben, ob der Bundesgesetzgeber von der Möglichkeit der Beschränkung des Fernmeldegeheimnisses unter angemessener Berücksichtigung des rechtsstaatlichen Grundsatzes der Verhältnismäßigkeit Gebrauch gemacht hat. Hier sind aus der Sicht des Datenschutzes erhebliche Zweifel angebracht.

Diese beginnen bereits bei der Geeignetheit der Maßnahme. Die „Zielgruppe" des Verbrechensbekämpfungsgesetzes besteht aus Personengruppen, die professionell und mit einem hohen Organisationsgrad operieren und nach aller Erfahrung Zugang zu den modernsten Techniken der Verschlüsselung ihrer fernmündlichen Kommunikation haben, die überdies aufgrund ihres bekannten Erfindungsreichtums andere Wege der Kommunikation nutzen und den Auswirkungen der Maßnahme im Zweifel ausweichen können. Demgegenüber wird eine neue Dimension der Fernmeldeüberwachung für alle Bürger eingeführt, bei der nach Art der Rasterfahndung ohne jeden Anfangsverdacht in großer Zahl Unbeteiligte in empfindlicher Weise in Abhörmaßnahmen einbezogen werden. Unverhältnismäßig sind sowohl diese Menge wie auch die Eingriffstiefe in jedem einzelnen Fall, die dadurch verschärft ist, daß die Betroffenen in aller Regel von dem Vorgang nichts erfahren.

Mit seinem zwischenzeitlichen Erlaß einer einstweiligen Anordnung (vom 5. Juli 1995, 1 BvR 2226/94, EuGRZ 95, 353) hat das Bundesverfassungsgericht zu erkennen gegeben, daß es den tatsächlichen Eingriffscharakter des Gesetzes außerordentlich hoch einschätzt.

5.2 Entwurf eines Gesetzes über das Bundeskriminalamt

Wenn nunmehr elf Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts der Entwurf eines Gesetzes über das Bundeskriminalamt vorgelegt wird, so ist dies zu begrüßen. Wie überfällig die Regelung ist, beweist die Entscheidung des Hessischen Verwaltungsgerichtshofes vom Juni dieses Jahres, die dem BKA für seine Dateien im Blick auf die zu schaffende gesetzliche Grundlage keine Übergangsfrist mehr zubilligt. Schon im Rahmen der Vorarbeiten für den jetzt vorliegenden Entwurf der Bundesregierung nahm der LfD Rheinland-Pfalz zu einem Teil der Grundtendenz wie auch zu verschiedenen Einzelregelungen kritisch Stellung.

So konnte zum Beispiel der Verzicht auf die im Vorentwurf vorgesehenen Befugnisse zur sog. „Feststellung eines Anfangsverdachtes" erreicht werden. Gleiches gilt für die Speicherung der Daten von Zeugen und Opfern anzunehmender künftiger Straftaten. Hier wurde deren Einwilligung als Voraussetzung einer Speicherung durchgesetzt.

Auch am jetzigen Entwurf bleibt die Grundtendenz zu kritisieren, die darauf abzielt, das Bundeskriminalamt zu einer den Länderpolizeien übergeordneten Ermittlungsbehörde mit eigenen Befugnissen zur Datenerhebung umzugestalten. Sollte damit de facto eine Art Bundeskriminalpolizei geschaffen werden, dann stellt sich die Frage, ob durch die Art und die Vielzahl der neuen Befugnisse der in Artikel 87 Absatz 1 des Grundgesetzes für das BKA eindeutig festgelegte Rahmen des polizeilichen Auskunfts- und Nachrichtenwesens überschritten wird. Auch Artikel 73 Nr. 10 GG läßt die Einrichtung einer eigenen Kriminalpolizei des Bundes nicht zu. Eine entgegenstehende Absicht müßte offen verfolgt werden. Voraussetzung hierfür wäre die Änderung des Grundgesetzes.

In diesen Zusammenhang gehört u. a. die vorgesehene Befugnis, „zur Ergänzung vorhandener Sachverhalte" bei den Polizeien des Bundes und der Länder Daten zu erheben und dies sogar bei anderen öffentlichen sowie nichtöffentlichen Stellen, soweit die inländischen Polizeien nicht über die Daten verfügen (§ 7 Abs. 2).

Mit der Konstruktion eines gemeinsam betriebenen föderalen Verbundsystems ist es nicht vereinbar, wenn die im Zentralrechner befindlichen, von den Ländern eingebrachten Daten weitgehend deren datenschutzrechtlicher Verantwortung entzogen werden (§§ 12, 32) und wenn obendrein das Kontrollrecht der Datenschutzbeauftragten der Länder auf ein bloßes Einsichtsrecht reduziert wird, das überhaupt nur in Zusammenarbeit mit dem Bundesbeauftragten für den Datenschutz ausgeübt werden kann. Hier konnte mit Hilfe der Landesregierung über den Bundesrat die Gegenposition im Sinne der Erhaltung des originären Kontrollrechts der Landesbeauftragten aufgebaut werden. Dies stimmt auch mit der Forderung des Datenschutzbeauftragten des Bundes und der Länder in ihrer Konferenzentschließung vom März 1995 (Anlage 18) überein.

5.3 Zusammenarbeit mit französischen Polizeibehörden

Am 3. Februar 1977 unterzeichneten die Innenminister der Regierung der Republik Frankreich und der Bundesregierung in Paris ein Abkommen über die Zusammenarbeit der beiderseitigen Polizeibehörden im Grenzbereich. In Ergänzung der über INTERPOL stattfindenden traditionellen Zusammenarbeit auf dem Gebiete der Kriminalpolizei wurden u. a. gegenseitige Unterstützung, Beratung sowie ein erweiterter Erfahrungs- und Nachrichtenaustausch vereinbart.

Hierzu wurden zur weiteren Konkretisierung am 12. Oktober 1992 zwischen dem Präfekten der Region Lothringen sowie den Innenministern von Baden-Württemberg, dem Saarland und von Rheinland-Pfalz 28 Punkte der polizeilichen Zusammenarbeit abgesprochen.

Soweit bei deren Realisierung insbesondere im Rahmen präventivpolizeilicher Zusammenarbeit personenbezogene Daten nach Frankreich und damit ins Ausland übermittelt werden, stellt sich im Sinne des Datenschutzes die Frage nach der Rechtsgrundlage. Die Absprache sieht in Punkt 11 vor: „Der Informationsaustausch erfolgt auf der Grundlage der gesetzlichen Bestimmungen."

Die Regelungen des Schengener Übereinkommens befassen sich nur mit einem Ausschnitt polizeilicher Tätigkeiten, wobei dort im Mittelpunkt des Interesses das Schengener Informationssystem (SIS) steht. Außerdem läßt das Schengener Durchführungsabkommen (SDÜ) in seinem Artikel 39 („Polizeiliche Zusammenarbeit") Absprachen der vorliegenden Art ausdrücklich unberührt. Soweit das SDÜ in diesem Zusammenhang überhaupt anzuwenden ist, läßt es ohnehin dem nationalen Recht weitgehend den Vorrang.

Eine rechtliche Übermittlungsgrundlage ist daher entsprechend dem präventiven Schwerpunkt der Absprache im Landesrecht zu suchen. Anders als in Baden-Württemberg und im Saarland enthält das POG Rheinland-Pfalz keine bereichsspezifische Regelung für die Übermittlung personenbezogener Daten durch die Polizei an ausländische öffentliche Stellen.

Bis zur Novellierung des POG ist daher das Landesdatenschutzgesetz anzuwenden (§§ 17 Abs. 2, 14 Abs.1 i. V. m. §§ 12 Abs. 4 Nr. 4 und 5 sowie 13 Abs. 2 Nr. 4). Dessen Regelungen gestatten im Grunde eine umfassende Zusammenarbeit bei Übermittlungen (zur Bekämpfung von Straftaten und Ordnungswidrigkeiten, zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbaren Gefahr für die öffentliche Sicherheit, zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person). Dabei wird „Bekämpfung von Straftaten" aufgrund der Gesetzgebungsgeschichte sowohl für präventive wie für repressive Maßnahmen verstanden.

Die Anwendung der genannten Regelungen auf das Abkommen und die Absprache sollte angesichts des weiten gesetzlichen Rahmens seitens des Ministeriums des Innern und für Sport unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit der Mittel konkretisiert werden. Insoweit finden Gespräche mit dem LfD statt. Wichtiger ist jedoch die möglichst rasche spezialgesetzliche Regelung. Hierzu ist darauf hinzuweisen, daß Nordrhein-Westfalen in sein Polizeigesetz eine ausdrücklich auf die Übermittlung im Rahmen polizeilicher Zusammenarbeit im Grenzgebiet bezogene Verordnungsermächtigung aufgenommen hat. Dies wäre auch in Rheinland-Pfalz geboten.

5.4 Novellierung des Polizei- und Ordnungsbehördengesetzes

Schon im 14. Tätigkeitsbericht wurde unter Tz. 5.13 auf die Notwendigkeit einer Neufassung der Informationsbestimmungen des Polizei- und Ordnungsbehördengesetzes hingewiesen, die bereits im Jahre 1986 in das PVG eingefügt wurden und die in der Systematik wie im Inhalt nicht mehr dem datenschutzrechtlichen Standard entsprechen, wie er in den übrigen Ländern zwischenzeitlich entwickelt wurde.

Insbesondere Befugnisnormen, die schwerwiegende Eingriffe in Grundrechte zulassen, müssen die Möglichkeiten und Grenzen polizeilichen Handelns zur Gefahrenabwehr sowohl für die Normanwender wie auch für die jeweils Betroffenen deutlicher erkennen lassen.

Außerdem hat die Praxis der vergangenen Jahre gezeigt, daß verschiedene im Interesse der Bürger notwendige Datenverarbeitungen in anderen Ländern normenklar geregelt sind, während sich ihre Zulässigkeit in Rheinland-Pfalz nur aufgrund z. T. komplizierter Auslegung ergibt. Die Folgen sind eine uneinheitliche Verwaltungspraxis und zeitlicher Mehraufwand. Schon im 14. Tätigkeitsbericht wurden in diesem Zusammenhang die Datenverarbeitungen zur Vorbereitung von Hilfeleistung und das Handeln in Gefahrenfällen (Tz. 5.13 Buchst. f), die Überprüfung der Zuverlässigkeit von Personen im Rahmen von Verwaltungsverfahren (a. a. O. Buchst. g) sowie die Übermittlung von Daten bei Suizidversuchen (a. a. O. Buchst. h) genannt.

Dabei ergeben die bei Kontrollen erkennbare Praxis wie auch weiterführende Überlegungen eine überwiegende Deckungsgleichheit der Ziele des Datenschutzes mit den berechtigten Forderungen der Polizeibeamten nach klaren und ihr rechtmäßiges Handeln zweifelsfrei absichernden Normen. Je mehr aufgrund der allgemeinen Entwicklung polizeiliches Eingriffshandeln gefordert ist und demzufolge auch im Einzelfall kritisch hinterfragt wird, um so mehr müssen die entsprechenden Rechtsgrundlagen zweifelsfrei und für jedermann erkennbar sein. Selbstverständlich darf die Regelungsdichte nicht die genannten Ziele wieder in Frage stellen.

Beispielhaft sind als weitere notwendige Regelungen zu nennen:

a) Die mit der französischen Regierung und den betroffenen Präfekten abgesprochene Grenzzusammenarbeit der Polizeien (siehe Tz. 5.3) bedarf der spezialgesetzlichen Regelung. Die jetzt praktizierte Ausrichtung an den Übermittlungsregelungen des LDSG an ausländische öffentliche Stellen bedarf im Einzelfall der eingrenzenden Anwendung.

b) Dringend erforderlich sind klare Regelungen für den Einsatz technischer Mittel zur verdeckten Datenerhebung sowohl im öffentlich zugänglichen Bereich als auch aus Wohnungen. Dabei ist eine klare Regelung unerläßlich, in welchen Fällen welche der zur Gefahrenabwehr gewonnenen Daten zu Zwecken der Strafverfolgung genutzt und weitergegeben werden dürfen. Gerade bei präventiven Datenerhebungen dieser Art im Bereich der organisierten Kriminalität dürften häufig neben den zur Gefahrenabwehr erforderlichen Erkenntnissen auch solche über begangene Straftaten anfallen (sog. Gemengelage). Hier darf es keine Unklarheiten zu Lasten der Beamten „vor Ort" geben. Schließlich kann der Umstand nicht außer acht bleiben, daß Artikel 13 GG in seiner jetzigen Form die heimliche Erhebung von Daten mit technischen Mitteln aus Wohnungen zu Zwecken der Strafverfolgung nicht zuläßt. Auf die Ausführungen im 14. Tätigkeitsbericht zum „Großen Lauscheingriff" (Tz. 5.5) ist in diesem Zusammenhang hinzuweisen. Eventuelle kompetenzrechtliche Einwände gegen den Standort einer entsprechenden Reglung im Polizeirecht des Landes sollten bis zu einer normenklaren Bundesregelung (StPO) nicht dazu dienen, den unsicheren und kaum durchschaubaren Rechtszustand auf diesem Gebiete andauern zu lassen.

c) Die Regelung für die Führung von Kriminalakten und die damit verbundenen Speicherungen sollte gesondert und ausdrücklich erfolgen und nicht wie im geltenden POG als „vorbeugende Straftatenbekämpfung" getarnt sein.

5.5 Hooligan-Listen an US-Behörden zur Fußball-WM?

Vor der Fußball-WM im Juni und Juli 1994 sind US-amerikanische Sicherheitsbehörden auf diplomatischem Wege an die zuständigen deutschen Stellen mit der Bitte herangetreten, ihnen zur Vorbereitung entsprechender Sicherungsmaßnahmen für die Fußball-WM personenbezogene Daten sog. „Fußballrowdys" zu übermitteln. Gewünscht wurden Informationen in standardisierter Form in der Gliederung nach vier verschiedenen Personenkategorien.

Den vom LfD dargelegten grundsätzlichen Bedenken hat sich das Ministerium des Innern und für Sport angeschlossen und einer pauschalen Übermittlung nicht zugestimmt. Mangels einer speziellen Rechtsgrundlage im POG oder in dem zu diesem Zeitpunkt noch geltenden alten LDatG wäre in Anlehnung an die Regelungen in den Polizeigesetzen einiger anderer Länder eine Übermittlung allenfalls in besonders gelagerten Einzelfällen in Frage gekommen. Hierzu wären konkrete Anhaltspunkte dafür erforderlich gewesen, daß bestimmte Personen die Weltmeisterschaft besuchen wollen, und zwar mit der Absicht, massiv zu stören.

Durch Verpflichtung der US-Stellen wäre die strikte Zweckbindung der Daten sowie deren unverzügliche Löschung nach der Weltmeisterschaft sicherzustellen gewesen. Darüber hinaus wurde zu erwägen gegeben, die Betroffenen über die Datenübermittlung in geeigneter Weise zu unterrichten, da sie ja immerhin gegebenenfalls erhebliche Kosten aufgewendet hätten und wegen der nicht bestehenden Visumpflicht erst an Ort und Stelle mit Schwierigkeiten bei der Einreise konfrontiert worden wären.

Soweit bekannt, wurden aus Rheinland-Pfalz in diesem Zusammenhang keine Daten übermittelt. In künftigen vergleichbaren Fällen könnte unter Berücksichtigung der näheren Umstände in ähnlicher Weise verfahren werden.

5.6 Örtliche Überprüfungen bei der Polizei

Örtliche Überprüfungen von Polizeistellen erfolgen entweder aus einem konkreten Anlaß oder um allgemeine Feststellungen über die Einhaltung von Vorschriften über den Datenschutz und über die Datensicherheit zu treffen. Dabei handelt es sich sowohl um Routinekontrollen als auch um gezielte Abklärungen bestimmter Bereiche, wie z. B. die Durchführung von Telefonüberwachungen nach § 100 a StPO.

Solche örtlichen Überprüfungen wurden in der Berichtszeit bei sieben Polizeiinspektionen, fünf Kriminalinspektionen, bei drei Polizei- und drei Kriminaldirektionen, beim Wasserschutzpolizeiamt und bei zwei Wasserschutzpolizeistationen sowie – z. T. mehrfach – bei zwei Polizeipräsidien und beim Landeskriminalamt durchgeführt.

Der dabei hergestellte Kontakt mit der „Polizeibasis" gibt auch die willkommene Gelegenheit zur Besprechung datenschutzrechtlicher Zweifelsfragen aus der örtlichen Praxis. Bei jeder Überprüfung erkundigen sich die Mitarbeiter des LfD nach derartigen aktuellen Problemstellungen. Dies fördert nach aller Erfahrung nicht nur die bei der Polizei des Landes ohnehin vorhandene starke Akzeptanz des Datenschutzes, sondern gibt auch die Möglichkeit, durch „Gegenkontrolle" festzustellen, wie sich einzelne datenschutzrechtliche Regelungen oder Maßnahmen vor Ort auswirken, also die Chance, Fehlentwicklungen gegebenenfalls zu korrigieren. Dabei kann auch immer häufiger festgestellt werden, daß datenschutzrechtliche Maßgaben in ihrer Wirkung mit den Bedürfnissen der polizeilichen Praxis übereinstimmen. So ist in aller Regel eine bereinigte Kriminalakte übersichtlicher; ihr für die Täterprognose wesentlicher Inhalt kann schneller erfaßt werden.

Folgende typische Kontrollgegenstände sind beispielhaft zu nennen:

- Die Überprüfung von Abfragen, insbesondere im allgemeinen polizeilichen Informationssystem POLIS, anhand von zuvor ausgewerteten Abfrageprotokollen des Landesrechenzentrums sowie anhand des jeweiligen Aktenrückhalts in den verschiedenen polizeilichen Vorgängen.
- Die Überprüfung der vorgeschriebenen automatischen und auch manuellen Zusatzprotokollierungen insbesondere bei solchen Geräten, von denen, wie aus Einsatzzentralen, häufig Abfragen für andere Bedienstete als den Gerätebediener selbst getätigt werden.
- Feststellungen zur Einhaltung von Rechtsvorschriften über den Datenschutz beim Betrieb und bei der Auswertung von Dateien nach den bestehenden Generalerrichtungsanordnungen „PHONE" (richterlich angeordnete Telefonüberwachungen) und „ERMITTLUNGSVERFAHREN" (auf Einzel-PC).

  Die Überprüfungen erfolgen anhand der beim LfD vorliegenden Kurzanmeldungen und sind insbesondere auf die Einhaltung der einschlägigen Bestimmungen der StPO bis hin zur gesetzmäßigen Vernichtung von zur Strafverfolgung nicht mehr erforderlichen Unterlagen gerichtet.
- Überprüfung von Spezialdateien, insbesondere im polizeilichen Dokumentationssystem „POLDOK", anhand der Vorgaben in den vorliegenden Errichtungsanordnungen.

– Feststellungen über die Rechtmäßigkeit von Speicherungen in den Sonderdateien des INPOL-Verbundsystems, wie z. B. den Arbeitsdateien PIOS und KAN-Bund (Landesbestand), mit Hilfe des vorhandenen Akteninhalts und anhand der kriminalpolizeilichen Meldedienste.

Gegenstand jeder allgemeinen Überprüfung ist die Führung der Kriminalpolizeilichen Sammlungen (KpS) oder „Kriminalakten". Hier geht es um den Stand der Aussonderung bei Altbeständen, den Inhalt im Blick auf die Täterprognose, den Umfang und die Dauer der Vorhaltung, aber auch um die Art der Verwahrung und die Zugangssicherung.

Weitere Prüfobjekte sind beispielsweise die Einhaltung von Lösch- und Prüffristen anhand der „Warnlisten" des LKA, die Haltung der Sicherheitsakten über Geheimschutzermächtigte, die Art der Aktenvernichtung, die Vorhaltung der Tonbandaufzeichnungen des Notrufes, Einsichtnahmen in das Paß- und Personalausweisregister wegen der dort vorhandenen Lichtbilder (Geschwindigkeitsüberschreitungen!), Inhalt und Weitergabe der Rapporte sowie Art und Dauer der Aufbewahrung der Durchschläge von Verkehrsunfallanzeigen.

Die Prüfergebnisse sind regelmäßig Gegenstand intensiver Erörterungen mit dem Ministerium des Innern und für Sport, wobei ebenso die von den Beamten vor Ort angesprochenen Fragen geklärt werden. Den Empfehlungen zur Verbesserung des Datenschutzes wurde dabei weitgehend entsprochen. Bei den aus der Prüftätigkeit folgenden Maßnamen wird der LfD regelmäßig bis zu deren endgültiger Realisierung beteiligt. So führten die örtlichen Feststellungen zu einer Reihe grundlegender Regelungen, wie bei der Behandlung der Zweitschriften in Ermittlungsverfahren, der Abschaffung von parallel geführten Handkarteien u. a.

Aus jüngster Zeit noch offen sind z. B. Maßnahmen zur Sicherstellung der Führung von Nachweisen über Einsichtnahmen in das Paß- und Personalausweisregister, die Behandlung von Mitteilungen über laufende Asylverfahren in den genannten Zweitschriften sowie die Möglichkeiten zur Überprüfung von Aktenrückhalten bei bestimmten POLIS-Abfragen, wenn die in Frage kommende Schicht am Prüftermin nicht anwesend ist und sich der Abfragegrund aus anderen Unterlagen nicht rekonstruieren läßt.

Hier geht es jedoch in erster Linie um die besten Realisierungsmöglichkeiten, nicht um im Grundsatz gegensätzliche Positionen.

Gravierende, insbesondere bewußte Verstöße gegen den Datenschutz wurden bei den Prüfungen insgesamt nicht festgestellt.

5.7 Drohbriefe nach unzulässiger Abfrage

Um dem Protest gegen eine geplante Sonderabfalldeponie Nachdruck zu verleihen, versandte ein Betroffener Drohbriefe an eine Reihe von Personen, darunter auch an ein Mitglied der Landesregierung. Die Adressen verschaffte er sich als Mitarbeiter eines Polizeipräsidiums durch unzulässige Abfragen im System EWOIS der Einwohnermeldebehörden, zu dem die Polizei über Online-Anschluß Zugang hat.

Der LfD wurde vom Ministerium des Innern und für Sport zu einem frühen Zeitpunkt über die Ermittlungen informiert und traf umgehend durch Bedienstete seiner Behörde sachliche Feststellungen vor Ort. Dabei bestätigte sich, daß in den in Frage kommenden Zeitabschnitten nicht nur eine unbestimmte Anzahl von Personen Zutritt zu den Diensträumen mit den benutzten Terminals hatte, sondern daß sich hier wieder einmal der Umstand auswirkte, daß die Abfrageprotokollierung bei EWOIS nur gerätebezogen, nicht aber auch an der Person des Nutzers orientiert ist. Auf diesen Umstand hatte der LfD bereits in mehreren Tätigkeitsberichten (12. Tb. Tz. 19.6, 13. Tb. Tz. 20.4 und 14. Tb. Tz. 21.5) hingewiesen. Nunmehr wird auf das massive Drängen und aufgrund der konkreten Empfehlungen des LfD eine entsprechende Regelung allgemein im Landesdaten- und Kommunikationsnetz realisiert.

Was den festgestellten unkontrollierten Zugang zu den Räumen mit aufgestellten Abfragegeräten betrifft, so wurde vom Ministerium des Innern und für Sport in Absprache mit dem LfD unmittelbar für Abhilfe gesorgt. In der in Vorbereitung befindlichen neuen Dienstanweisung der Polizei über den Datenschutz werden die entsprechenden Regelungen angemessen verdeutlicht.

5.8 Polizeiliche Datensammlung zur Kontakterleichterung

Zu Jahresbeginn 1994 wurde bekannt, daß ein Polizeipräsidium Daten über die in seinem Bereich amtierenden Bürgermeister und Beigeordneten mit Parteizugehörigkeit sammeln ließ, ebenso über die parteipolitische Zusammensetzung von Verbandsgemeinderäten. Die auf dieses Polizeipräsidium beschränkte Aktion sollte offensichtlich der allgemeinen Kontakterleichterung dienen. Gleichwohl war hierfür weder eine polizeirechtliche noch eine allgemein datenschutzrechtliche Rechtsgrundlage erkennbar. Soweit die Daten ohnehin aus offiziellen Handbüchern, also aus allgemein zugänglichen Quellen, hätten entnommen werden können, war die Eingriffstiefe gering und der ganze Vorgang überflüssig.

Der Minister des Innern und für Sport hat die Sammlung von Daten für den genannten Zweck sofort nach Bekanntwerden gestoppt.

5.9 Verkehrsunfallaufnahme-Richtlinie

Der überarbeitete Entwurf einer Neufassung des Rundschreibens des Ministeriums des Innern und für Sport „Aufgaben der Polizei bei Straßenverkehrsunfällen" (Verkehrsunfallaufnahme-Richtlinien) sieht u. a. die Benachrichtigung konsularischer Vertretungen bei Ausländerbeteiligung vor, wenn ausländische Staatsangehörige, die sich vorübergehend in Deutschland aufhalten, schwer verletzt oder getötet werden. Wenn Angehörige die erforderlichen Formalitäten veranlassen können, entfällt die Benachrichtigung.

Die Regelung geht im wesentlichen auf das Wiener Abkommen über konsularische Beziehungen von 1963 zurück.

Der LfD bat darum, in geeigneter Weise dafür Sorge zu tragen, daß bei verletzten Asylbewerbern und Flüchtlingen die Benachrichtigung dann unterbleibt, wenn Anhaltspunkte dafür vorliegen, daß dadurch schutzwürdige Belange der Ausländer beeinträchtigt werden könnten. Die Übernahme eines entsprechenden verbindlichen Hinweises in die Richtlinien ist inzwischen erfolgt.

Besonders begrüßt wird die nunmehr getroffene Regelung über die Unterrichtung der Straßenbaulastträger über Schadensverursacher bei Beschädigung von Gemeineigentum, wenn dies zur Geltendmachung von Ersatzansprüchen notwendig ist. Insbesondere wegen der Fälle, in denen noch nicht einmal ein Ordnungswidrigkeitenverfahren eingeleitet wird (sog. Kat. 5-Unfälle, vormals „A-Unfälle" oder „Bagatellunfälle"), sind die Vertreter des LfD bei örtlichen Feststellungen in Polizeidienststellen häufig auf den erhöhten Verwaltungsaufwand hingewiesen worden, der dadurch entstand, daß die Straßenbaulastträger zunächst nur auf die Tatsache der Schädigung, nicht aber auf den Schadensverursacher aufmerksam gemacht werden durften. Dies wurde nicht selten zu Unrecht dem Datenschutz angelastet.

5.10 Blutalkohol

Das Thema Blutalkoholuntersuchungen, schon in den beiden letzten Tätigkeitsberichten angesprochen (13. Tb. Tz. 5.6 und 14. Tb. Tz. 5.28), beschäftigt den Datenschutz noch immer. Die Aufmerksamkeit, die dieser Angelegenheit gewidmet werden muß, folgt aus der Vielzahl und der Sensibilität der im ärztlichen Untersuchungsbericht enthaltenen medizinischen Feststellungen u. a. über Medikamenten- und Drogeneinnahme, Krankheiten wie Diabetes, Epilepsie, Geisteskrankheit, frühere Schädelhirntraumata sowie Gewicht und Konstitution. Dabei ist zu berücksichtigen, daß die Erhebungen in aller Regel nicht mit Zustimmung der Betroffenen erfolgen.

Im Zusammenhang mit einer jetzt bundeseinheitlichen Verwaltungsvorschrift über die Feststellung von Alkohol im Blut bei Straftaten und Ordnungswidrigkeiten war u. a. zu entscheiden, wie die der Blutprobe beigefügten Unterlagen bei der Übersendung an die Untersuchungsstelle zu anonymisieren sind, denn diese braucht bei der Feststellung des Blutalkoholgehaltes nicht zu wissen, um wen es sich handelt.

Daß anonymisiert werden muß, ergibt sich aus der in Rheinland-Pfalz in Kraft gesetzten Version der Verwaltungsvorschrift (vom 6. Juli 1995 – JM 4103 – 4 – 132/95), wo es unter 3.5.2 u. a. heißt: „Sofern eine Ausfertigung der Untersuchungsstelle übersandt wird, ist sie in der Weise zu anonymisieren, daß zumindest Anschrift, Geburtstag und und Geburtsmonat nicht übermittelt werden."

Trotz mehrfach geäußerter Bedenken des LfD blieb das Ministerium der Justiz bei dem Standpunkt, trotz der Weitergabe des vollen Namens in Verbindung mit dem Alter (Geburtsjahr) bleibe der Betroffene für den Empfänger anonym. Die bessere Alternative, die die Verwendung einer unverwechselbaren Nummer in Verbindung mit dem Geburtsdatum vorsieht, wird unter Hinweis auf angeblich gehäuft auftretende ablauftechnische Probleme nicht akzeptiert, obwohl die Nennung der sachbearbeitenden Dienststelle der Polizei und der Entnahmezeitpunkt eigentlich keine Identifizierungsprobleme aufkommen lassen können.

Hier wird der leichteren Handhabung unter ungenügender Beachtung des Persönlichkeitsrechts der Betroffenen der Vorzug gegeben.

5.11 Übermittlungen von Informationen über Drogenkonsum an Führerscheinstellen

Am 24. Juni 1993 (DVBl. S. 995 ff.) hat das Bundesverfassungsgericht die Frage entschieden, unter welchen Voraussetzungen Haschischkonsum es rechtfertigen kann, ein medizinisch-psychologisches Gutachten über die Eignung zum Führen von Kraftfahrzeugen zu fordern. Nach den Gründen der Entscheidung rechtfertigt der einmalige Gebrauch von Cannabisprodukten eine solche Maßnahme nicht.

In Übereinstimmung mit dem Ministerium des Innern und für Sport vertrat der LfD die Auffassung, daß diese Feststellung nicht ohne Auswirkung darauf bleiben kann, unter welchen Voraussetzungen die Polizei Erkenntnisse über Drogenkonsum an die Führerscheinstellen weiterzugeben hat oder nicht.

Nach eingehender Erörterung mit dem LfD hat daher das Ministerium mit Rundschreiben vom 27. Juni 1994 an die Polizeibehörden im wesentlichen folgende Regelung getroffen:
Gewinnt die Polizei bei Maßnahmen der Gefahrenabwehr Erkenntnisse über Drogenkonsum einer Person, dann liegt die Übermittlung an die Führerscheinstelle grundsätzlich im Ermessen der Polizei. Eine Übermittlung kommt jedoch ebenso grundsätzlich dann in Betracht, wenn die betroffene Person harte Drogen konsumiert, Führerscheininhaber ist und die Möglichkeit des Zugriffs auf ein Kraftfahrzeug hat. Dann wird wohl in der Regel eine Gefahr anzunehmen sein. Für Konsumenten sog. „weicher Drogen" muß es auf die Würdigung des Einzelfalles ankommen. Eine Übermittlung gewonnener tatsächlicher Erkenntnisse wird je nach den näheren Umständen in Frage kommen, wenn der Betroffene diese Drogen zumindest gewohnheitsmäßig konsumiert oder davon abhängig ist.

Wurden hingegen die Erkenntnisse über jede Art des Drogenkonsums im Zuge strafrechtlicher Ermittlungen gewonnen, liegt die Entscheidung über deren Weitergabe an die Führerscheinstellen nicht mehr bei der Polizei, sondern bei den zuständigen Justizbehörden (siehe Nr. 4, 46 der bundeseinheitlich erlassenen Anordnung über Mitteilungen in Strafsachen – MiStra –). Dabei spielt es keine Rolle, ob die Straftat selbst einen Betäubungsmittelbezug hat oder ob die fraglichen Erkenntnisse „bei Gelegenheit" entstanden sind.

5.12 „Geisterautos" und „Schrottfrisierungen"

Auf Kraftfahrzeugkriminalität spezialisierte Straftäter kaufen in letzter Zeit zunehmend Schrottfahrzeuge auf, um den Kraftfahrzeugbrief zu erlangen. Dieser kann in zweifacher Weise „genutzt" werden: Es wird ein dem Unfallfahrzeug entsprechendes Auto gestohlen (sog. Doublette) und mit Hilfe der nummerntragenden Teile des Schrottfahrzeugs umfrisiert. Mit diesen technischen Daten, die mit denen des Kfz-Briefes jetzt übereinstimmen, wird das Fahrzeug als „gewaschen" weitgehend ohne Entdeckungsrisiko nutzbar (sog. Schrottfrisierung).

Die Alternative ist weniger aufwendig:
Der Kfz-Brief des Schrotts wird vorgelegt und ein Fahrzeug angemeldet, das nicht exisistiert (sog. Geisterauto); es wird nach der Zulassung als gestohlen gemeldet und mit der Versicherung betrügerisch abgerechnet.

Polizeilicherseits wird nun bundesweit überlegt, die Bekämpfung dieser Art von Straftaten, die offensichtlich der organisierten Kriminalität zuzuordnen sind, durch eine verbesserte Zusammenarbeit mit den Zulassungsstellen zu intensivieren. Vorgesehen sind Informationsübermittlungen an die Polizei bei der Wiederzulassung von Fahrzeugen mit technischem Totalschaden im Einzelfall, wenn es sich um jüngere Fahrzeuge mit verhältnismäßig hohem Anschaffungswert handelt. Liegen andere Anhaltspunkte auf Schrottfrisierungen vor, wäre die Polizei ebenfalls zu verständigen.

Auf eine Anfrage des Ministeriums des Innern und für Sport hat der LfD, vorbehaltlich der Kenntnis und Prüfung näherer Einzelheiten über den Umfang der Maßnahme und das anzuwendende Verfahren, im einzelnen grundsätzlich keine durchgreifenden Bedenken aus der Sicht des Datenschutzes erhoben.

Die in Frage kommenden Daten über die erste Zulassung und die Wiederzulassung, über den Hersteller und Typ des Fahrzeugs sowie über erhebliche Schäden müssen oder dürfen nach § 3 Abs. 1 und 2 der Fahrzeugregisterverordnung im örtlichen Fahrzeugregister gespeichert werden; ihre Übermittlung zur Verfolgung von Straftaten und zur Gefahrenabwehr wird in § 35 Abs. 1 des Straßenverkehrsgesetzes zugelassen, wenn es um die Bestimmung von Personen in ihrer Eigenschaft als Fahrzeughalter oder von Fahrzeugen eines Halters geht. Hierzu zählt auch die Feststellung, ob der Wiederanmelder auch Halter ist. Darunter muß ebenso die Feststellung fallen, ob ein vom „Halter" angemeldetes Fahrzeug überhaupt existiert.

Bei Anwendung der genannten Bestimmungen darf nicht übersehen werden, daß es dem Gesetzgeber bei ihrer Schaffung generell darum ging, daß die Daten der Register im erforderlichen Umfang auch zur Verfolgung von Straftaten zur Verfügung stehen. Das muß insbesondere für alle Straftaten gelten, die sich auf Kraftfahrzeuge beziehen.

Wenn die Übermittlungskriterien – wie es sich andeutet – entsprechend eng gezogen werden, wird man auch davon ausgehen können, daß in den genannten Fällen jeweils hinreichende tatsächliche Anhaltspunkte vorliegen, die einen Anfangsverdacht begründen und damit im Sinne der §§ 152 und 163 der StPO sowie § 12 LDSG die so informierte örtliche Polizei zur jeweiligen Nachprüfung berechtigen.

Jedenfalls steht im vorstehenden Zusammenhang auch für den LfD ein erhebliches und zwingendes öffentliches Interesse an der wirksamen Bekämpfung der hoch schadensintensiven Kfz-Kriminalität außer Zweifel.

5.13 Welchem Zweck dient das Kfz-Kennzeichen auf dem Verwarnungsblock?

Wird eine geringfügige Verkehrsordnungswidrigkeit durch eine wirksame gebührenpflichtige Verwarnung geahndet, so kann die Tat nicht mehr unter den gleichen tatsächlichen und rechtlichen Gesichtspunkten verfolgt werden; die Sache ist abgeschlossen.

Dem LfD wurde bekannt, daß bei einem Teil der Polizeibehörden Verwarnungsblöcke verwendet werden, auf deren Stammabschnitten das Kennzeichen des betreffenden Fahrzeugs festgehalten wird. Dies ist zur Aufgabenerfüllung der Polizei nicht erforderlich. Bei Nachfragen und Beschwerden seitens der Betroffenen ist eine Zuordnung problemlos durch Zusammenführen des Stamm- und des Quittungsabschnittes möglich.

Das Ministerium des Innern und für Sport stimmt mit dieser Beurteilung überein und hat die Praxis entsprechend geändert.

5.14 Keine Fahndung im Personalausweisregister nach Verwarnungssündern

Im 14. Tätigkeitsbericht wurde unter Tz. 5.16 auf die landesweite Praxis hingewiesen, die Lichtbilder in den Personalausweis- und Paßregistern zur Täteridentifizierung bei Verkehrsordnungswidrigkeiten im Regelfall nicht zu nutzen.

Im Oktober 1994 hat der „Bund-Länder-Fachausschuß für Straßenverkehrsordnungswidrigkeiten" einen Abgleich des Beweisfotos mit dem Paßbild im Personalausweis- oder Paßregister in allen Fällen gefordert. Auch bei geringsten zu ahndenden Geschwindigkeitsüberschreitungen (beisp. um zehn km/h), die nur mit einer gebührenpflichtigen Verwarnung belegt werden, hätte die Polizei bei der für den Wohnort des Betroffenen zuständigen Personalausweis- oder Paßbehörde bei Zweifeln an der Identität die Lichtbilder einsehen müssen.

Das Ministerium des Innern und für Sport sowie der LfD stimmen darin überein, daß dies zu weit geht. Man verständigte sich darauf, daß die genannte Methode der Identifizierung nur dann anzuwenden ist, wenn es sich um Verstöße handelt, die wegen ihrer Schwere in der „Verkehrssünderkartei" in Flensburg zu Eintragungen führen.

Damit wird einerseits den gestiegenen Anforderungen an die Verkehrssicherheit Rechnung getragen, andererseits aber auch die Gesetzeslage berücksichtigt. Sowohl im Paßgesetz als auch im Personalausweisregistergesetz sind Einsichtnahmen zu anderen als Registerzwecken nämlich eindeutig als Ausnahme konzipiert. Hier würden sie aber ansonsten zur Regel gemacht. Die regelmäßige Einsichtnahme auch bei bloßen Verwarnungstatbeständen wäre auch nicht verhältnismäßig. Dem durchaus massiven Eingriff stünden in der Praxis nämlich nur eingeschränkte Erfolgschancen gegenüber. Das Beweisbildmaterial ist oft nur bedingt brauchbar und die Paßbilder sind großteils veraltet. Im übrigen führt nur eine Identifizierung des Halters selbst zur Klärung der Sache. Ist tatsächlich eine andere Person gefahren, ist die Maßnahme von vornherein wirkungslos.

5.15 Geplante Änderungen beim polizeilichen Dokumentationssystem (POLDOK) und beim kriminalpolizeilichen Meldedienst (KPMD)

Die Eingabe in die verschiedenen einzelnen POLDOK-Dateien wird teilweise dezentral von den sachbearbeitenden Dienststellen, großteils aber auch zentral vom LKA aufgrund der eingegangenen KPMD-Meldungen durchgeführt. Dabei wird wegen der Spezialität der einzelnen POLDOK-Dateien nicht der gesamte Inhalt der KPMD-Meldungen elektronisch eingegeben und damit verwertet. Es ist nunmehr beabsichtigt, unter Auflösung eines Teiles der POLDOK-Einzeldateien, wie beispielsweise der Dateien über Tageswohnungseinbrüche (TWE) und Umweltdelikte, eine größere vereinheitlichte POLDOK-Datei als Falldatei zu schaffen, bei der die sachbearbeitenden Dienststellen ihre Daten jeweils dezentral eingeben. Dadurch entfallen insoweit der Meldedienst an das LKA und die dortige manuelle Auswertung. Der Aktenrückhalt besteht dann nicht mehr in Form der Meldungen beim LKA, sondern in Gestalt des vollen Ermittlungsvorganges bei der sachbearbeitenden Dienststelle. Dies stellt sich aus der Sicht des Datenschutzes als Fortschritt dar, denn der Aktenrückhalt bei der eingebenden Stelle ist dann umfassend.

Besondere Bedeutung für den Datenschutz gewinnt das Vorhaben aber durch die landesweite Abrufbarkeit der aus den betroffenen POLDOK-Dateien zusammengefaßten Datenbestände und ihre Recherchierfähigkeit. Neu ist auch die planmäßige Aufnahme von Umwelt-Ordnungswidrigkeiten. Damit könnte die Datenverarbeitung in einem Teil des POLDOK-Systems aus der Sicht des Datenschutzes eine andere Dimension gewinnen, die besondere Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung erforderlich macht. Der LfD ist vom Ministerium des Innern und für Sport frühzeitig unterrichtet und bei den Überlegungen zur Neugestaltung des Meldedienstes und der neu zu formulierenden Errichtungsanordnung hinzugezogen worden. Die entsprechenden Arbeiten sind noch nicht abgeschlossen. Schon zu Beginn hat der LfD verschiedene Erfordernisse aus der Sicht des Datenschutzes angesprochen. So ist in geeigneter Weise sicherzustellen, daß zu jedem Betroffenen im allgemeinen polizeilichen Informationssystem POLIS ein Hinweis enthalten ist, wenn zu ihm ein Bestand in der neuen POLDOK-Datei enthalten ist. Das soll gewährleisten, daß insbesondere bei Auskunftserteilungen und Löschungen den Rechten der Betroffenen in vollem Umfange entsprochen werden kann. Weiterhin sind die Personendatensätze in ihrem Umfang nach Art der Beteiligung der Betroffenen deutlich abzustufen. So müssen z. B. Geschädigte und Anzeigenerstatter nicht mit dem gleichen umfangreichen Datensatz gespeichert werden wie Beschuldigte und Verdächtige. Auch wird im weiteren Vorbereitungsverfahren zu prüfen sein, ob der Katalog der in Frage kommenden Straftaten im Blick auf die Erforderlichkeit landesweiter Recherchierbarkeit einzelner örtlich begrenzter Delikte überarbeitet und auf das Ziel der Datei zugeschnitten werden sollte.

Der LfD wird weiterhin seine Empfehlungen zu den einzelnen Überlegungen im Vorbereitungsverfahren einbringen.

An der Erforderlichkeit der Maßnahme insgesamt bestehen keine Zweifel. Die erhöhte Mobilität der Straftäter sowie ihr räumliches und zunehmend deliktsübergreifendes Handeln zwingen die Polizei zu Verfahren, die dieser Lage in angemessener Weise entsprechen.

5.16 In welchen polizeilichen Dateien können personenbezogene Daten gespeichert sein?

§ 25 f POG gewährt den Betroffenen gegenüber den allgemeinen Ordnungsbehörden und gegenüber der Polizei einen Anspruch auf Auskunft über die zu ihrer Person gespeicherten Informationen nach näherer Maßgabe. Bei der Bearbeitung von Eingaben muß oft festgestellt werden, daß einerseits den Betroffenen nicht alle Speichermöglichkeiten bekannt sind. Andererseits berücksichtigen und nutzen die Polizeibehörden bei der Auskunftserteilung nicht in jedem Falle alle vorhandenen Dateien einschließlich existierender Spezialdateien. Nicht selten beschränkt sich die Auskunft auf das allgemeine polizeiliche Informationssystem POLIS, dessen Abfrage auch in der Mehrzahl der Fälle ausreichend sein dürfte. Tatsächlich kann es aber sein, daß zwar eine POLIS-Abfrage negativ ist, gleichwohl aber Daten eines Betroffenen zum Beispiel im Vorgangsverwaltungssystem POLADIS gespeichert sind. Nicht alle Stellen der Polizei sind damit ausgerüstet. Wo dieses System aber installiert ist, kann es sein, daß Daten dort auch in aktuellen Vorgängen oder archiviert gespeichert sind, wenn nach der Bearbeitung eines Vorgangs die Voraussetzungen für eine Speicherung in POLIS nicht vorgelegen haben. Weiterhin kann es sein, daß für kurze Zeit die Daten eines Betroffenen im Einsatz-Leit- und Informationssystem ELIAS, das bei einigen größeren Stellen der Polizei in Betrieb ist, gespeichert sind. Dies ist insbesondere dann der Fall, wenn der Name des Betroffenen im Zusammenhang mit Maßnahmen erwähnt wurde, die über die jeweilige Funkzentrale bearbeitet wurden.

Eine Abfrage von INPOL ist nur vollständig, wenn sie vom LKA aus erfolgt. Speicherungen z. B. in den zur Unterstützung der Strafverfolgung und der Gefahrenabwehr in bestimmten Bereichen des Staatsschutzes entwickelten und bundesweit beim BKA geführten Dateien PIOS und APIS können nur vom LKA erkannt und abgefragt werden.

Zu bestimmten Tat- oder Gefahrenkomplexen werden von der Polizei des Landes Dateien im polizeilichen Spurendokumentationssystem POLDOK eingerichtet. Auch hier gibt es einzelne Dateien, die nur vom Landeskriminalamt abgefragt werden können.

Bei alledem sollten um Auskunft ersuchende Betroffene den Grund ihrer Anfrage möglichst umfassend darstellen, um schnelle und gezielte Recherchen zu ermöglichen. Für die die Auskunft erteilenden Stellen ist es geboten, anhand der ihnen bekannten Umstände möglichst umfassend abzufragen. Dabei ist daran zu erinnern, daß sich das Auskunftsrecht nicht nur auf in Dateien, sondern auch in Akten gespeicherte personenbezogene Daten erstreckt.

Ausgehend vom räumlichen Geltungsbereich des POG als Landesgesetz wendet sich ein Betroffener wegen vermuteter Speicherungen durch Behörden des Bundes oder anderer Länder dorthin. Dort befindet sich auch der entsprechende Aktenrückhalt.

5.17 Speicherungsdauer ausländerrechtlicher Verstöße in INPOL

Das Problem der Verhinderung illegaler Wiedereinreisen wurde in der Berichtsperiode bundesweit kontrovers diskutiert. Die Daten ausgewiesener oder abgeschobener Personen werden – soweit bekannt – allgemein zehn Jahre in der Personenfahndung des INPOL-Systems gespeichert. Gesetzliche Grundlage dieser Speicherungen sind die in den Polizeigesetzen enthaltenen Bestimmungen, wonach die Polizei personenbezogene Daten zur Erfüllung von Aufgaben speichern darf, die ihr durch andere Rechtsvorschriften übertragen sind (in Rheinland-Pfalz: § 25 a Abs. 1 Ziff. 4 i. V. m. § 1 Abs. 2 POG). Die hier zu erfüllende Aufgabe ist die der Polizei in § 63 Abs. 6 des Ausländergesetzes übertragene Festnahme und Zurückschiebung sich unerlaubt im Bundesgebiet aufhaltender Ausländer. Die Kenntnis bereits verfügter Ausweisungen und erfolgter Abschiebungen ist hierzu unerläßlich, weil diese Maßnahmen nach § 8 Abs. 2 AuslG ein Einreise- und Aufenthaltsverbot sozusagen „automatisch" nach sich ziehen. Soweit Speicherungen dieser Art im INPOL-System vorgenommen werden, erfolgt dies bundesweit in der Regel auf bis zu zehn Jahre. Damit bleiben mögliche Fristverkürzungen berücksichtigt, die sich dann ergeben können, wenn die Wiedereinreisesperren auf Antrag der ausländischen Person befristet werden.

Die Ersuchen für die Aufnahme der Daten in den INPOL-Fahndungsbestand werden von der jeweils zuständigen Ausländerbehörde gestellt, wo sich dementsprechend auch der Aktenrückhalt befindet. Die Prüf- und Löschfristen richten sich demzufolge primär nach Ausländerrecht, weniger nach den polizeirechtlichen Bestimmungen.

Die Notwendigkeit der Verfahrensweise wird mit den praktischen Erfahrungen mit sich illegal aufhaltenden Personen begründet. Der LfD hat frühzeitig in dieser Frage einen Meinungsaustausch mit dem Ministerium des Innern und für Sport begonnen, das zusagte, auf der Basis der Praxis nach Inbetriebnahme des Schengener Informationssystems und der Anwendung des neuen Ausländerzentralregistergesetzes, zu dem nunmehr die Durchführungsverordnung ergangen ist, die Erforderlichkeit der bestehenden Verfahrensweise zu überprüfen, wozu auch die Überprüfungs- und Löschungsfristen gehören.

Allerdings dürfte das Ausländerzentralregister als Ersatz für die Speicherung in der INPOL-Fahndungsdatei kaum in Betracht kommen, weil es systembedingt nicht die notwendige Aktualität aufweist und außerdem die Zugriffsmöglichkeiten eingeengt sind.

5.18 Auswertung von Fingerabdrücken auch im Ausländer- und Asylbestand des BKA

Im Automatischen Fingerabdruck-Identifizierungssystem (AFIS) des Bundeskriminalamtes werden jeweils getrennt auch Fingerabdrucksammlungen von Ausländern nach § 41 AuslG und von Asylbewerbern nach § 16 Abs. 1 AsylVerfG geführt. Für die Nutzung dieser Bestände auch zu polizeilichen Zwecken der Gefahrenabwehr und der Strafverfolgung gelten unterschiedliche Voraussetzungen. Während für den Bestand nach dem Ausländergesetz (§ 78 Abs. 3) die Fingerspurenauswertung zu den genannten Zwecken ohne weitere Einschränkung zulässig ist, fordert das Asylverfahrensgesetz (§ 16 Abs. 5) für die entsprechende Nutzung der im Asylbestand gespeicherten Abdrücke die durch bestimmte Tatsachen begründete Annahme, daß dies zur Aufklärung einer Straftat führen wird oder zur Abwendung einer erheblichen Gefahr erforderlich ist.

Die Abfrage im Wiesbadener AFIS-Bestand erfolgt durch das Landeskriminalamt. Dorthin wenden sich die sachbearbeitenden Polizeidienststellen, wenn sie eine Spur abgeglichen haben wollen.

Um insbesondere bei Rechercheersuchen im Bestand für Asylbewerber die Gründe für deren Nützlichkeit im Einzelfall nachprüfbar zu gestalten, hat das Ministerium des Innern und für Sport auf Anregung des LfD sichergestellt, daß diese jeweils in geeigneter Weise in Kurzform aktenkundig gemacht werden. Das LKA wird darüber hinaus zu Prüfzwecken die Untersuchungsanträge befristet aufbewahren.

6. Verfassungsschutz

6.1 Überprüfungen der Verfassungsschutzbehörde

Auch in dieser Berichtsperiode fanden mehrere systematische Überprüfungen der Verfassungsschutzbehörde des Landes statt. Überprüft wurden insbesondere Dateien und Akteninhalte sowie schwerpunktmäßig Datenflüsse innerhalb der Behörde und mit anderen Verfassungsschutzbehörden.

Dabei ergaben sich verschiedene Fragestellungen. Unter anderem geht es um den Umfang ereignisbezogener Mitteilungen an andere Landesverfassungsschutzbehörden. Sollen diesen auch Daten solcher Personen mitgeteilt werden, die keinerlei Bezug zu dem betreffenden Bundesland haben? Die Erforderlichkeit läßt sich nur nach den besonderen Umständen des Einzelfalles beurteilen. Hierzu zählen die Bedeutung des zu bearbeitenden Komplexes, die überregionale Bedeutung des Berichtsinhalts unter besonderer Berücksichtigung eines wahrscheinlich überregionalen Auftretens der Betroffenen. Nach Auffassung des LfD läßt sich die Erforderlichkeit der Übermittlung nicht ausschließlich nach dem „Territorialprinzip" beurteilen. Keineswegs wäre es zulässig, in Berichten an andere Verfassungsschutzbehörden ohne Prüfung der Erforderlichkeit die Daten aller beteiligten Betroffenen zu übermitteln.

Gegenstand grundsätzlicher Erörterung ist auch die Möglichkeit, daß in Dateien, die einer Volltextrecherche zugänglich sind, Personen vorkommen, über die kein eigener Datensatz existiert, weil ihre Daten nur im Kontext gespeichert wurden, ohne daß sie selbst Gegenstand der Beobachtung sind. Es kann sich z. B. um den Inhaber einer Gaststätte handeln, in der sich zu beobachtende Personen treffen, ohne daß ein einschlägiger Bezug zu ihm selbst besteht. Dem Ministerium des Innern und für Sport wurde empfohlen, beim Feststellen derartiger Speicherungen die Daten solcher „Drittpersonen" zu löschen, wenn keine Rechtsgrundlage für die Speicherung besteht. Gibt es einen materiellen Speicherungsgrund, wäre ein entsprechender Datensatz anzulegen. Bei Neueingaben ist streng nach diesem Grundsatz zu verfahren.

In älteren Sachakten befanden sich u. a. Hinweise über Familienangehörige von Betroffenen mit Wertungen wie „arbeitsscheu, asozial, Strafverurteilungen der Geschwister, Suizidversuche mit Tabletten" usw. Der LfD hat dies beanstandet und gefordert, daß auch aus anderen Sachakten bei jeweiliger Nutzung entsprechende Inhalte entfernt werden.

6.2 Sicherheitsüberprüfungen gesetzlich regeln

Aufgrund der zwischenzeitlich eingetretenen Veränderungen der europaweiten Sicherheitslage wurden die „Richtlinien für die Sicherheitsüberprüfung von Personen im Rahmen des Geheimschutzes" – Sicherheitsrichtlinien – überarbeitet und im Entwurf auch dem LfD zur Stellungnahme zugeleitet.

Zu begrüßen sind die deutlichen Verbesserungen gegenüber der bisherigen Praxis, die u. a. in verkürzten Aufbewahrungs- und Speicherfristen bestehen sowie in dem erkennbaren Bestreben, unter Berücksichtigung verschiedener Empfehlungen des LfD Anzahl und Umfang der Überprüfungen weiter zu reduzieren. Aufgrund der Stellungnahme des LfD wurden weitere Verbesserungen im Sinne des Datenschutzes aufgenommen.

Trotz dieser unbestreitbaren Fortschritte ist die teilweise einseitig gewichtete Grundtendenz, wie sie schon im Sicherheitsüberprüfungsgesetz des Bundes enthalten ist, fortgeführt. Dies wird beispielsweise deutlich beim Quellenschutz im Rahmen der Anhörung des Betroffenen. Gegen strafbare Äußerungen einer „Quelle" kann er praktisch nichts unternehmen.

Besonders gravierend ist es aber, daß die z. T. empfindlichen Eingriffe in das Recht auf informationelle Selbstbestimmung nur in Richtlinien getroffen werden. Die von der Verfassung her bestehende Notwendigkeit, derartige Regelungen in einem Gesetz zu treffen, ist unbestritten. Es darf hierzu auf die Rechtsprechung des Bundesverfassungsgerichts zur sog. „Wesentlichkeitstheorie" (BVerfGE 20, 150 ff.) hingewiesen werden, wie auch auf die einschlägige Fachliteratur.

Das Recht der Sicherheitsüberprüfung ist zwar in weiten Teilen von der Einwilligung der Betroffenen beherrscht, gleichwohl ermöglicht es unabhängig von deren Bewertung im Einzelfall prinzipiell schwere Grundrechtseingriffe, z. B. bei der Verkürzung des Auskunfts- und Einsichtsrechts des Betroffenen, wie auch bei den Erhebungsmethoden und bei der Verwendung der Daten.

Deshalb muß auch weiterhin die möglichst rasche Schaffung einer geeigneten Rechtsgrundlage durch ein Gesetz gefordert werden, wie es beim Bund und in Nordrhein-Westfalen bereits realisiert ist und in den eingebrachten Gesetzentwürfen mehrerer Landesregierungen angestrebt wird.

6.3 Novellierung des Verfassungsschutzgesetzes
– Richtervorbehalt für den „Großen Lauscheingriff" aus Wohnungen! –

Mit dem geltenden Landesverfassungsschutzgesetz reagierte Rheinland-Pfalz insoweit als erstes Land auf das Volkszählungsurteil des Bundesverfassungsgerichts von 1983. In der Zwischenzeit ist die Rechtsentwicklung gerade auf diesem Gebiete erheblich fortgeschritten. Das Bundesverfassungsschutzgesetz wie auch die Gesetze der anderen Bundesländer folgen einer anderen Systematik. Zum Beispiel werden die Bestimmungen über Aufgaben, Befugnisse und Datenverarbeitung deutlich getrennt und detaillierter gefaßt. Auch aus Gründen der Normenklarheit und Transparenz ist es nunmehr geboten, die Rechtslage in Rheinland-Pfalz anzupassen.

Als notwendige Regelungen sind darüber hinaus beispielhaft zu nennen: Bestimmungen über die vom Bundesverfassungsgericht im Volkszählungsurteil geforderte Zweckbindung der verarbeiteten Daten sowie einschränkende Regelungen hinsichtlich der Daten von Unbeteiligten, von sog. „Intimdaten" und von Daten unorganisierter Einzelpersonen.

Ein besonderer Schwerpunkt wird die an rechtsstaatlichen Erkenntnissen ausgerichtete Weiterentwicklung der Bestimmungen über die „besonderen Informationserhebungen" und über die Verwendung „nachrichtendienstlicher Mittel" unter rechtsstaatlichen Erfordernissen sein müssen.

Eine komplette und abschließende Aufzählung dieser technischen und methodischen Mittel erscheint zwar nicht realistisch, doch wird man von einer transparenten Regelung nur dann sprechen können, wenn wenigstens die wesentlichen zum Einsatz kommenden Mittel beispielhaft im Gesetz aufgeführt sind.

Strikt normenklarer Regelung bedarf das mit technischen Mitteln erfolgende heimliche Mithören oder Aufzeichnen des in einer Wohnung nichtöffentlich gesprochenen Wortes im Rahmen der Ermächtigung des Artikels 13 Abs. 3 GG. Der Schwere des Eingriffs müssen die näheren Bestimmungen über den Anwendungsbereich und die Voraussetzungen entsprechen. Dies muß auch für die Verwendung der hierbei und bei vergleichbar gravierenden Eingriffen gewonnenen Informationen zu anderen Zwecken gelten. Gerade in diesem Zusammenhang ist darauf hinzuweisen, daß Artikel 13 GG im Blick auf die verdeckte Informationsgewinnung aus Wohnungen keine Ermächtigung enthält, die auch Zwecke der Strafverfolgung umfaßt. Nur dessen Absatz 3 enthält die hier in Anspruch zu nehmende Ermächtigung für den weiteren präventiven Bereich. Die Verwendung dabei gewonnener Erkenntnisse zur Strafverfolgung ist insoweit vom Grundsatz her nicht bedenkenfrei. In speziell diesem Punkt ist eine absolut normenklare Regelung zu fordern, die sogar Verweisungen auf andere Gesetze ausschließt.

Nach Auffassung des LfD ist es aus rechtsstaatlichen Gründen unerläßlich, das Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes aus Wohnungen mit technischen Mitteln und in ihrer Schwere vergleichbare Eingriffe von der richterlichen Einzelfallentscheidung abhängig zu machen, wie das auch für die Polizei im präventiven Bereich vorgeschrieben ist. Für den Betroffenen stellt sich die Maßnahme nämlich in Art und Schwere gleich dar, ob sie nun aus Gründen der polizeilichen Gefahrenabwehr oder in Wahrnehmung von Aufgaben des Verfassungsschutzes erfolgt. Deshalb wäre es nicht einsehbar, wenn die formalen rechtsstaatlichen Voraussetzungen unterschiedlich sein sollten. Die richterliche Zustimmung ist in Deutschland und in den übrigen westlichen Demokratien traditionell und durchweg das klassische Mittel zur Vorkontrolle schwerwiegender staatlicher Eingriffe in Menschenrechte im konkreten Einzelfall. Dies findet in der Bevölkerung eine hohe Akzeptanz und erleichtert die Hinnahme der gesetzlichen Befugnis zu diesem Grundrechtseingriff.

6.4 NADIS – Identifizierungsmerkmale zur Aktenauffindung –

Nach § 6 des Bundesverfassungsschutzgesetzes müssen die Verfassungsschutzbehörden des Bundes und der Länder zur Erfüllung ihrer gegenseitigen gesetzlichen Unterrichtungspflicht beim Bundesamt für Verfassungsschutz gemeinsame automatisierte Dateien führen. In Erfüllung dieser Verpflichtung wird das Nachrichtendienstliche Informationssystem (NADIS) geführt. Nach Satz 2 der genannten Bestimmung enthalten diese Dateien nur die Daten, die zum Auffinden von Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind. Zum Auffinden von Akten müssen Personen dann identifiziert werden, wenn die üblichen Personaldaten wie Name, Geburtsdatum u. a. unbekannt sind. Dann müssen zusätzliche Merkmale weiterhelfen, um festzustellen, ob es zu einer bestimmten Person eine Akte gibt.

Nach einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom April 1994 darf eine Aktenauffindungsdatei nur die Daten enthalten, die für das Auffinden der Akten und für die dazu notwendige Identifizierung von Personen erforderlich sind. Darüber, was und vor allem wie viele zusätzliche typisierte Suchbegriffe hierfür erforderlich sind, gibt es unterschiedliche Auffassungen. Auswahl und Umfang müssen in dem genannten Sinne streng zweckorientiert sein und müssen dem Verfassungsgrundsatz der Verhältnismäßigkeit entsprechen. Mit dem Ministerium des Innern und für Sport ist der LfD der Auffassung, daß nicht mehr oder weniger uferlos geeignet erscheinende Identifikationsmerkmale verwendet werden können, daß man aber andererseits auch nicht eine zu enge Begrenzung etwa auf klassische Personaldatensätze oder Aufzählungen wie in § 111 des Ordnungswidrigkeitengesetzes (Falsche Namensangabe) vornehmen kann, ohne den gesetzlichen Zweck der Datei zu gefährden.

Schließlich liegt eine möglichst exakte Personenidentifizierung beim Aktenfinden im Sinne des Datenschutzes. Verwechslungen auf diesem Gebiet können nämlich für davon Betroffene zu einschneidenden Folgen führen.

6.5 Keine Auswertung von Wahlunterstützungslisten durch den Verfassungsschutz

In einem anderen Bundesland wurde durch die Intervention des dortigen LfD und nach massiver Pressekritik eine Praxis des Verfassungsschutzes abgestellt, Erkenntnisse aus Unterstützungslisten für eine Partei zur Europawahl auszuwerten und zu speichern.

Ein derartiges Verfahren wäre im Ergebnis auch nach Auffassung des LfD Rheinland-Pfalz wegen Verstoßes gegen den Grundsatz der Verhältnismäßigkeit rechtswidrig gewesen. Wegen der unbestreitbaren Nähe zum Wahlgeheimnis handelt es sich bei der Unterschriftsleistung um ein besonders sensitives Datum. Andererseits kann die Kenntnis dieses Umstandes für den Verfassungsschutz nur von zweitrangiger Bedeutung sein.

Eine Überprüfung beim Landesverfassungsschutz ergab, daß hier Wahlunterstützungslisten aufgrund einer internen Verfügung von 1979 nicht ausgewertet werden.

7. Justiz

7.1 Kompetenzkonflikte: MAJA – die Entwicklung von Justizautomation unter Ausschluß des LfD?

Der LfD hatte sich beim Amtsgericht Zweibrücken angemeldet, um dort örtliche Feststellungen im Zusammenhang mit dem Verfahren zur Automation der gerichtlichen Geschäftsstellen „MAJA" (Mainzer automatisierte Justizanwendungen) durchzuführen. Daraufhin wurden seitens des Ministeriums der Justiz Zweifel an seiner diesbezüglich bestehenden Kontrollkompetenz geäußert. Als Ergebnis einer deshalb anberaumten Besprechung wurde festgestellt, daß in dieser Frage im Grundsätzlichen zwar keine Übereinstimmung zu erzielen war, daß aber der Versuch unternommen werden sollte, auf der Basis von konkreten datenschutzrechtlichen Fragestellungen einen Kompromiß zu erzielen.

Der LfD hat zu diesem Zweck seine Position gegenüber dem Justizministerium schriftlich im Februar 1995 wie folgt konkretisiert:

Nach § 24 Abs. 2 LDSG beschränkt sich die Kontrollzuständigkeit des LfD im Bereich der Gerichte auf die „Verwaltungsangelegenheiten". Streitig ist, wie dieser Begriff auszulegen ist.

Einerseits wird die Auffassung vertreten, daß jede Tätigkeit der Gerichte, die nicht von der richterlichen Unabhängigkeit umfaßt ist, zu den Verwaltungsangelegenheiten im Sinne des LDSG gehöre.

Es gibt andererseits aber auch maßgebliche Meinungen, die nur die Tätigkeiten der Justiz den Verwaltungsangelegenheiten zuordnen, die nicht als Erfüllung der Aufgaben der rechtsprechenden Gewalt im Sinne der Artikel 92, 97 GG, §§ 4 Abs. 1, 25 Deutsches Richtergesetz qualifiziert werden können.

Bereits die DSK hat gegenüber dem Ministerium der Justiz folgende Auffassung formuliert: „Die Datenschutzkommission ist der Ansicht, daß durch § 24 Abs. 1 LDatG nur der Bereich der richterlichen Unabhängigkeit von ihrer Kontrollkompetenz ausgenommen ist. In dem Umfang, in dem dem Justizministerium Weisungsbefugnisse zustehen, stehen auch der Datenschutzkommission Kontrollbefugnisse zu, wenn die Verarbeitung personenbezogener Daten betroffen ist."

Diese Auffassung teilt der LfD grundsätzlich. In entsprechendem Sinn haben sich auch andere LfD geäußert. Nach Sinn und Zweck des Gesetzes ist von der Richtigkeit dieses Grundsatzes auszugehen. Für die identische Rechtslage in Hamburg hat die Justizbehörde der Freien und Hansestadt Hamburg diese Auffassung wie folgt bestätigt:

„Nach dem Gesetzeswortlaut sind die Gerichte der Datenschutzkontrolle entzogen, soweit sie nicht in Verwaltungsangelegenheiten tätig werden. Es sind daher aus dem Bereich der den Gerichten allgemein zugewiesenen Tätigkeiten diejenigen abzutrennen, die als Verwaltungsangelegenheiten zu bezeichnen sind. Einigkeit besteht zu der gesetzgeberischen Motivation dieser Regelung. Mit der Herausnahme der gerichtlichen Tätigkeiten aus der Datenschutzkontrolle soll die verfassungsrechtlich gewährleistete Unabhängigkeit der Rechtsprechung gesichert werden (statt vieler Dammann in Simitis/Dammann/Mallmann/Reh, BDSG/Kommentar, 3. Auflage 1981, § 19 RdNr. 7 und – besonders deutlich – § 7 RdNr. 55 ff.)."

Daraus folgt: Der Begriff der „Verwaltungsangelegenheiten" im LDSG betrifft nicht nur diejenigen Tätigkeiten der Gerichte, die keinen Bezug zu der in richterlicher Unabhängigkeit vorgenommenen Spruchtätigkeit haben. Zur Gerichtsverwaltung in diesem Sinne gehören vielmehr alle Angelegenheiten, die nicht der richterlichen Unabhängigkeit unterliegen. Die Gerichtsverwaltung, also die Verwaltungstätigkeit, die die Gerichte selbst betrifft, gehört ebenso wie die Justizverwaltung, die die Unterstützung der Rechtsprechung zum Gegenstand hat, zu den Verwaltungsaufgaben in diesem Sinn (vgl. Schmidt/Räntsch, Kommentar zum Deutschen Richtergesetz, § 4 RdNr. 16). Auch die Angelegenheiten, die in §§ 21 a bis 21 i GVG geregelt sind, gehören zu den Verwaltungsangelegenheiten, die der Datenschutzkontrolle unterworfen sind. Zwar sind diese Tätigkeiten zwingende Grundlage für die Erfüllung der rechtsprechenden Aufgabe der Gerichte. Die Art und Weise ihrer Wahrnehmung unterliegt jedoch nicht der richterlichen Unabhängigkeit.

Allerdings sind auch bei Zugrundelegung dieses Maßstabes Zweifelsfragen in der Praxis nicht auszuschließen. Deswegen hat der LfD versucht, durch die beispielhafte Aufzählung bestimmter Aspekte einen konkreten Konsens in diesem Bereich zu erzielen. Da die Meinungsverschiedenheiten zunächst bei der Prüfung des Geschäftsstellenautomationssystems „MAJA" offenbar geworden sind, geht der LfD im folgenden von Bereichen aus, die im Zusammenhang mit der Einrichtung eines gerichtlichen Geschäftsstellenautomationssystems aus seiner Sicht zu Verwaltungsangelegenheiten im Sinne des § 24 Abs. 2 LDSG gehören.

a) Das Geschäftsstellenautomationssystem wird durch das Ministerium der Justiz in Zusammenarbeit mit einer privaten Stelle entwickelt und den Gerichten angeboten. Soweit also die Phase der Entwicklung und des Anbietens an die Gerichte betroffen ist, kann die richterliche Unabhängigkeit an keinem Punkt eine Rolle spielen. Dies gilt insbesondere für die Systemkonzeption, z. B. das grundsätzliche Datenschutzkonzept. Entscheidungen in diesem Zusammenhang bereiten den konkreten gerichtlichen Einsatz nur vor. Sie unterliegen als solche nicht der richterlichen Unabhängigkeit. In diesem Zusammenhang abgegebene Stellungnahmen des LfD betreffen nur mittelbar richterliche Tätigkeiten und sind deshalb von dem Kontrollausschluß des § 24 Abs. 2 LDSG nicht betroffen.

b) Im konkreten Einsatz des Geschäftsstellenautomationssystems sind folgende Fragen von der richterlichen Unabhängigkeit unberührt:
   - Welche Verfahrensdaten aus abgeschlossenen Verfahren werden für welchen Zeitraum automatisiert gespeichert?
   - Welche Dateien mit personenbezogenen Daten sind auf Dauer unabhängig von einem laufenden Verfahren im System gespeichert?
   - Wer hat auf solche Daten zu welchem Zweck Zugriff? Durch welche technisch-organisatorischen Maßnahmen wird die Zugriffskontrolle sichergestellt?
   - Welche technischen und organisatorischen Datenschutzvorkehrungen gem. § 9 LDSG sind generell durch das MAJA-Verfahren vorgegeben, welche können vor Ort eingerichtet werden, welche Empfehlungen gibt das Justizministerium hierzu?

c) Der richterlichen Unabhängigkeit unterliegen demgegenüber folgende Festlegungen und Tätigkeiten:
   - Datenspeicherungen im System aus laufenden Verfahren;
   - Nutzung der Daten im laufenden Verfahren;
   - einzelne Übermittlungsvorgänge im laufenden Verfahren.

Das Ministerium der Justiz hat im Gegensatz dazu die Auffassung geäußert, daß die Hilfstätigkeiten der Geschäftsstellen für die richterlichen Aufgaben nicht als Verwaltungsangelegenheiten im Sinne des LDSG anzusehen seien.

Demgegenüber hält der LfD an seiner anderslautenden Auffassung fest.

Thesenhaft formuliert: Der LfD besitzt in allen datenschutzrelevanten Fällen eine Kontrollbefugnis, in denen auch das Ministerium der Justiz aufgrund seiner Justizverwaltungskompetenz Zuständigkeiten wahrnimmt.

Die praktischen Auswirkungen dieser unterschiedlichen rechtlichen Auffassungen sind aber möglicherweise zunächst jedenfalls gering: Das Ministerium der Justiz hat die Bereitschaft geäußert, den LfD im Rahmen der Projektplanung, Entwicklung, Programmierung und Umsetzung der technisch-organisatorischen Datenschutzkonzeption von Geschäftsstellenautomationssystemen umfassend zu beteiligen. Wenn das Ministerium dies als Inanspruchnahme einer Beratung auffaßt, für die keine Rechtspflicht bestünde, so hätte dieser Vorbehalt jedenfalls keine wesentliche praktische Auswirkung.

Diese Verfahrensweise würde allerdings voraussetzen, daß dem LfD im Bereich der Automation der Geschäftsstellen – Mainzer automatisierte Justizanwendungen, MAJA – umfassend die Informationen zur Verfügung gestellt würden, die sein Tätigwerden in diesem Sinne ermöglichen. Dazu gehört auch, ihm ein Kennenlernen der technischen Ausstattung ohne Beschränkung vor Ort zu gewähren. Der LfD geht davon aus, daß das Ministerium in diesem Sinne verfahren wird.

7.2 Gesetzliche Defizite

7.2.1 Dateienregelungen im Strafverfahren, Ergänzung der Strafprozeßordnung

In vielen vorangegangenen Tätigkeitsberichten hat der LfD bereits das Fehlen von Datenverarbeitungsregelungen in der Strafprozeßordnung angesprochen und ergänzende Regelungen angemahnt.

Insoweit besteht volles Einvernehmen zwischen dem LfD und dem Minister der Justiz: Die 66. Justizministerkonferenz hat in einem ausdrücklichen Beschluß „erneut" mit großem Nachdruck auf die zwingende Notwendigkeit hingewiesen, für die Datenverarbeitung der Staatsanwaltschaften eine den Maßstäben des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz entsprechende gesicherte Rechtsgrundlage zu schaffen. Die Justizminister halten es für ein länderunfreundliches Verhalten des Bundes, daß dieser noch keine entsprechende Gesetzesinitiative ergriffen hat. Sie sähen sich wegen der Untätigkeit der Bundesregierung berechtigter Kritik ausgesetzt. Einzelne Gerichte hätten zudem zu erkennen gegeben, daß sie die vom Bundesverfassungsgericht eingeräumte Übergangsfrist als abgelaufen ansehen. Damit bestünde unmittelbar die Gefahr, daß die Rechtsprechung flächendeckend die automatisierte Datenverarbeitung der Staatsanwaltschaften wegen Fehlens einer gesetzlichen Grundlage für nicht mehr zulässig erkläre.

Weil der von der Bundesregierung seit Jahren zugesagte Entwurf für ein Strafverfahrensänderungsgesetz (Dateienregelung im Strafverfahren) nicht vorgelegt worden sei, hätten die Länder im Herbst 1994 den Entwurf eines Strafverfahrensänderungsgesetzes beschlossen.

Dieser dringende Appell der Justizministerkonferenz wird vom LfD ausdrücklich begrüßt.

Bezüglich der inhaltlichen Ausgestaltung der Dateiregelungen für das Strafverfahren und sonstiger Datenschutzregelungen im Bereich der Strafverfolgungsbehörden bestehen jedoch Differenzen zwischen dem LfD und dem Ministerium der Justiz. Diesbezüglich hat es eine umfassende Diskussion gegeben. In deren Verlauf hatte der LfD Anlaß zu betonen, daß er nachvollziehbaren Argumenten aus der Sicht der Strafrechtspflege aufgeschlossen gegenüberstehe. Auch aus seiner Sicht kann der Datenschutz der Bürger keinesfalls einen absoluten Vorrang gegenüber anderen Rechtsgütern und insbesondere auch nicht gegenüber der Strafrechtspflege beanspruchen. Es sollte jedoch aus seiner Sicht Anliegen aller Beteiligten sein, in vertiefenden Erörterungen die datenschutzrechtlichen Positionen und die berechtigten Belange der Strafrechtspflege miteinander zu vereinbaren. Beide Belange sind angemessen zu berücksichtigen. Der vorgelegte Entwurf der Länder zu den Dateienregelungen im Strafverfahren wird diesem Anspruch aus der Sicht des LfD nicht gerecht. Dazu mag mit beigetragen haben, daß das Ministerium der Justiz zunächst davon abgesehen hat, die seitens des Datenschutzes vorgetragenen Vorschläge inhaltlich zu erörtern.

Der LfD hat auch Verständnis dafür, daß bei bundesgesetzlichen Regelungsvorhaben ein Landesressort nicht stellvertretend für den Bund Diskussionen führen möchte, die primär auf der Ebene des Bundes auszutragen sind. Dann aber, wenn die Länder eigenständige Vorschläge für ein Bundesgesetz formulieren und wenn das Land Rheinland-Pfalz federführend an der Erarbeitung eines solchen Gesetzgebungsvorschlages beteiligt ist, erwartet der LfD, daß die Anliegen des Datenschutzes zur Kenntnis genommen, inhaltlich ernstgenommen sowie sachlich gewürdigt werden. Gleichermaßen erwartet er, daß er über die Überlegungen informiert wird, die zu einer Ablehnung seiner Anregungen führen; besser noch wäre es, ihn in den entsprechenden Diskussionsprozeß aktiv einzubeziehen. Er geht davon aus, daß dies künftig auch und gerade im Verhältnis zum Ministerium der Justiz der Fall sein wird. Die Entwicklung der letzten Monate in diesem Bereich bestärkt ihn jedenfalls in dieser Erwartung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zu den inhaltlichen Anforderungen an die Ergänzung der StPO aus datenschutzrechtlicher Sicht Beschlüsse gefaßt, die als Anlagen abgedruckt sind (Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam zur Informations-

verarbeitung im Strafverfahren, Anlage 8, sowie Beschluß der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu fehlenden bereichsspezifischen gesetzlichen Regelungen bei der Justiz, Anlage 13).

7.2.2 Aufbewahrungsfristen – eine angemessene Regelung ist überfällig

Die Aufbewahrungsfristen für Papierunterlagen (Akten, Urteile etc.) sind im Justizbereich auch deshalb von besonderer Bedeutung, weil sie gleichzeitig Maßstab für die Speicherdauer in automatisierten Systemen sind. Bereits im 14. Tätigkeitsbericht hat der LfD erläutert, welche Forderungen er deshalb in diesem Zusammenhang an die Landesjustizverwaltung richtet. Leider hat sich kein wesentlicher Fortschritt auf diesem Gebiet gezeigt. Nach wie vor diskutieren viele Landesjustizverwaltungen diese Problematik primär unter dem Gesichtspunkt „Speicherplatz für Akten" (so ausdrücklich ein dem LfD vorliegendes Schreiben des hier federführenden nordrhein-westfälischen Ministeriums) und berücksichtigen den Grundrechtsschutzaspekt dieser Materie aus der Sicht des LfD unzureichend. Er hat sich deshalb intensiv darum bemüht, eine einheitliche Auffassung der Datenschutzbeauftragten hierzu herbeizuführen. Ergebnis dieser Bemühungen ist ein Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, der als Anlage abgedruckt ist (Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995 zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich, Anlage 20). Der LfD erwartet, daß sich das rheinland-pfälzische Justizministerium für die Realisierung der dort formulierten Anliegen einsetzt.

7.3 Bundes-SISY – der entscheidende Schlag gegen Ladendiebe oder eine überflüssige und zu umfassende Zentraldatei?

Mit dem Verbrechensbekämpfungsgesetz wurde auch die gesetzliche Grundlage für ein bundesweites staatsanwaltschaftliches Register aller eingeleiteten Ermittlungsverfahren, das „Staatsanwaltschaftliche Informationssystem (SISY)", § 478 StPO, geschaffen.

Es ist vorgesehen, den Staatsanwaltschaften ein eigenes Informationssystem zur Verfügung zu stellen, das im wesentlichen die Informationen enthält, die auch in den polizeilichen Verbunddateien (insbes. INPOL) gespeichert werden, allerdings ohne daß der bei der Polizei erreichte Datenschutzstandard (differenzierte Löschungsregelungen, Abrufprotokollierungen) vorgesehen ist. Damit wird einer Vielzahl neuer Stellen der Direktabruf sensibler Daten ermöglicht und das Potential datenschutzrechtlicher Gefährdungen wesentlich erweitert.

Für die einen ist eine solche Datensammlung ein entscheidender Schritt in der Kriminalitätsbekämpfung, für die anderen eine unverhältnismäßige, zumindest überflüssige Sammlung von Verdachtsdaten über Bürger, die oft unschuldig sind oder zu deren Gunsten jedenfalls die Unschuldsvermutung spricht. Unter dem Aspekt, daß bundesweit jährlich ca. drei Millionen Ermittlungsverfahren eingeleitet werden, von denen weit über 50 % eingestellt werden, weil kein hinreichender Tatverdacht zur Anklageerhebung besteht, ist die Bedeutung dieser Speicherungen kaum zu überschätzen.

Der Gesetzgeber hat eine solche Zentraldatei für erforderlich gehalten. Der LfD hatte deutlich dagegen votiert. Die Diskussion könnte jetzt also nur noch darum geführt werden, ob das Gesetz verfassungswidrig ist. Nach der Auffassung des LfD müssen derzeit jedenfalls alle Anstrengungen unternommen werden, um bei der Ausgestaltung des Systems und bei den technischen und organisatorischen Datenschutzmaßnahmen die Grundrechtsbeschränkungen der Betroffenen so gering wie möglich zu halten.

Entscheidend ist aus seiner Sicht, daß mißbräuchliche Abfragen entweder bereits technisch-organisatorisch ausgeschlossen werden oder daß zumindest durch wirksame Protokollierungs- und Prüfungsmaßnahmen ein vergleichbarer Sicherheitsstandard erreicht wird. Dies wird allerdings erst konkret beurteilt werden können, wenn die Realisierung dieses Systems, die für 1998 erwartet wird, weiter vorangeschritten ist.

7.4 Geschäftsstellenautomation der Staatsanwaltschaften, CUST und GAST

Nach wie vor ist das Geschäftsstellenautomationssystem GAST in Betrieb, dessen datenschutzrechtliche Defizite bereits Gegenstand der Berichterstattung vor vier Jahren waren (13. Tb. Tz. 7.3.2). Es hat sich zudem gezeigt, daß in diesem System Schwierigkeiten bei der Löschung von Daten aus eingestellten Verfahren aufgetreten sind, die zu einer äußerst arbeitsintensiven manuellen Nachbearbeitung aller zur Löschung anstehenden Fälle (die Zahl beträgt mehrere Zehntausend) zwingen. Der LfD wird die Effektivität der Überarbeitung durch örtliche Feststellungen überprüfen.

Die Einrichtung von CUST (s. 14. Tb. Tz. 7.3.3) ist vorangeschritten. Es wurden intensive Diskussionen mit dem Ministerium der Justiz darüber geführt, ob die automatisierte Datenverarbeitung bei den Staatsanwaltschaften unter Nutzung der Systeme GAST und CUST einer besonderen gesetzlichen Grundlage bedarf sowie ob die vorgesehenen organisatorischen und technischen Maßnahmen des Datenschutzes ausreichen, das informationelle Selbstbestimmungsrecht der Betroffenen angemessen zu schützen.

Die Frage, ob eine besondere gesetzliche Grundlage für solche automatisierten Speicherungen der Staatsanwaltschaften erforderlich ist, wurde vom LfD bislang zurückhaltend beantwortet, da auch seiner Auffassung nach die effektive Strafverfolgung unter heutigen Bedingungen den Einsatz der ADV im Geschäftsstellenbereich der Staatsanwaltschaften erfordert und da er – zumindest für eine angemessene Übergangszeit – die vorhandenen allgemeinen Rechtsgrundlagen der Strafprozeßordnung und der Datenschutzgesetze als ausreichende Basis ansah.

Der Schwerpunkt seiner Bemühungen in diesem Zusammenhang lag und liegt demgegenüber darauf, angemessene Maßnahmen des technischen und organisatorischen Datenschutzes beim Betrieb solcher Datenbanken zu fordern, die aus seiner Sicht höchst sensible Informationen auch über solche Personen enthalten, die ohne eigenes Zutun und eigene Verantwortung mit den Strafverfolgungsbehörden in Berührung gekommen sind.

Dabei waren und sind aus seiner Sicht insbesondere folgende Fragen bedeutsam:

- Welche Maßnahmen werden getroffen, um die Rechte der Opfer bei der Datenspeicherung angemessen (und das heißt hier: in besonderer Weise) zu schützen?
- Welche Maßnahmen werden getroffen, um insbesondere die Daten Betroffener aus eingestellten oder mit Freispruch abgeschlossenen Verfahren angemessen vor unbefugten Zugriffen zu sichern?
- Welche Maßnahmen sichern, daß Speicherung und Nutzung unter Beachtung des Verhältnismäßigkeitsgrundsatzes erfolgen?

Die bislang mit dem Justizministerium getroffenen Vereinbarungen zu diesen Bereichen stellen aus der Sicht des LfD eine Minimallösung dar, die deutlich hinter dem datenschutzrechtlich erstrebenswerten Zustand zurückbleibt. Hier bereiten dem LfD nach wie vor die Fragen der nicht vorhandenen (Lese-)Zugriffsbeschränkungen innerhalb der Staatsanwaltschaften sowie die an Stelle der Zugriffsbeschränkungen vorgesehenen Teilprotokollierungen erfolgter Zugriffe Schwierigkeiten. Ein umfassendes Konzept des technischen und organisatorischen Datenschutzes ist ohne solche Zugriffsbeschränkungen und ergänzende Protokollierungen bei sensiblen Daten – wie sie hier in Rede stehen – nicht vorstellbar.

Nunmehr sind dem Landtag in Schleswig-Holstein zwei Gesetzentwürfe über die staatsanwaltschaftlichen Verfahrensregister vorgelegt worden: zum einen der Gesetzentwurf der Fraktion der F.D.P. vom 16. August 1995, Drucksache 13/2917, zum anderen der Gesetzentwurf der Landesregierung, Drucksache 13/2927, vom 22. August 1995. In beiden Entwürfen werden die vom LfD angesprochenen Fragen sehr viel datenschutzfreundlicher geregelt, als dies der bisherigen Sachlage in Rheinland-Pfalz entspricht.

Vor dem Hintergrund der zu erwartenden gesetzlichen Regelung in Schleswig-Holstein hat der LfD gefordert, auch in Rheinland-Pfalz eine gesetzliche Regelung zu schaffen. Zumindest aber sollte der dort formulierte Standard des technischen und organisatorischen Datenschutzes für GAST und CUST realisiert werden.

Die auch im Zusammenhang mit dem bundesweiten staatsanwaltschaftlichen Informationssystem „SISY" bestehende Problematik der Speicherung von Daten, die in polizeilichen Informationssystemen längst gelöscht sein müssen, ist hier in verstärktem Umfang festzustellen: Daten über gem. § 170 Abs. 2 StPO eingestellte Verfahren, die von der Polizei sofort nach Bekanntwerden der Einstellung zu löschen sind, werden in den staatsanwaltschaftlichen automatisierten Datensammlungen mindestens fünf Jahre (u. U. länger) aufbewahrt. Dies ist aus der Sicht des LfD unangemessen (vgl. hierzu die Forderungen unter 7.2.2). Der bei der Polizei erreichte Standard des Grundrechtsschutzes wird durch das staatsanwaltschaftliche Informationssystem in allen Fällen erheblich verschlechtert.

7.5 Telefonabhörmaßnahmen

7.5.1 Örtliche Feststellungen bei einer Staatsanwaltschaft des Landes

Gegenstand des Informationsinteresses des LfD waren die Fragen der Telefonüberwachung bei abgeschlossenen Strafverfahren, insbesondere die Einhaltung der Vorschrift über die unverzügliche Vernichtung von Unterlagen aus einer Telefonüberwachung, wenn diese für Zwecke des Strafverfahrens nicht mehr benötigt werden (§ 100 b Abs. 6 StPO).

Die Prüfung hat ergeben, daß von elf geprüften Strafverfahren, in denen die Telefonüberwachung eingesetzt wurde und die zwischenzeitlich abgeschlossen sind, in zwei Verfahren die TÜ-Unterlagen vollständig weiter aufbewahrt werden, um in Verfahren gegen andere Beschuldigte verwendet zu werden. In allen anderen Fällen bestand Einigkeit, daß eine Vernichtung der TÜ-Unterlagen „unverzüglich" gem. den Vorgaben des § 100 b Abs. 6 StPO zu erfolgen hatte. Im Widerspruch zur Vernichtungspflicht befanden sich in drei Verfahren noch schriftliche TÜ-Unterlagen im Zeitpunkt der Prüfung in den Akten. In einem Fall wurden die Unterlagen bereits im Beisein des feststellenden Beamten vernichtet, in zwei anderen Fällen erfolgte dies

nach Abschluß der örtlichen Feststellungen. In einem Fall, in dem die Telefonüberwachung nichts Belastendes ergeben hatte, dennoch aber Anklage erhoben werden konnte, war nach Auffassung des LfD die Aufbewahrung und die Übersendung der TÜ-Unterlagen an das Gericht nicht zulässig. In sieben Fällen waren erst in Vorbereitung des Besuchs des Mitarbeiters des LfD Vernichtungen durchgeführt worden. Nur in einem Fall erfolgte die Vernichtung auch aus der Sicht des LfD „unverzüglich", in acht Fällen sind Verspätungen zu konstatieren; die Verspätungen liegen zwischen zwei Monaten und fast zwei Jahren.

In den Fällen, in denen der Anschlußinhaber nicht auch Beschuldigter war, wurden nur die Beschuldigten, nicht aber die Anschlußinhaber über die durchgeführte TÜ unterrichtet.

Ein Fall betraf einen öffentlichen Münzfernsprecher sowie ein öffentliches Kartentelefon. Der richterliche Beschluß hatte die Abhörmaßnahme ausdrücklich auf Gespräche des Beschuldigten beschränkt. Dennoch wurden zunächst alle Gespräche aufgezeichnet. Darunter waren keine Gespräche des Beschuldigten. Eine Löschung erfolgte erst nach der (akustischen) Feststellung, daß die Anrufe nicht vom Beschuldigten ausgingen.

In keinem Fall entsprach die Protokollierung der Löschung von Bändern und der Vernichtung von Unterlagen den Anforderungen, die aus datenschutzrechtlicher Sicht an eine korrekte Protokollierung zu stellen sind (vgl. auch Kleinknecht/Meyer, StPO-Kommentar, Anm. 7 zu § 100 b).

Aus der Sicht des LfD ist es erforderlich, daß durch das Ministerium der Justiz landesweite einheitliche Vorgaben formuliert werden, um

- tatsächlich unverzüglich die TÜ-Unterlagen zu vernichten und die Bänder zu löschen,
- die Benachrichtigung der nicht beschuldigten Anschlußinhaber sicherzustellen sowie um
- die Protokollierungen, die aus seiner Sicht eine unverzichtbare Schutzfunktion für die Effektivität der Durchsetzung der Vernichtungspflicht haben, aussagekräftig zu gestalten.

Die konkreten Vorschläge hierzu ergeben sich unten aus Tz. 7.5.3.

7.5.2 Sonstige Beanstandungen

Aus Anlaß von Eingaben eines einzelnen Betroffenen einer Telefonüberwachungsmaßnahme hatte sich der LfD mit folgenden Aspekten dieses Ermittlungsverfahrens, das im Zeitpunkt der Eingaben wegen nicht hinreichenden Tatverdachts gem. § 170 Abs. 2 StPO eingestellt worden war, zu befassen:

a) Raumgesprächsaufzeichnungen (s. hierzu Tb. 14, Tz. 7.3.4.2);

b) Aufzeichnung von Verteidigertelefonaten (s. hierzu Tb. 14, Tz. 7.3.4.3);

c) Versendung eines Originalbeweisbandes mit Verteidigertelefonaten an das Landeskriminalamt eines anderen Bundeslandes;

d) rechtzeitige Vernichtung der Telefon-Abhörprotokolle;

e) weitere Aufbewahrung von Teilen der Telefon-Abhörprotokolle in anderen Ermittlungsakten als denen des Ursprungsverfahrens;

f) Vernichtung beschlagnahmter Kontounterlagen in den Ermittlungsakten;

g) Vernichtung von beschlagnahmten privaten Telefonnotizzetteln in den Ermittlungsakten;

h) Vernichtung von beschlagnahmten Tagebuchaufzeichnungen und daraus gefertigten Kopien in den Ermittlungsakten;

i) Vernichtung von ED-Unterlagen; Aufbewahrung von Lichtbildern des Beschuldigten in der Ermittlungsakte;

j) Verpflichtungserklärung eines zur Übersetzung eines Telefonats eingesetzten Privatmannes;

k) Auskunftsanspruch über die Person dieses eingesetzten Übersetzers (zur allgemeinen Problematik des Auskunftsanspruchs aus Strafverfahren s. unten 7.6);

l) Fehlblätter in der TÜ-Akte;

m) Speicherung in der Datei Fish beim BKA sowie in POLIS/INPOL;

n) Durchsuchungsbeschluß, Unterrichtung der Drittbetroffenen über den Verfahrensausgang;

o) Anlage von Sonderakten über Pressereaktionen auf diesen Fall bei der Staatsanwaltschaft;

p) beim Amtsgericht verschwundene Strafanzeigen des Betroffenen gegen Amtsträger;

q) Zulässigkeit der Übermittlung eines Einstellungsbeschlusses an den beschuldigten Amtsträger (Kriminalbeamten).

Der LfD konnte das Vorgehen der Staatsanwaltschaft nicht in allen Punkten akzeptieren. Eine Darstellung der Einzelheiten soll an dieser Stelle jedoch unterbleiben. Folgerungen von allgemeinerer Bedeutung für die Durchführung von Telefonüberwachungsmaßnahmen sind unten unter Tz. 7.5.3 dargestellt.

7.5.3 Vorschläge für eine datenschutzgerechtere Ausgestaltung der Überwachung des Fernmeldeverkehrs

Nicht nur als Ergebnis der örtlichen Feststellungen zur Frage der Durchführung von Fernmeldeüberwachungsmaßnahmen gem. §§ 100 a ff. StPO bei einer Staatsanwaltschaft im Land (s. o. Tz. 7.5.1), sondern auch als Folge einer inzwischen langjährigen Beschäftigung mit den in diesem Zusammenhang entstehenden Problemen hat der LfD dem Ministerium der Justiz folgende Vorschläge zur Verbesserung des Datenschutzes bei Telefonabhörmaßnahmen auf der Ebene der Ausführung der gesetzlichen Vorschriften vorgetragen (nur dieser Bereich kann durch das Ministerium durch eine Verwaltungsvorschrift geregelt werden):

a) Es sollten einheitliche Vorgaben für alle Staatsanwaltschaften des Landes getroffen werden, bestimmte Aufzeichnungen über die durchgeführten TÜ-Maßnahmen vorzunehmen, um aussagekräftige Statistiken in diesem Zusammenhang zu erhalten. Es erscheint der Bedeutung der TÜ-Maßnahmen in bezug auf die Grundrechte der Betroffenen (zu denen ja bei weitem nicht nur beschuldigte oder verdächtige Personen gehören) nicht angemessen, wenn Festlegungen über solche Statistiken mit ganz unterschiedlichem Inhalt durch die jeweiligen Behördenleiter getroffen werden können. Als Ersatz der vor einigen Jahren abgeschafften Berichtspflicht sollten detaillierte, aussagekräftige Statistiken mit gleichem Inhalt landesweit vorgeschrieben werden.

   Der Erhebungskatalog, der von einer Arbeitsgruppe im Auftrag des Strafrechtsausschusses der Justizministerkonferenz entwickelt worden ist, bleibt weit hinter dem Erforderlichen zurück. Zusätzlich wären mindestens folgende Informationen statistisch zu erheben:

   Zahl und Art der abgehörten Anschlüsse, differenziert nach
   - öffentlich zugänglichen Anschlüssen (z. B. öffentliche Telefonzellen, Gaststätten);
   - Anschlüsse, deren Inhaber nicht beschuldigt ist;
   - Telefonanschlüsse im C- oder D-Netz;
   - sonstige;

   Dauer der tatsächlichen Abhörmaßnahme;

   Zahl der aufgezeichneten Telefonate;

   Art der Beendigung des jeweiligen Ermittlungsverfahrens (Urteil mit Ergebnis; Einstellung unter Angabe der Rechtsgrundlage);

   Angabe, ob Erkenntnisse aus der TÜ für das Ermittlungsergebnis bedeutsam waren;

   Angabe, ob die TÜ-Unterlagen für weitere Ermittlungsverfahren bedeutsam waren (wenn ja, Angabe der Zahl).

b) Die Überwachungsangelegenheiten nach §§ 100 a ff. StPO sollten als besonderes Sachgebiet grundsätzlich einem bestimmten Dezernenten zugewiesen werden. Der Dezernent müßte die Überwachung persönlich leiten und sich ständig über die Überwachungsergebnisse unterrichten (so Nr. 2.1 der schleswig-holsteinischen Richtlinien für die Staatsanwaltschaften und die Polizei zur Überwachung des Fernsprechverkehrs in Strafsachen).

c) Die derzeitige Regelung in Nr. 2.15 der VV sieht vor, daß ein ständiges Mithören durch Polizeibeamte nur erfolgen solle, wenn anzunehmen sei, daß aufgrund des Ergebnisses der Überwachung sofortige Maßnahmen erforderlich seien. Diese Formulierung ist aus der Sicht des LfD zu eng: Ein ständiges Mithören kann auch aus anderen Gründen erforderlich sein, etwa um beim Abhören eines öffentlich zugänglichen Telefonanschlusses (Telefonzelle, Gaststätte) Gespräche, die nicht vom Beschuldigten geführt werden, sofort von der Aufzeichnung auszuschließen.

d) Von erheblicher Bedeutung ist es, die Anforderung des § 100 b Abs. 6 StPO der „unverzüglichen" Vernichtung von TÜ-Unterlagen wirksam umzusetzen, wenn diese für das Strafverfahren nicht mehr von Bedeutung sind. Hierzu sind folgende Maßnahmen erforderlich:

   aa) In der Verwaltungsvorschrift sollte angeordnet werden, daß die TÜ-Unterlagen grundsätzlich mit besonderer Kenntlichmachung den Ermittlungsakten beizuheften sind, daß diese Unterlagen also grundsätzlich zu einem Sonderheft zu nehmen sind, aus dem sich auch die Quelle eindeutig ergeben muß.

   bb) Spätestens im Zeitpunkt der Einstellungsverfügung im Falle der Einstellung gem. § 170 Abs. 2 StPO oder nach Erlaß eines rechtskräftigen Urteils ist über die Frage zu entscheiden, ob Bänder und Unterlagen zu löschen bzw. zu vernichten sind oder ob, zu welchem Zweck und durch wen sie weiter aufzubewahren wären. Folgende zulässige Alternativen dürften bestehen:

– Anordnung der Vernichtung der TÜ-Unterlagen und Löschung der Bänder, Protokollierung s. unten;

– Weitergabe der TÜ-Unterlagen und -bänder zu den Ermittlungsakten eines anderen Beschuldigten, wenn diese Vorgänge für dieses Ermittlungsverfahren bedeutsam sind. Die Abgabe wäre – in ähnlicher Detaillierung wie im Fall der Vernichtung – genau zu protokollieren. Im aufnehmenden Verfahren wäre dann über den Zeitpunkt der Vernichtung bzw. Löschung in entsprechender Weise zu entscheiden.

– Zu entscheiden wäre, ob im Fall der Einstellung gem. § 170 Abs. 2 StPO wegen nicht hinreichenden Tatverdachts die Möglichkeit der weiteren Aufbewahrung besteht. Aus datenschutzrechtlicher Sicht neigt der LfD hier zu einer restriktiven Auffassung. Wenn das Ministerium der Justiz es aber für zulässig und geboten hält, sollte eine entsprechende Regelung in die VV aufgenommen werden. Denkbar wäre es, die weitere Aufbewahrung der TÜ-Unterlagen und -bänder unter der Feststellung zuzulassen, daß ein Restverdacht verblieben ist und daß die TÜ-Unterlagen möglicherweise für ein Wiederaufgreifen des Falles Bedeutung erlangen können. Die hierfür maßgeblichen Gesichtspunkte wären aktenkundig zu machen.

cc) Es sollte vorgeschrieben werden, daß die Staatsanwaltschaft durch die ermittelnden Polizeidienststellen über das Fertigen bzw. das Vorhandensein von Abschriften aus den TÜ-Unterlagen sowie über die Fertigung von Phone-Dateien – Sicherungsdisketten und -kopien – jeweils unverzüglich zu unterrichten ist.

dd) Inhaltlich müßten die Vorgaben für die Protokollierung der Löschung bzw. Vernichtung von TÜ-Unterlagen präzisiert werden.

Bei der Löschung der entstandenen Tonbänder sollte folgendes aufgezeichnet werden:

– Anzahl der zu löschenden Bänder, getrennt nach Arbeits- und Beweisbändern; technische Kurzbeschreibung der Bänder (in erster Linie Laufzeit);

– Zahl der aufgezeichneten und damit gelöschten Gespräche;

– Angabe des genauen Löschungsdatums;

– Bezeichnung der Löschtechnik (Nennung des eingesetzten Löschverfahrens);

– Nennung des die Löschung verantwortlich durchführenden Beamten.

ee) Im Zusammenhang mit der Vernichtung von schriftlichen Aufzeichnungen wären folgende Angaben zu protokollieren:

– Bezeichnung nach Art (Inhalt) und Anzahl, z. B. „Verbindungsdaten der Gespräche Nr. 1 – 3000"; „35 Blätter Wortprotokolle (TÜ-Niederschriften)"; „200 Seiten Ausdrucke aus der Phone-Datei";

– Angabe des genauen Vernichtungsdatums;

– Nennung des die Vernichtung verantwortlich durchführenden Bediensteten;

– Bezeichnung der Vernichtungsart (Nutzung des hauseigenen Aktenvernichters o. ä.).

ff) Bezüglich der durch die Polizei vorzunehmenden Löschung bzw. Vernichtung sollte es dabei bleiben, daß ein Staatsanwalt hierbei anwesend zu sein hat (vgl. § 100 b Abs. 6 StPO).

f) In der VV sollte vorgeschrieben sein, daß die TÜ-Bänder bei der ermittelnden Polizeidienststelle im Asservatenraum sicher aufzubewahren sind und daß eine Kontrolle des Bestandes anhand von schriftlichen Unterlagen (Papierbelegen, z. B. Karteikarten o. ä.) möglich sein muß.

g) Weiterhin sollte deutlich gemacht werden, daß die Benachrichtigungspflicht gem. § 101 StPO nicht nur gegenüber dem Beschuldigten besteht; wenn der Beschuldigte nicht zugleich auch Anschlußinhaber des abgehörten Telefonanschlusses ist, sollte ausdrücklich vorgegeben werden, auch den oder die Anschlußinhaber zu unterrichten.

h) In die VV sollte eine Regelung über die Verwendung von Informationen aus Abhörmaßnahmen zum Zweck der Gefahrenabwehr eingefügt werden.

i) Der LfD hält seine Forderung aufrecht, die automatisierte Aufzeichnung von Telefonaten technisch so auszugestalten, daß bestimmte Verbindungen (die mit der Telefonnummer des Verteidigers) von der Aufzeichnung ausgeschlossen werden können.

Ob und in welchem Umfang die verantwortlichen Ministerien diesen Empfehlungen folgen, ist derzeit noch nicht absehbar.

7.6 Auskunftsansprüche gegen die Strafverfolgungsbehörden?

Aufgrund einer Eingabe hatte sich der LfD mit der Frage zu befassen, ob und gff. in welchem Umfang Auskunftsansprüche betroffener Bürger gegenüber der Staatsanwaltschaft außerhalb des Akteneinsichtsrechts des Beschuldigten gem. § 147 StPO bestehen, wenn Erkenntnisse über diese Bürger bei der Strafverfolgungsbehörde vorhanden sind.

Er vertritt hierzu folgende Auffassung:

Die StPO enthält derzeit keine Rechtsgrundlage für solche Auskünfte. § 147 StPO betrifft nur die Akteneinsicht des Beschuldigten während des Strafverfahrens.

Auch das Strafverfahrensänderungsgesetz wird keine umfassende Regelung dieser Frage mit sich bringen: §§ 475 und 486 des StVÄG-Entwurfs, die diesen Bereich regeln, betreffen nur ganz bestimmte Datenbestände: zum einen solche Daten, die in Akten enthalten sind, die dem Gericht vorliegen oder diesem im Falle der Erhebung der öffentlichen Klage vorzulegen wären (§ 475 StVÄG-Entwurf), zum anderen Daten, die in Dateien gespeichert werden (§ 486 StVÄG-Entwurf).

Alle in sonstigen Datenbeständen enthaltenen Informationen (etwa Informationen in staatsanwaltlichen Handakten, in sonstigen staatsanwaltschaftlichen, polizeilichen oder gerichtlichen Unterlagen) sind von der Auskunftsregelung nicht betroffen. Zudem differenzieren die genannten Entwurfsregelungen nicht nach der Stellung des Auskunftsbegehrenden als „Betroffener" i. S. des Datenschutzes oder als sonstiger Auskunftsbegehrender.

Das LDSG ist für die Frage der Auskunftserteilung an den Betroffenen durch Organe der Rechtspflege (i. S. d. § 18 Abs. 6 LDSG) nicht heranzuziehen. Dabei neigt der LfD zu der Auffassung – ohne insoweit seine Meinungsbildung abgeschlossen zu haben –, daß in diesem Zusammenhang eine ausschließliche Bundeskompetenz besteht und für landesrechtliche Regelungen kein Raum mehr ist, wenn es um Fragen geht, die unmittelbar vom Strafverfahrensrecht geregelt werden oder die als sein unmittelbarer Annex anzusehen sind.

Damit ergibt sich die Frage, ob nicht derzeit außerhalb des Anwendungsbereichs des § 147 StPO (und künftig auch außerhalb des Anwendungsbereichs der §§ 475 und 486 StPO) ein Auskunftsanspruch nach allgemeinen Vorschriften besteht.

a) Auskunftsanspruch nach § 19 BDSG

Es könnte die Auffassung vertreten werden, ein Auskunftsanspruch folge aus § 1 Abs. 2 Nr. 2 a bzw. b i. V. m. § 12 Abs. 2 Nr. 1 bzw. 2, 19 BDSG. Aus den genannten Vorschriften ergibt sich, daß § 19 BDSG, der die Auskunft an Betroffene regelt, für öffentliche Stellen der Länder anzuwenden ist, soweit sie entweder Bundesrecht ausführen oder als Organe der Rechtspflege tätig werden, es sich nicht um Verwaltungsangelegenheiten handelt und der Datenschutz insoweit nicht durch Landesgesetz geregelt ist.

Die Auskunftserteilung im Bereich der Rechtspflege ist nach dem oben Ausgeführten durch Landesgesetz überhaupt nicht regelbar. Insoweit wäre also das bereichsspezifische Bundesrecht und – ergänzend – das BDSG anzuwenden. Die Verweisung auf § 19 BDSG für die in §§ 1 und 12 genannten öffentlichen Stellen der Länder (darunter auch ausdrücklich die Organe der Rechtspflege) würde sonst auch leerlaufen (vgl. hierzu Dammannn, in Simitis/Dammann/Geiger/ Walz, Komm. z. BDSG, Anm. 210, 211, 216, 217 zu § 1 BDSG).

b) Auskunftsanspruch unmittelbar aus dem Grundgesetz (Artikel 1 Abs.1, 2 Abs.1 GG)

Es wird die Auffassung vertreten, ein solcher Auskunftsanspruch ergebe sich unmittelbar aus der Verfassung. Rechtsgrund eines solchen Anspruchs des Betroffenen sind das allgemeine Persönlichkeitsrecht sowie das informationelle Selbstbestimmungsrecht der Artikel 1 Abs. 1, 2 Abs. 1 Grundgesetz. Die Rechtsprechung geht schon bislang in den verschiedensten Zusammenhängen in weitem Umfang davon aus, daß derjenige, über den Informationen bei einer Behörde gespeichert werden, von Verfassungs wegen einen Auskunftsanspruch über den Inhalt solcher Informationen und auch über die Empfänger im Falle der Übermittlung hat. Über dieses Auskunftsbegehren des Bürgers ist nach pflichtgemäßem Ermessen zu entscheiden (OVG Koblenz, Urteil vom 21. Juli 1982, NJW 83, 2957; VGH München, NJW 1980, 198; VGH München, Beschluß vom 21. März 1991, NVWZ-RR 92, 72; BFH, Urteil vom 8. Februar 1994, BB 94, 1413, wo ein solcher Anspruch selbst für Informationen, die dem Steuergeheimnis unterliegen, festgestellt wird; ausdrücklich offengelassen vom Bundesverwaltungsgericht, Urteil vom 20. Februar 1990, NJW 1990, 2761).

Der Berliner Senator der Justiz vertritt beispielsweise die Auffassung, daß ein solcher Auskunftsanspruch auch gegenüber der Justiz bei abgeschlossenen Strafverfahren bestünde.

Ein Rechtsgebiet, in dem dahinter zurückbleibende Regelungen gelten, ist dem LfD nicht bekannt. Man könnte allerdings einwenden, die StPO habe bewußt keine Auskunftsregelung zugunsten des Betroffenen für Informationen getroffen, die nicht von ihren eigenen Auskunfts- und Einsichtsregelungen umfaßt werden. Eine solche Auslegung müßte allerdings verfassungsgemäß sein. Dies ist nicht der Fall: Der von Verfassungs wegen geltende Anspruch könnte durch ein Gesetz nicht konkludent durch bloßes Nichtregeln von Sachverhalten beseitigt werden.

Es ist also immer eine Ermessensentscheidung über die Auskunftserteilung zu treffen. Das Interesse des Betroffenen an umfassender Information wäre beispielsweise gegenüber folgenden anderen Gesichtspunkten abzuwägen:

- Gefährdung der Aufgabenerfüllung der auskunfterteilenden Stelle,
- Gefährdung von sonstigen Allgemeininteressen,
- überwiegende berechtigte Interessen eines Dritten.

Die Frage, ob § 19 BDSG oder der aus der Verfassung unmittelbar herzuleitende Auskunftsanspruch heranzuziehen ist, kann unentschieden bleiben: Aus der unterschiedlichen Herleitung des Anspruchs resultieren keine unterschiedlichen Beurteilungskriterien.

Dem Betroffenen ist also auf Antrag eine begründete Ermessensentscheidung zu erteilen. Bei Zugrundelegung der genannten Kriterien würde nach Ansicht des LfD auch in jedem Einzelfall ein sachangemessenes Ergebnis erzielbar sein, das sowohl der Funktionsfähigkeit der staatlichen Stellen wie dem Persönlichkeitsrecht der Betroffenen angemessen Rechnung trägt.

Das Ministerium der Justiz besteht demgegenüber auf seiner hiervon abweichenden Auffassung.

7.7 Darf ein Strafurteil an eine ausländische Vormundschaftsbehörde übersandt werden?

Aus Anlaß der Bearbeitung einer Eingabe ist die datenschutzrechtliche Problematik der „Rechtshilfeordnung für Zivilsachen" (ZRHO) ins Blickfeld geraten. Hintergrund der Befassung mit dieser Materie war folgender Fall:

Eine schweizerische Gemeinde, welche die Aufgaben der Vormundschaftsbehörde wahrzunehmen hat, erbat von einer rheinland-pfälzischen Staatsanwaltschaft die Übersendung eines Strafurteils. Sie wollte in einem Sorgerechtsstreit beurteilen können, ob der Kindesvater, der mit dem Strafurteil verurteilt worden war, eine Gefährdung seiner Tochter verursachen könnte. Die rheinland-pfälzische Staatsanwaltschaft ist dem Ersuchen nachgekommen.

Diese Urteilsübersendung ist als Hilfeleistung einer deutschen Justizbehörde (Staatsanwaltschaft) gegenüber einer ausländischen Verwaltungsbehörde (Vormundschaftsbehörde) anzusehen. Das Verfahren, in dem Hilfe geleistet wurde, war eine Sorgerechtsangelegenheit, also eine zivilrechtliche Angelegenheit.

Die Gesetze und zwischenstaatlichen Vereinbarungen, die Hilfeleistungen in zivilrechtlichen Angelegenheiten zum Gegenstand haben, wie das Haager Übereinkommen über den Zivilprozeß vom 1. März 1954 oder die dazu ergangenen Zusatzvereinbarungen, regeln ausschließlich gerichtliche Verfahren. Behördliche Verfahren sind davon nicht betroffen.

Behördliche Auskunftsersuchen in einem Zivilverfahren sind nach §§ 94 bis 97 der ZRHO zu beurteilen.

Diese Rechtshilfeordnung ist jedoch keine zwischenstaatliche Vereinbarung, kein Gesetz und keine Rechtsverordnung, also kein (formelles) Gesetz. Es handelt sich vielmehr um eine gleichlautende Verwaltungsvorschrift der Justizministerien (bundeseinheitlich aufgrund eines Beschlusses der 25. Justizministerkonferenz in München am 19. Oktober 1956 in Kraft gesetzt, 1976 neu gefaßt, Fundstelle: Piller/Hermann, Justizverwaltungsvorschriften, Lose-Blatt-Sammlung, Beck-Verlag; vgl. zur Rechtsnatur der ZRHO etwa Puttfarken, NJW 88, 2155). Datenübermittlungen können auf diese Rechtshilfeordnung also grundsätzlich nicht gestützt werden.

Folgende Schwierigkeit kommt im vorliegenden Zusammenhang hinzu: §§ 94 bis 97 ZRHO nennen keine inhaltlichen Kriterien für die Zulässigkeit entsprechender Aktenübersendungen bzw. Urteilsübermittlungen. Es handelt sich hierbei vielmehr ausschließlich um Verfahrensregelungen, die vorsehen, daß entsprechende Ersuchen grundsätzlich einer „Prüfungsstelle" (dem Landgerichtspräsidenten) und der Landesjustizverwaltung vorzulegen sind. Nach welchen Kriterien die entscheidungsbefugten Stellen Daten übermitteln sollen, ergibt sich aus der Rechtshilfeordnung nicht.

Fraglich ist also, ob insofern ergänzend das allgemeine Datenschutzrecht mit seinen Regelungen für die Übermittlung in das Ausland herangezogen werden kann.

Wenn man dies für unangemessen hält, wäre zu fordern, Fälle der vorliegenden Art bereichsspezifisch gesetzlich zu regeln. Im Bereich der Hilfeleistung in Strafsachen ist eine solche gesetzliche Regelung (das Gesetz über die internationale Rechtshilfe in Strafsachen) in Kraft.

Aus der Sicht des LfD wäre aber eine vergleichbare gesetzliche Regelung für den Bereich der Hilfeleistung in Zivilsachen bzw. behördlichen Verfahren nicht unbedingt erforderlich. Der LfD ist vielmehr der Auffassung, daß die Regelungen des allgemeinen Datenschutzrechts über Datenübermittlungen ins Ausland (§ 17 LDSG bzw. § 17 BDSG) auch Grundlage von Datenübermittlungen durch die Justiz sein können.

7.8 Datenschutz für Opfer und Zeugen

Der Datenschutz bei Opfern und Zeugen von Straftaten wird immer wieder von Betroffenen als unzureichend beklagt. Das Strafverfahren hat gewichtige Eingriffe in das informationelle Selbstbestimmungsrecht aller Beteiligten, des Beschuldigten natürlich in erster Linie, aber auch der Zeugen und Opfer zur Folge. Die besondere Situation des Opfers liegt darin, daß es häufig völlig ohne eigenes Zutun, ohne eigene Verantwortung in eine Situation gekommen ist, in der es staatliche Informationseingriffe dulden muß. Schon aus diesem Grund sind seine berechtigten Interessen grundsätzlich höher zu gewichten als die anderer Beteiligter, die es meist selbst zu verantworten haben, daß sie sich in einer Situation befinden, in der sie diesen Informationseingriffen ausgesetzt sind.

Die Abwägung im konkreten Fall ist schwierig. Ebenso schwierig ist es, gegenüber dem Gesetzgeber Vorschläge für gesetzliche Neuregelungen zu formulieren. Das Opferschutzgesetz und die darauf erfolgten Änderungen auf der Ebene der Verwaltungsvorschriften, insbesondere die Richtlinien für das Straf- und Bußgeldverfahren (RiStBV), haben sicher schon einiges in Richtung Opferdatenschutz bewirkt. Diese Richtlinien dürften übrigens in der Praxis mindestens ebenso wichtig sein wie das Gesetz. Beispielhaft ist hier auf die Nr. 4 c RiStBV, allgemeine Rücksichtnahme auf den Verletzten bei den Ermittlungen, zu verweisen. Nr. 19 a regelt die besondere Rücksicht auf den Verletzten als Zeugen, ihm sollen insbesondere Mehrfachvernehmungen erspart werden; schließlich ist Nr. 131 a RiStBV zu erwähnen, wonach auch die Staatsanwaltschaft zu prüfen hat, ob nicht die Öffentlichkeit zum Schutz des Verletzten von der Verhandlung ausgeschlossen werden sollte. Der Staatsanwalt selbst soll eigenverantwortlich initiativ werden und einen entsprechenden Antrag stellen, wenn der Verteidiger, aus welchen Gründen auch immer, dies unterläßt.

Ergänzend sind die Regelungen im Gerichtsverfassungsgesetz über den Ausschluß der Öffentlichkeit im Interesse des Zeugen oder Verletzten zu erwähnen (§ 171 b GVG). In diesem Zusammenhang ist weiter eine Regelung bedeutsam, die wohl in der Praxis noch nicht die Rolle spielt, die sie im Opferinteresse haben sollte, nämlich die Vorschrift des § 174 Abs. 3 GVG, wonach der Vorsitzende in der Verhandlung im Interesse der Zeugen und Verletzten eine Geheimhaltungsverpflichtung für alle Beteiligten aussprechen kann. Diese Geheimhaltungsverpflichtung betrifft dann nicht nur das, was verhandelt wird, sondern auch die schriftlichen Vorgänge, den Akteninhalt. Rechtsfolge dieser Verpflichtung ist, daß ein Verstoß nach § 353 d StGB strafbar ist.

Es ist ein wesentliches Anliegen des LfD, daß diese rechtlichen Möglichkeiten in der Praxis auch in allen geeigneten Fällen genutzt werden. Auch andere vorhandene Regelungen, wie z. B. § 68 StPO, könnten durchaus opferfreundlicher genutzt werden, als es derzeit geschieht. So vertritt die Rechtsprechung fast einmütig, daß mit dem Begriff „Wohnort", der vom Zeugen anzugeben ist, die genaue Wohnanschrift gemeint sei. Im Interesse der Opferzeugen liegt es aber nahe, den Begriff „Wohnort" in diesem Zusammenhang wörtlich zu nehmen. Diese Auffassung vertreten etwa auch Rebmann und mit ihm einige andere Kommentatoren der Strafprozeßordnung. Die gegenteilige Auffassung der Rechtsprechung und der Strafverfolgungsbehörden hat nachteilige Folgen für die Opferzeugen. Dies ist auch bei Bußgeldverfahren, im Verwarnungsgeldverfahren, aber auch bei Strafbefehlen bedeutsam. Hier ist es üblich, daß der Zeuge auf Bußgeldbescheiden, auf Verwarnungsgeldbescheiden und auf dem Strafbefehl mit Namen und Anschrift angegeben wird. Dies hat die Folge, daß Betroffene – nicht nur Opfer, aber auch Opfer –, die die Strafverfolgungsbehörden informiert haben, belästigt und gefährdet werden.

Als Argument gegen die Möglichkeit zur Geheimhaltung der Anschrift von Opferzeugen wird darauf verwiesen, bereits die Angabe des Wohnortes begründe schon solche Gefährdungslagen, denn man müsse nur die Meldebehörden um Auskunft fragen, eine einfache Melderegisterauskunft sei ohne weitere Voraussetzung zulässig. Dem ist entgegenzuhalten, daß Personen, die wirklich gefährdet sind oder sich gefährdet fühlen und die auch entsprechende Tatsachen glaubhaft machen können, die Möglichkeit haben, eine Sperre im Melderegister eintragen zu lassen, so daß hier ein wirksamer Datenschutz rechtlich durchsetzbar ist.

Das Hauptargument, warum Name und auch konkrete Wohnanschrift des Zeugen so wichtig seien, ist, daß dem Beschuldigten ermöglicht werden müsse, die Glaubwürdigkeit des Zeugen konkret zu überprüfen. Es müsse möglich sein, in seinem Wohnumfeld seinen Leumund zu erkunden und der Frage nachzugehen, ob es sich hier um einen notorischen Lügner handelt. Gegen dieses Argument ist bisher noch keine überzeugende Widerlegung gelungen. Rebmann hat in diesem Zusammenhang vorgeschlagen, einen Treuhänder einzuschalten, der im Interesse des Beschuldigten die Glaubwürdigkeit prüft, ohne selbst – wie der Verteidiger – eine enge Verbindung zum Beschuldigten zu haben. Es soll also eine Art Treuhandsanwalt eingeschaltet werden, der die Glaubwürdigkeitsprüfung übernimmt, das Ergebnis dem Verteidiger mitteilt und damit verhindert, daß der Verteidiger selbst die sensiblen Informationen zur Kenntnis bekommt; denn die Situation des Verteidigers gegenüber seinem Mandanten ist schwierig, wenn er Informationen zurückhalten will.

Ob das ein praktikabler Vorschlag ist, sollte aus der Sicht des Datenschutzes vertieft diskutiert und erwogen werden.

Bei der Besorgnis der Gefährdung genügt die Angabe einer ladungsfähigen Anschrift des Opferzeugen. Das ist derzeit objektiv zu prüfen. Dies bedeutet, daß bei der Besorgnis bloßer Belästigungen ein solcher Opferschutz nicht möglich ist.

Angesichts der geschilderten Haltung der Rechtsprechung wird man einen besseren Schutz des Opferzeugen in bezug auf die Angabe seiner Wohnanschrift wohl nur auf der Basis einer förmlichen Rechtsänderung erreichen können.

Auch bei den meldegesetzlichen Möglichkeiten, den Opferschutz zu realisieren, ist die Praxis nicht fehlerfrei. Selbst wenn eine Sperre im Melderegister eingetragen ist, besteht aufgrund der Vielzahl der abfrageberechtigten Stellen immer die Gefahr, daß solche Sperren versehentlich nicht berücksichtigt werden.

Defizite in der Praxis dürften auch im Bereich des § 174 Abs. 3 GVG bestehen. Der Gerichtsvorsitzende sollte insbesondere dann von der Möglichkeit, Geheimhaltungspflichten auszusprechen, Gebrauch machen, wenn Gutachten mit intimen Details über Zeugen und Opfer vorgelegt werden, beispielsweise im Zusammenhang mit der Beurteilung der Glaubwürdigkeit. Diese Gutachten enthalten ja häufig sehr intime Details über die Lebensgeschichte des Zeugen oder der Zeugin. Insbesondere dann, wenn keine anderen Zeugen als das Opfer da sind (beispielsweise in Vergewaltigungsprozessen) und dann ein Glaubwürdigkeitsgutachten gefertigt wird, in dem die gesamte Lebensgeschichte des Opfers dargestellt wird, ist diese Geheimhaltungsverpflichtung wichtig. Diese äußerst sensiblen und geheimhaltungsbedürftigen Informationen könnten auf dem Weg über § 174 Abs. 3 GVG geschützt werden.

In diesem Zusammenhang ist ein Fall zu schildern, der dem LfD vorgetragen wurde. Eine junge Frau hatte nach einem Gaststättenbesuch noch ihren Zufallsbekannten begleitet. Im weiteren Verlauf des Abends kam es dann zu einer Auseinandersetzung. Die Frau erklärte anschließend gegenüber der Polizei, es habe ein Vergewaltigungsversuch vorgelegen, sie habe sich gewehrt und weglaufen können. Im Verlauf der weiteren Aufklärung der Angelegenheit zog der Staatsanwalt, sicher zu Recht, eine große Zahl verschiedener Akten über das Opfer bei. Darunter Familiengerichtsakten, denn es war geschieden und es hatte Auseinandersetzungen über das Sorgerecht gegeben. In der Vergangenheit war es zudem zu Strafanzeigen der Frau gegen ihren ehemaligen Ehemann wegen verschiedener Vorfälle gekommen. Alle entsprechenden Akten wurden beigezogen. Aus diesen Akten ergab sich dann auch, daß die Frau im Zusammenhang mit ihrer Scheidung suizidgefährdet und in einer Nervenklinik gewesen war. Hinzu kam eine Akte über ein lange zurückliegendes Warenhausdiebstahlsverfahren. Aufgrund all dieser Erkenntnisse hat die Staatsanwaltschaft dann beschlossen, keine Anklage zu erheben, sondern eine Einstellungsverfügung zu erlassen. Kurz vor dem förmlichen Erlaß dieser Einstellungsverfügung hat der Verteidiger des beschuldigten Mannes Akteneinsicht beantragt und auch die Informationen aus den beigezogenen Akten erhalten. Über ihn hat der Beschuldigte von diesen für das Opfer negativen Tatsachen Kenntnis erhalten. In der Folge, so hat die Betroffene glaubhaft vorgetragen, seien diese sensiblen Informationen aus ihrem Vorleben bei ihrer Arbeitsstelle bekanntgeworden. Sie könne dort nicht mehr leben, sie müsse ihre Lebensverhältnisse grundlegend ändern und umziehen.

Es stellt sich die Frage, ob in einem solchen Fall das Interesse des Beschuldigten an vollständiger Akteneinsicht wirklich in jedem Stadium des Verfahrens vor den Interessen des Opfers Vorrang haben muß. Sicher ist dieses Recht des Beschuldigten grundlegend wichtig. In einer Situation, in der die Einstellung des Verfahrens aber faktisch beschlossen ist, sind die Verteidigungsinteressen des Beschuldigten objektiv stark reduziert. Dennoch läßt die Formulierung des § 147 StPO hier wohl kaum einen Spielraum. Dies war jedenfalls die Wertung der zuständigen Generalstaatsanwaltschaft, die auf der Grundlage des Wortlauts des § 147 StPO eine Abwägung zwischen Verteidigungs- und Opferinteresse für völlig unzulässig hielt. Auch in diesem Zusammenhang wäre eine Verbesserung der Lage des Opfers nur durch eine Gesetzesänderung zu erreichen.

Die gesonderte Aufbewahrung von Unterlagen, z. B. in Sonderheften, würde ebenfalls eine Verbesserung des Opferdatenschutzes bewirken. Zum einen gibt es jetzt schon gesetzliche Regelungen, die eine gesonderte Aufbewahrung von Unterlagen vorsehen, beispielsweise § 68 Abs. 3 Satz 3 StPO, aber auch § 101 Abs. 4 Satz 1 StPO, wonach die Informationen über den Einsatz besonderer Observationsmittel unter den gleichen Voraussetzungen wie die in § 68 genannten Informationen über den gefährdeten Zeugen gesondert aufzubewahren sind. Dies gilt zumindest so lange, wie das Ermittlungsziel gefährdet ist bzw. wie hier eine besondere Geheimhaltungsbedürftigkeit besteht. Gleiches gilt für die Unterlagen über den Einsatz eines verdeckten Ermittlers nach § 110 b Abs. 2 StPO. Dieser Gedanke der gesonderten Aufbewahrung von Unterlagen zum Schutz besonderer Geheimhaltungsbedürfnisse ist der StPO also nicht fremd. Es ist auch darauf hinzuweisen, daß es sicherlich keiner gesetzlichen Grundlage bedarf, um die Aktenordnung insoweit zu ändern, daß solche Informationen, die geeignet sind, das Opfer besonders zu gefährden, gesondert aufbewahrt werden müssen. Beispielsweise existiert in Hessen eine Verwaltungsvorschrift im Justizbereich, die vorsieht, daß die bereits erwähnten psychologischen Gutachten über Opfer und Zeugen, aber auch über Beschuldigte in einem besonderen Aktenheft aufbewahrt werden müssen. Dies hat die erwünschte Folge, daß auch nach Abschluß des Strafverfahrens, wenn verschiedene Stellen Interesse an einer Einsichtnahme in die Akte bekunden, jeweils gesondert zu entscheiden ist, ob auch diese besonders schutzbedürftigen Teile übersandt werden müssen. In Rheinland-Pfalz existiert solch eine Regelung noch nicht.

Eine weitere Maßnahme zum Schutz der Opferzeugen ist die Vernehmung in Abwesenheit des Beschuldigten. Dies bedeutet, daß zunächst staatsanwaltschaftliche statt richterliche Vernehmungen durchgeführt werden sollten, denn bei den richterlichen Vernehmungen hat der Beschuldigte ein Anwesenheitsrecht nach § 168 c StPO, bei den staatsanwaltschaftlichen Vernehmungen gilt dies wohl nicht in gleichem Umfang, bei polizeilichen Vernehmungen gibt es kein solches Anwesenheitsrecht. Auch dies wäre ein Gesichtspunkt, unter dem in der Praxis mehr als in der Vergangenheit auf Interessen des Opfers geachtet werden könnte.

Abschließend sind noch andere Gesichtspunkte des Opferdatenschutzes zu erwähnen:

Zunächst zum Problem der Wahrung der ärztlichen Schweigepflicht bei Zeugen und Opfern: Das generelle Beschlagnahmeverbot von ärztlichen Unterlagen gilt – jedenfalls nach der h. M. (OLG Celle, NJW 65, 362 f m. w. N.) – nur dann, wenn diese ärztlichen Unterlagen den Beschuldigten betreffen. Hier gibt es einen Wertungswiderspruch, der nur schwer erträglich ist. Die den Beschuldigten betreffenden ärztlichen Unterlagen dürfen ohne seine Zustimmung nicht beschlagnahmt werden. Insofern gilt vorrangig der Schutz der ärztlichen Schweigepflicht. Wenn die ärztlichen Unterlagen das Opfer betreffen, gilt dieser Vorrang der ärztlichen Schweigepflicht nicht. Dann haben die Interessen des Opfers zurückzustehen. In diesem Zusammenhang ist auf einen Beschluß des Landgerichts Hamburg (NJW 90, 780) hinzuweisen, in dem ausgeführt wird, auch hier müßten im Lichte der Entwicklung des informationellen Selbstbestimmungsrechts die Interessen des Opfers betont werden. Auch für das Opfer gelte ein entsprechendes Beschlagnahmeverbot, das heißt, ärztliche Unterlagen dürften nur mit Zustimmung des Opfers für das Strafverfahren genutzt werden. Allerdings sind auch die Gegenargumente in diesem Zusammenhang einzubeziehen: Dann entstünde ein Wertungswiderspruch insofern, als das Opfer sogar zwangsweise einer körperlichen Untersuchung unterzogen werden kann, wenn diese Untersuchung zu Beweiszwecken erforderlich ist. Dennoch ist der als Ausgangspunkt geschilderte Wertungswiderspruch kaum zu akzeptieren, wonach der Beschuldigte in bezug auf seine ärztlichen Unterlagen stärker geschützt wird als das Opfer.

Aus datenschutzrechtlicher Sicht ist ein weiterer Bereich erwähnenswert, der auch Opferschutzorganisationen als Adressaten datenschutzrechtlicher Anforderungen betrifft. So erfolgen im Rahmen des Täter-Opfer-Ausgleichs Datenübermittlungen, wobei in diesem Stadium des Verfahrens der Beschuldigte wohl kaum noch Informationen erfahren wird, die er vorher nicht schon hatte. Dennoch sind Datenübermittlungen in diesem Zusammenhang dann nicht ganz unproblematisch, wenn in diesen Täter-Opfer-Ausgleich private Organisationen eingeschaltet werden und die Opfer in entsprechende Übermittlungen nicht eingewilligt haben.

Nach dem Jugendgerichtsgesetz wird der Täter-Opfer-Ausgleich im Regelfall vom Jugendamt durchgeführt. Auch die Übermittlungen an das Jugendamt in diesem Zusammenhang sind nicht unproblematisch, wenn hier zu weitgehend Akteninhalte weitergegeben werden.

Aus datenschutzrechtlicher Sicht sind diese Gesichtspunkte im Zusammenhang mit dem Täter-Opfer-Ausgleich auch deshalb im Blick zu behalten, weil diese Maßnahmen künftig verstärkt durchgeführt werden sollen: Als fortgeltendes Recht der DDR gibt es die Möglichkeit hierzu jedenfalls in den neuen Bundesländern; im Verbrechensbekämpfungsgesetz ist ebenfalls vorgesehen, den Täter-Opfer-Ausgleich auszuweiten.

In Rheinland-Pfalz ist der EDV-Einsatz bei den Staatsanwaltschaften schon vergleichsweise weit fortgeschritten. Hier werden die UJS-Register bei den Staatsanwaltschaften bereits automatisiert geführt, allerdings nicht landesweit vernetzt, sondern jeweils beschränkt auf den Bereich der einzelnen Staatsanwaltschaften. Die damit einhergehende Gefährdung in bezug auf die Opferdaten hält sich damit also noch in Grenzen, ist aber im Blick auf die Absicht künftiger Vernetzung grundsätzlich bedeutsam.

Aus der Sicht des Datenschutzes sind demnach folgende Defizite zu beklagen:

- Das Verhältnis Beschuldigter/Verteidiger ist aufgrund der derzeitigen Rechtslage in bezug auf den Opferdatenschutz unbefriedigend geregelt.
- Auch für die Angabe der Wohnanschrift des Opfers wären gesetzliche Klarstellungen nützlich, zumindest in der Hinsicht, daß die Wohnortangabe nicht die Angabe der genauen Anschrift umfaßt.
- § 147 StPO sollte mit dem Ziel ergänzt werden, bei der Gewährung von Akteneinsicht für den Beschuldigten zumindest dann eine Abwägung mit Opferinteressen zu ermöglichen, wenn die Einstellung des Verfahrens beabsichtigt ist.
- § 174 Abs. 3 GVG sollte auf das gesamte Strafverfahren erweitert werden, mit der Möglichkeit, Geheimhaltungsverpflichtungen auch außerhalb der Durchführung von Hauptverhandlungen aufzuerlegen.
- In automatisierten Systemen sind Opferdaten besonders zu schützen.

7.9 Die private Nutzung dienstlicher DV-Geräte durch Justizbedienstete oder: Wie weit darf die Dienstbehörde dem Bediensteten unbemerkt ins Private folgen?

Das Ministerium der Justiz hielt es für erforderlich, die Nutzung dienstlicher EDV-Anlagen (PCs, Textverarbeitungssysteme) durch die Bediensteten zu deren privaten Zwecken zu regeln. Grundsätzlich wird das Recht auf eine solche Nutzung von einer Genehmigung des Behördenleiters abhängig gemacht. Dieser sowie die jeweils zuständigen DV-Stellen der Oberlandesgerichte, der Generalstaatsanwaltschaften, der JVA Diez und der EDV-Projektgruppe des Ministeriums der Justiz sind berechtigt, die private Nutzung und die verarbeiteten Daten zu überprüfen.

Eine solche Überprüfung, insbesondere der zu privaten Zwecken gespeicherten Daten, dürfte zwangsläufig mit einer Erhebung personenbezogener Daten der betroffenen Bediensteten einhergehen. Auf Anregung des LfD hat das Ministerium der Justiz dankenswerterweise deshalb folgende datenschutzrechtliche Konkretisierungen vorgenommen:

Es hat bestimmt, daß Daten, die im Rahmen dieser Überprüfung zur Kenntnis genommen worden sind, durch die prüfende Stelle nur zum Zweck der Überwachung der Einhaltung dieser Dienstanweisung und für die sich daraus notwendig ergebenden Folgerungen genutzt werden dürfen.

Außerdem hat es geregelt, daß der betroffene Bedienstete spätestens nach Abschluß der Kontrolle über die erfolgten Kontrollmaßnahmen, in deren Verlauf von ihm gespeicherte personenbezogene Daten zur Kenntnis genommen wurden, informiert werden soll.

Diese Regelungen, insbesondere auch die genannten – aus datenschutzrechtlicher Sicht wesentlichen – Restriktionen werden an Bedeutung gewinnen, wenn die Verlagerung dienstlicher Tätigkeiten in den häuslichen Bereich unter Nutzung von EDV (home-working) zunehmen wird. Sie könnten Vorbild für entsprechende Regelungen außerhalb des Justizressorts sein.

7.10 Strafvollzug

7.10.1 Das Strafvollzugsgesetz läßt die Datenschutzfragen noch immer ungeregelt

Zu dem Thema der fehlenden bereichsspezifischen Datenschutzregelungen für den Strafvollzug ist in Fortsetzung einer von der DSK begründeten Tradition – wie schon in den vorangegangenen Tätigkeitsberichten – wiederum darauf hinzuweisen, daß ein Fortgang nicht zu erkennen ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat erneut und dringlich auf dieses Defizit in ihrem Beschluß vom 25. August 1994, der als Anlage abgedruckt ist, aufmerksam gemacht (Beschluß der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu fehlenden bereichsspezifischen gesetzlichen Regelungen bei der Justiz, Anlage 13).

7.10.2 Anstaltsöffentlicher Ausruf mit Nennung des Anlasses

Als Beispiel für eine Eingabe aus dem Bereich des Strafvollzugs soll folgender Fall kurz erwähnt werden: Ein Gefangener hat sich darüber beschwert, daß häufig Gefangene anstaltsintern ausgerufen werden würden. Sie würden per Lautsprecher zum Anstaltsleiter, zum Besucherraum oder zur Poststelle gerufen, wobei für jeden Gefangenen und jeden sonst in der Anstalt Anwesenden der Anlaß des Ausrufens deutlich würde. Es könne dann dazu kommen, daß Mithäftlinge dieses Wissen (etwa über den Paketempfang) ausnutzen könnten. Die betroffene Justizvollzugsanstalt (JVA) hat zugesichert, künftig ein Verfahren zu wählen, bei dem der Anlaß des Ausrufens nicht bekannt gemacht wird.

7.10.3 Dürfen Standesamtsbücher in der JVA gebunden werden?

Eine Verbandsgemeinde unterbreitete dem LfD folgende Frage:
Seit vielen Jahren würden Buchbindearbeiten für die Gemeinde in der JVA durchgeführt. U.a. würden auch Personenstandsbücher mit Heirats-, Sterbe- und Geburtsregistern sowie die Sitzungsprotokolle des Gemeinderats und seiner Ausschüsse gebunden. Da die Arbeiten – worauf die beauftragte JVA nochmals ausdrücklich hingewiesen habe – durch Strafgefangene durchgeführt würden, erbat sie Auskunft, ob die Inanspruchnahme der JVA in dem genannten Bereich aus datenschutzrechtlicher Sicht zulässig sei.

Der LfD hat diese Frage wie folgt beurteilt:
Bei den Buchbindearbeiten handelt es sich um „Hilfstätigkeiten bei der Datenverarbeitung", die im Rahmen einer Auftragsdatenverarbeitung nach § 4 LDSG durchgeführt werden. Nach Absatz 2 der genannten Vorschrift besteht eine Verpflichtung zur sorgfältigen Auswahl der auftragnehmenden Person oder Stelle. In Wahrnehmung dieser Verpflichtung sind einerseits die schutzwürdigen Belange der Betroffenen, andererseits die Zuverlässigkeit der beim Auftragnehmer Beschäftigten zu berücksichtigen.

Eintragungen in Personenstandsregister sind nicht selten außerordentlich sensitiv. Zu denken ist beispielsweise an verdeckte Adoptionen oder an Geschlechtsumwandlungen, die hier dokumentiert sind. Von der Zuverlässigkeit der Strafgefangenen, die bei derartigen Arbeiten eingesetzt werden, kann sicherlich nicht ohne weiteres ausgegangen werden. Sie befinden sich in keinem Beschäftigungsverhältnis, haben bei Datenschutzverstößen also keine dienst- oder arbeitsrechtlichen Folgen zu gewärtigen, sind keine Amtsträger und demnach durch § 203 Abs. 2 StGB nicht strafbedroht und auch die Strafbestimmungen des LDSG (§ 35) wären nur dann anzuwenden, wenn eine unzulässige Verwendung von Daten in Bereicherungs- oder Schädigungsabsicht erfolgte.

Im Ergebnis hat der LfD davon abgeraten, in der Justizvollzugsanstalt Personenstandsbücher binden zu lassen.

Diese Überlegung wird auch gestützt durch die Entscheidung des Ministeriums der Justiz, zur Wahrnehmung von Hilfstätigkeiten im Verwaltungsbereich von Justizvollzugsanstalten des Landes grundsätzlich keine Gefangenen einzusetzen, wenn sie hierbei Kenntnis von personenbezogenen Daten erlangen können.

Sitzungsprotokolle sind sicherlich von geringerer Sensitivität; hier dürften – soweit öffentliche Sitzungen betroffen sind – die Überlegungen zur Zuverlässigkeit der Strafgefangenen kein entscheidendes Hindernis für die Wahrnehmung von Hilfstätigkeiten bei der Datenverarbeitung ergeben.

8. Schulen, Hochschulen, Wissenschaft

8.1 Zentrale Vorgaben für die automatisierte DV in Schulen fehlen

Aus der Sicht des LfD ist es unabdingbar, den Schulverwaltungen eine Handreichung zum Thema Datenschutz und Datensicherheit beim Einsatz von Arbeitsplatzrechnern zur Verfügung zu stellen. Im November 1993 hat das zuständige Ministerium einen entsprechenden Entwurf vorgelegt, zu dem der LfD im Dezember 1993 Anregungen, Änderungen und Ergänzungen vorgeschlagen hat. Diese wurden inhaltlich weitgehend akzeptiert, so daß die Veröffentlichung im Frühjahr 1994 hätte erfolgen können. Bis heute warten die Schulen allerdings auf diese für die Praxis notwendige Arbeitshilfe vergeblich.

Die Gründe für die Verzögerung sind nicht bekannt. Was auch immer die Ursachen sind: Der LfD bedauert das Ergebnis und hofft, daß diese Klage im nächsten Tätigkeitsbericht nicht mehr erhoben werden muß.

8.2 Schulverwaltungsprogramm COSIS/ISCO

Für den Einsatz an rheinland-pfälzischen Schulen wurde im Auftrag des Ministeriums für Bildung, Wissenschaft und Weiterbildung das Verfahren COSIS entwickelt. Nach mehrfachen Änderungen und einem Wechsel der entwickelnden Stelle wird das Verfahren unter der Bezeichnung ISCO in einem Schulversuch erprobt. Das Programm ISCO soll den rheinland-pfälzischen Schulen kostenlos zur Verfügung gestellt werden, der Zeitpunkt der Einführung ist jedoch noch offen.

Der LfD Rheinland-Pfalz hat im Rahmen seiner Beteiligung am Verfahren ISCO entsprechende Empfehlungen ausgesprochen. Diese betrafen neben der Begrenzung des vorgesehenen Datenumfangs Fragen der Zugriffskontrolle, der Absicherung der eingesetzten Arbeitsplatzrechner, der Auswertungsmöglichkeiten, der Protokollierung, der Löschungszeitpunkte sowie des Datenaustausches mit dem Statistischen Landesamt für Zwecke der Schulstatistik. Die Empfehlungen des LfD sollen bei der weiteren Entwicklung des Verfahrens berücksichtigt werden.

Die steigenden Anmeldezahlen für andere Schulverwaltungsprogramme zum Datenschutzregister zeigen, daß in diesem Bereich ein entsprechender Bedarf vorhanden ist. Aus der Sicht des LfD ist beim Einsatz derartiger Programme ein ausreichender technisch-organisatorischer Datenschutz sicherzustellen. Neben der Forderung nach einer Information der Schulleitungen (vgl. Tz. 8.1) bedingt dies die Berücksichtigung entsprechender Maßnahmen in den o. g. Bereichen. Die vorliegenden Erkenntnisse zeigen, daß diese bei den eingesetzten Programmen nicht in jedem Fall unterstützt werden.

Soweit die ausgesprochenen Empfehlungen umgesetzt werden, wäre es aus der Sicht des LfD wünschenswert, den Schulen, die einen entsprechenden Bedarf artikulieren, ISCO baldmöglichst zur Verfügung zu stellen, um dem Einsatz von Programmen, welche die datenschutzrechtlichen Anforderungen nur unzureichend berücksichtigen, zu begegnen.

8.3 Verfahren zur Lernmittelfreiheit im Schuljahr 1994/1995

8.3.1 Rechtsänderungen durch die Landesverordnung vom 8. April 1994, Gestaltung der Antragsunterlagen

Aufgrund einer Eingabe ist der LfD auf folgende Umstände aufmerksam geworden:

Das seinerzeit mit der DSK im einzelnen abgestimmte Verfahren zur Beantragung von Lernmittelfreiheit (vgl. 12. Tb. Tz. 10.1.2.2) wurde mit dem Schuljahr 1994/1995 aus datenschutzrechtlicher Sicht wesentlich geändert. In der nunmehr in Kraft gesetzten Landesverordnung ist geregelt, daß Nachweise der Antragsteller nicht mehr nur im Einzelfall aufgrund einer Ermessensentscheidung des Schulträgers, sondern grundsätzlich im Regelfall beizufügen sind.

Der LfD hätte es begrüßt, wenn er über die Absicht, die genannte Verordnung in dieser datenschutzrechtlich bedeutsamen Frage zu ändern, bereits im Vorfeld informiert worden wäre. Unabhängig hiervon hat er in den Antragsformularen bzw. auf dem beigefügten Informationsblatt die Angabe der Rechtsgrundlage für die Erhebung der in diesem Zusammenhang erforderlichen Daten vermißt. Die Pflicht zu einer solchen Information der Betroffenen folgt aus § 5 Abs. 2 LDSG.

Das zuständige Ministerium hat die Unterlassung eingeräumt und zugesagt, die Formulare künftig zu ergänzen.

8.3.2 Verfahren bei staatlich anerkannten Privatschulen

Ein wesentlicher Fortschritt aus datenschutzrechtlicher Sicht war die als Ergebnis einer intensiven öffentlichen Diskussion getroffene Festlegung, daß die Schulen und schulische Bedienstete keine Kenntnis von den Einkommensverhältnissen der Eltern erhalten, sondern daß ausschließlich die Schulträger (in erster Linie also die Schulämter der Kommunen) die Antragsbearbeitung vornehmen.

Bei den Privatschulen ist dies teilweise auf Schwierigkeiten gestoßen. Den LfD haben Eingaben von Eltern erreicht, die erklärten, sie hätten für ihre Kinder, die ein privates staatlich anerkanntes Gymnasium besuchen, Anträge auf Lernmittelfreiheit gestellt. Diese Anträge mit den entsprechenden Einkommensnachweisen würden vom Schulsekretariat des Gymnasiums bearbeitet. Auf ihre Frage sei ihnen erklärt worden, der Schulträger, der von Gesetzes wegen für die Bearbeitung zuständig sei, habe die Bearbeitung der Anträge an das Schulsekretariat delegiert.

Damit wäre im Bereich dieser privaten staatlich anerkannten Gymnasien ein Zustand eingetreten, der vor einigen Jahren bereits zu intensiven datenschutzrechtlichen Diskussionen geführt hat und der durch das derzeit gewählte Verfahren bei staatlichen Schulen verhindert wird.

Dies ist aus datenschutzrechtlicher Sicht nur dann akzeptabel, wenn eine andere Verfahrensweise nicht möglich ist. Die Schule sollte solche Daten grundsätzlich nicht zur Kenntnis erhalten, schon um jedem Anschein die Grundlage zu entziehen, daß sie zweckentfremdet werden könnten.

Vor diesem Hintergrund hat der LfD das zuständige Ministerium um Auskunft ersucht, ob die privaten staatlich anerkannten Gymnasien insoweit der staatlichen Rechtsaufsicht unterliegen und ob dort eine Möglichkeit gesehen werde, das datenschutzrechtliche Anliegen in diesem Zusammenhang zu fördern.

Das Ministerium hat zwar die Frage, ob es aufsichtlich tätig werden könne, verneint. Es hat aber gleichwohl die privaten Schulen wiederholt gebeten, wie die staatlichen Stellen zu verfahren. Der LfD hat die Beschwerdeführer ergänzend an den im konkreten Fall zuständigen kirchlichen Datenschutzbeauftragten verwiesen.

8.4 Dürfen die Schulen den BAföG-Ämtern die Schulabbrecher melden?

Es ist die Frage problematisiert worden, ob die berufsbildenden Schulen jeden Schulabbrecher an das zuständige Amt für Ausbildungsförderung melden dürfen bzw. ob sie jeden Schulabbrecher, der eine Schulbesuchsbescheinigung erhalten hat, diesen Ämtern melden dürfen.

Problematisch ist die Angelegenheit deshalb, weil nur ein bestimmter Prozentsatz derjenigen Schüler, die eine Schulbesuchsbescheinigung zum Zweck der BAföG-Beantragung erhalten und BAföG-Leistungen beantragen, tatsächlich auch BAföG-Mittel beziehen. Die Höhe dieses Prozentsatzes ist streitig; die Schätzungen schwanken zwischen 10 und 50 %.

Vor diesem Hintergrund hat es der LfD für angemessen gehalten, daß die Ämter für Ausbildungsförderung den Schulen die Namen derjenigen Schüler mitteilen, die tatsächlich BAföG-Leistungen beziehen.

Nunmehr ist diese Frage in anderem Sinn gesetzlich geregelt worden: In das BAföG (§ 47 Abs. 3) wurde eine neue Vorschrift eingefügt, die sinngemäß wie folgt lautet: Ist dem Auszubildenden von einer Ausbildungsstätte für Zwecke der BAföG-Beantragung bescheinigt worden, daß er sie besucht, so unterrichtet die Ausbildungsstätte das Amt für Ausbildungsförderung unverzüglich, wenn der Auszubildende die Ausbildung abbricht.

Durch diese Regelung wird zwar nicht verhindert, daß überflüssige Datenübermittlungen mit sensiblen Informationen erfolgen – überflüssig sind nämlich die Übermittlungen über den Ausbildungsabbruch derjenigen Schüler, die BAföG zwar beantragt haben, aber dennoch keine Leistungen beziehen. Auf der Ebene des Bundes war aber keine datenschutzfreundlichere Regelung erreichbar. Der LfD verkennt auch nicht die tatsächlichen Probleme, die entstünden, wenn den Schulen die Listen der tatsächlich BAföG-Leistungen in Anspruch nehmenden Schüler von den BAföG-Ämtern übermittelt werden müßten.

8.5 Die Berufung eines neuen Schulleiters unter Beteiligung der Presse

Aufgrund einer Eingabe ist der LfD auf folgenden Vorgang aufmerksam geworden: Der Rat einer Verbandsgemeinde hat im Verfahren zur Herstellung des Benehmens bei der Besetzung der Schulleiterstelle der örtlichen Grundschule in öffentlicher Sitzung beraten, ob der Vorschlag der Bezirksregierung, die Leitung der Grundschule einem bestimmten Lehrer zu übertragen, akzeptiert werden kann. Das Ergebnis der Beratungen hat die Verbandsgemeinde in ihrem amtlichen Mitteilungsblatt unter Nennung der Namen der betroffenen Bewerber veröffentlicht. Außerdem wurde aufgrund der öffentlichen Sitzung in der Presse ausführlich auch unter der Nennung des Namens des Beschwerdeführers über diese Angelegenheit berichtet.

Der LfD vertritt die Auffassung, daß es sich hier um eine Personalangelegenheit gehandelt hat, die in nichtöffentlicher Sitzung zu beraten war. Entsprechend hätte auch keine Veröffentlichung erfolgen dürfen. Der LfD hat sowohl die Beratung über die Herstellung des Benehmens bei der Besetzung der Schulleiterstelle in öffentlicher Sitzung als auch die entsprechende Veröffentlichung im amtlichen Mitteilungsblatt der Verbandsgemeinde als Verstoß gegen datenschutzrechtliche Vorschriften beanstandet.

8.6 Das neue Universitätsgesetz

Drei unterschiedliche Fragenkomplexe hatten im Zusammenhang mit der Verabschiedung des Universitätsgesetzes besondere datenschutzrechtliche Bedeutung:

a) Werden im Zusammenhang mit der Erstellung von Lehrberichten personenbezogene oder personenbeziehbare Daten (gff. durch welche Stelle) erhoben, gespeichert und veröffentlicht (s. hierzu 8.5.1.)?

b) In welchem Umfang haben die neu zu bestellenden Frauenbeauftragten an den Universitäten sowie die ihnen zugeordneten Ausschüsse für Frauenfragen das Recht, personenbezogene Daten von Bewerbern sowie Betroffenen bei Personalmaßnahmen zu erheben, zu speichern und zu übermitteln (s. hierzu 8.5.2.)?

c) Ist es geboten, die Erhebung und Verarbeitung von Studentendaten durch die Universitäten nicht nur im Rahmen einer Ermächtigungsgrundlage für den Erlaß von Einschreibeordnungen, sondern durch eine gesonderte normenklare Regelung im Universitätsgesetz selbst einer Lösung zuzuführen (s. hierzu 8.5.3.)?

8.6.1 Lehrberichte

Auf Anregung des LfD ist die Regelung eingefügt worden, daß die Hochschule für ihre Aufgaben in der Lehre die Studierenden anonym über die Art und Weise der Vermittlung von Lehrinhalten in den Lehrveranstaltungen befragen und die gewonnenen Daten verarbeiten darf. Soweit sie Namen von Lehrenden enthalten, dürfen die Ergebnisse nur hochschulöffentlich mitgeteilt werden (§ 20 Abs. 3 Universitätsgesetz). Zu der hier bestehenden Frage des Eingriffs in die grundgesetzlich geschützte Lehrfreiheit der Professoren hat sich der LfD bewußt nicht geäußert: diese Frage liegt außerhalb seines Zuständigkeitsbereichs. Aus datenschutzrechtlicher Sicht hat er diese Regelung akzeptiert: Bei den Daten über die Lehrpersonen handelt es sich grundsätzlich um Informationen, die universitätsöffentlich sind. Sie betreffen zudem die Amtsausübung des Lehrpersonals. Vor diesem Hintergrund ist eine gesteigerte datenschutzrechtliche Schutzbedürftigkeit nicht festzustellen. Die Anwendung des allgemeinen verfassungsrechtlichen Erforderlichkeitsgrundsatzes in diesem Zusammenhang dürfte dem Schutzbedürfnis der Betroffenen genügen.

8.6.2 Datenerhebungsbefugnisse und weitere Regelungen zur Datenverarbeitung durch Frauenbeauftragte und Ausschüsse für Frauenfragen

Der LfD hat folgende gesetzliche Regelungen vorgeschlagen:

- Verbot der Speicherung personenbezogener Daten bei der Frauenbeauftragten und dem Ausschuß für Frauenfragen; zumindest sollten solche Speicherungen nur in Ausnahmefällen und nur mit Zustimmung der Betroffenen zulässig sein.
- Auch unter diesen Voraussetzungen sollten Unterlagen über konkrete Personalmaßnahmen unmittelbar nach Bestandskraft der Maßnahme vernichtet werden; entsprechende Daten in automatisierten Verfahren wären zu löschen. Für die Ausschüsse für Frauenfragen sollte Entsprechendes gelten.
- Soweit durch die Frauenbeauftragten personenbezogene Bedienstetendaten gespeichert werden, sollten hierfür ergänzend die Regelungen des Landesbeamtengesetzes über die Führung von Personalakten (§§ 102 bis 102 g LBG) für anwendbar erklärt werden.

Diese Vorschläge sind in § 67 Abs. 5 Universitätsgesetz übernommen worden.

8.6.3 Bereichsspezifische Regelung der Verarbeitung personenbezogener Studentendaten

Die Verlagerung der Regelungsbefugnis auf die Hochschulen im Wege der Ermächtigung in § 63 Abs. 3 Hochschulgesetz hatte sich als wenig wirksam erwiesen. Die Hochschulen waren in diesem Zusammenhang offensichtlich im Regelfall nicht im erforderlichen Maße sensibilisiert und informiert, um diese Ermächtigung sachangemessen auszufüllen. Die auf dieser Basis ergangenen Regelungen der Einschreibeordnungen beschränkten sich vielmehr allzu häufig auf generalklauselartige allgemeine Bestimmungen. Eine Abkehr von dem Weg, gesetzlich nur einen Regelungsauftrag in einer Ermächtigungsvorschrift für die Einschreibeordnungen der Hochschulen vorzugeben, erschien dem LfD auch unter dem Gesichtspunkt sachangemessen, daß die Einschreibeordnungen nur für einen Teil der hier regelungsbedürftigen Datenverarbeitungsvorgänge der richtige Ort sein

können: Die Einschreibeordnungen regeln das Verfahren zur Einschreibung sowie den Umfang der bei der Einschreibung erhobenen Daten und deren hochschulinterne Verwendung. Folgende Bereiche werden davon nicht umfaßt:

- Erhebung und Verwendung von Daten außerhalb des Einschreibeverfahrens, im Verlauf des Studiums;
- Verwendung von Daten zu Zwecken außerhalb der universitären Aufgaben.

Entsprechend dieser Überlegungen wurde in § 63 Abs. 4 Universitätsgesetz eine Rechtsverordnungsermächtigung aufgenommen, die das Wissenschaftsministerium verpflichtet, datenschutzrechtliche Regelungen in Ergänzung der Einschreibeordnungen zu treffen.

8.7 Datenschutz in Netzen: Wer ist bei der Betreibung eines Netzes durch die verfaßte Studentenschaft verantwortlich?

Für die Informationen, die in einem Netz angeboten werden, ist in datenschutzrechtlicher Hinsicht die speichernde Stelle verantwortlich. Dies ist der Anbieter von Informationen. Der Netzbetreiber dürfte hier als dessen Auftragnehmer anzusehen sein, der eine Serviceleistung für die anbietende Person oder Stelle (User), die als speichernde Stelle im rechtlichen Sinn anzusehen ist, erbringt. Der Auftragnehmer (Netzbetreiber) hat im allgemeinen keine eigene Verantwortung für die datenschutzrechtliche Zulässigkeit der Datenverarbeitungen, die der Auftraggeber (User) veranlaßt. Wenn allerdings eine öffentliche Stelle ein Netz betreibt oder dieses Netz zur Nutzung anbietet – dies geschähe hier durch die verfaßte Studentenschaft –, dann gilt folgendes:

Das Netz darf nur für solche Aktivitäten genutzt werden, die der Aufgabe der betreibenden öffentlichen Stelle (der verfaßten Studentenschaft) entsprechen. Die Aufgaben der verfaßten Studentenschaft ergeben sich aus § 106 Hochschulgesetz. Danach nimmt die Studentenschaft Angelegenheiten der ihr angehörenden Studenten wahr. Ihr obliegt es, die fachlichen, wirtschaftlichen und sozialen Interessen der Studenten zu vertreten, zu hochschulpolitischen Fragen Stellung zu nehmen, die Studenten bei der Durchführung des Studiums zu beraten, die kulturellen Anliegen der Studenten zu fördern, die überregionalen und internationalen Studentenbeziehungen zu pflegen, den Studentensport zu fördern. Es fällt schwer, die Betreibung eines Informationsnetzes unter eine dieser enumerativ gesetzlich aufgezählten Aufgaben zu subsumieren. Selbst wenn dies möglich wäre, müßten sich aber auch die das Netz nutzenden Personen oder Stellen auf die Verfolgung der genannten Zwecke beschränken. Insoweit obliegt dem Netzbetreiber – der verfaßten Studentenschaft – sicherlich eine Prüfungspflicht, alle diejenigen User aus dem Netz auszuschließen, die hiervon abweichende Ziele verfolgen.

Ein weiteres Problem entsteht dadurch, daß im vorliegenden Fall eine öffentliche Stelle als Netzbetreiber für Private auftritt: Dies ist der Fall, weil wohl vorgesehen ist, daß Privatpersonen oder private Vereinigungen das Netz der verfaßten Studentenschaft nutzen können. Öffentliche Stellen dürfen nicht dazu beitragen, daß rechtswidrige Handlungen Privater begangen werden. Sie haben jedenfalls das ihnen Mögliche dazu beizutragen, daß solche rechtswidrigen Handlungen unterbleiben. Dies ergibt sich letztlich aus dem Prinzip der Gesetzmäßigkeit der Verwaltung und dem Rechtsstaatsprinzip (Artikel 20 Abs. 3 GG), es folgt aber auch schon aus § 4 Abs. 2 LDSG. Bei der Zurverfügungstellung von Kommunikationsnetzen ist dies sicherlich nicht durch die Prüfung jedes einzelnen Beitrages möglich; dieses Ziel kann jedoch durch vertragliche oder sonstige (durch eine Satzung oder eine Benutzungsordnung erfolgende) rechtlich wirksame Bindungen der Netzteilnehmer sowie durch gelegentliche Stichprobenprüfungen und wirksame Sanktionen gegenüber den Nutzern bei Zuwiderhandlungen erreicht werden. Die Prüfkompetenzen des Systemadministrators gegenüber den Netznutzern wären ebenfalls rechtlich verbindlich festzulegen.

Bei einem Kommunikationsnetz in Trägerschaft einer öffentlichen Stelle gehört auch eine angemessene Aufklärung der Nutzer über die datenschutzrechtlichen Schranken der Datenverarbeitung zu den Aufgaben des Netzbetreibers.

8.8 Krebsregister

Mit dem Inkrafttreten des Bundeskrebsregistergesetzes ist das rheinland-pfälzische Modell der Krebsregisterführung in wesentlichen Punkten bundesrechtlich vorgeschrieben worden: Die auf überregionaler Ebene zentrale Erfassung von Krebsfällen in einem Register, das zweigeteilt ist in eine Vertrauensstelle, die personenbezogene Daten erhält, aber nicht auf Dauer speichert, und eine Registerstelle, die nur anonymisierte Daten erhält und diese dauerhaft speichert, mit der Möglichkeit der Deanonymisierung unter Hinzuziehung einer dritten Stelle, die den Schlüssel für die Entschlüsselung der bei der Registerstelle „asymmetrisch" verschlüsselten Daten aufbewahrt (vgl. 14. Tb. Tz. 8.3).

In Rheinland-Pfalz arbeitet das Krebsregister des Tumorzentrums Mainz e. V. auf der Basis der Einwilligung der betroffenen Patienten (mit der Folge einer nur ca. 70prozentigen Erfassung der Krebsfälle) seit mehreren Jahren nach diesen Vorgaben. Die bundesgesetzlich vorgesehene Erfassung auch ohne Einwilligung kann erst dann praktiziert werden, wenn der Landesgesetzgeber zur Umsetzung des Bundesrechts ein Landesgesetz erlassen hat. Dafür gilt eine Frist bis zum 31. Dezember 1999 (§ 1 Bundeskrebsregistergesetz). Nach dem derzeitigen Erkenntnisstand wird die Landesregierung diese Frist weitgehend ausschöpfen.

Der LfD hat an verschiedenen beratenden Sitzungen einer Bund-Länder-Arbeitsgemeinschaft teilgenommen, die sich mit den praktischen Fragen der Umsetzung des Bundesgesetzes befaßt hat. Klärungsbedürftig aus datenschutzrechtlicher Sicht sind insbesondere folgende Einzelfragen:

- Wer soll schlüsselverwaltende Stelle für die Entschlüsselung sein?
- Nach welchen Kriterien soll welche Stelle über die Zulässigkeit einer Entschlüsselung entscheiden?
- Welche sicheren asymmetrischen Verschlüsselungsmethoden existieren?
- Wie ist die gebotene Unabhängigkeit der Registerstelle von der Vertrauensstelle organisatorisch zu erreichen?
- Welche Stelle ist für die Verfahrensentwicklung, insbesondere die Pflege des Verschlüsselungsverfahrens insgesamt, zuständig?

Diese und ähnliche Fragen werden im Gesetzgebungsverfahren des Landes zu klären sein.

8.9 Datenschutzfragen beim Kirchenaustritt

Der LfD wurde wiederholt um Stellungnahme gebeten, ob dann, wenn Kirchenaustritte im Pfarrblatt der Gemeinde veröffentlicht oder im Rahmen eines Jahresrückblicks von der Kanzel unter Namensnennung der Betroffenen bekanntgemacht werden, datenschutzrechtliche Vorschriften verletzt werden. Es wurde auch schon der Wunsch geäußert, daß der LfD die Kirchenbehörde und den tätig gewordenen Pfarrer darauf hinweisen sollte, derartige Veröffentlichungen künftig zu unterlassen.

Den genannten Anliegen konnte der LfD nicht entsprechen: Seine gesetzlich abschließend geregelte Zuständigkeit beschränkt sich auf die datenschutzrechtliche Kontrolle öffentlicher Stellen des Landes Rheinland-Pfalz (§ 24 Abs. 1 i. V. m. § 2 Abs. 1 LDSG).

Die großen Kirchen könnten zwar auch in ihrer Eigenschaft als öffentlich-rechtliche Körperschaften als „öffentliche Stelle" in diesem Sinn angesehen werden. Aus § 15 LDSG ergibt sich jedoch eindeutig, daß öffentlich-rechtliche Religionsgesellschaften keine öffentliche Stelle im Sinne des § 2 Abs. 1 LDSG sind. Dies entspricht auch der Verfassungsrechtslage: Der Staat darf in die inneren Verhältnisse der Kirchengemeinschaften nicht regelnd eingreifen. Dementsprechend haben die großen öffentlich-rechtlichen Religionsgemeinschaften eigene kirchenrechtliche Datenschutzregelungen erlassen.

Der LfD kann in diesen Fällen also nur empfehlen, sich an den zuständigen kirchlichen Datenschutzbeauftragten zu wenden.

Der Vollständigkeit halber sei aber zu den angesprochenen inhaltlichen Fragen auf ein Urteil des Amtsgerichts Landau verwiesen, das Schmerzensgeldansprüche eines Betroffenen mit beachtlichen Gründen zurückgewiesen hat (nicht veröffentlichtes rechtskräftiges Urteil des AG Landau, Zweigstelle Bad Bergzabern, vom 21. Dezember 1994, Az. C 354/94).

9. Umweltschutz

9.1 Umweltinformation im Verwaltungsverfahren – von der EU-Richtlinie zum Umweltinformationsgesetz

Das Umweltinformationsgesetz (UIG), dessen Entstehungsgeschichte im 14. Tätigkeitsbericht (Tz. 9.1) ausführlich erläutert wurde, ist am 16. Juli 1994 in Kraft getreten (BGBl. I, 1490 ff.). Es setzt die Richtlinie des Rates vom 7. Juni 1990 (90/313/EWG) über den freien Zugang zu Informationen über die Umwelt in deutsches Recht um. Der Anspruch auf Informationszugang steht nach § 4 UIG Bürgern und juristischen Personen des Privatrechts ohne Nachweis eines Interesses zu. Bei der Prüfung des Zugangsrechts spielt es deshalb keine Rolle, ob der Antragsteller ideelle oder kommerzielle Zwecke verfolgt und inwieweit es sich dabei um rechtlich geschützte Positionen handelt. Grundsätzlich wird mit dem UIG das Recht eines jeden geregelt, freien Zugang zu Informationen über die Umwelt zu erhalten, die bei einer Behörde oder bei natürlichen oder juristischen Personen des privaten Rechts geführt werden, die im Bereich des Umweltschutzes öffentlich-rechtliche Aufgaben wahrnehmen. Der Anspruch auf den freien Informationszugang besteht jedoch nicht unbeschränkt. So ist gem. § 8 Abs. 1 UIG ein Anspruch nicht gegeben, soweit durch das Bekanntwerden der Information personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt werden. Die Weitergabe von Umweltinformationen, die personenbezogene Angaben enthalten, stellt einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung aus Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 Grundgesetz dar. Der deutsche Gesetzgeber hat in diesem Zusammenhang von der Möglichkeit nach Artikel 3 Abs. 2, 5. Spiegelstrich der Richtlinie Gebrauch gemacht, wonach die Mitgliedstaaten vorsehen können, daß ein Zugangsantrag abgelehnt werden kann, wenn die Vertraulichkeit personenbezogener Daten berührt ist. Mit dem Begriff des Schutzes der Vertraulichkeit wird deutlich, daß die Richtlinie den Schutz personenbezogener Daten nicht schlechthin vorsieht. Vielmehr ist ein sachlich begründetes Geheimhaltungsinteresse erforderlich. Wann dieses vorliegt, läßt der Wortlaut der Bestimmung offen. So wird in § 8 Abs. 1 UIG die Umsetzung dieser gemeinschaftsrechtlich eröffneten Möglichkeit mittels einer Generalklausel vorgenommen. Die UIG-Regelung verpflichtet zur Abwägung im Einzelfall, ohne der Verwaltung dafür inhaltliche Maßstäbe bereitzustellen. Es bleibt abzuwarten, ob diese mangelnde Bestimmtheit die Lösung des Konflikts zwischen Informationsanspruch und Datenschutz erschweren wird.

9.2 Altablagerungs- und Altstandortkataster

Aufgrund örtlicher Feststellungen beim Landesamt für Umweltschutz und Gewerbeaufsicht (LfUG) hat sich folgendes ergeben:

Mit der Entwicklung des Altablagerungskatasters wurde eine Privatfirma beauftragt. Die nach § 26 Landesabfallwirtschafts- und Altlastengesetz (LAbfWAG) erforderliche Erhebung wurde in den Jahren 1986 bis 1989 durch verschiedene Ingenieurbüros durchgeführt. Für die Erfassung wurden die Erhebungsbögen an die Privatfirma übersandt und durch diese erfaßt. Nach der Erfassung wurden die Daten per Diskette an das LfUG übersandt. Die Daten waren auf der Diskette im Klartext abgelegt. Eine Verschlüsselung der Daten erfolgte nicht. Nach der Übernahme der erfaßten Daten durch das LfUG wurden die Daten an die jeweilige Bezirksregierung per Diskette übersandt. Auch bei dieser Versendung waren die Daten im Klartext abgelegt. Dies hatte zur Folge, daß bei einem Verlust der Diskette für Dritte die Möglichkeit bestanden hätte, die gespeicherten Daten zur Kenntnis zu nehmen. Um dies zu vermeiden, sollten – so die Forderung des LfD – künftig die Daten in verschlüsselter Form auf den Disketten gespeichert werden.

Das Altstandortkataster befand sich zum Zeitpunkt der örtlichen Feststellungen in der Phase der Programmierung. Mit der Entwicklung des Verfahrens wurde ebenfalls die oben erwähnte Privatfirma beauftragt.

Die dort getroffenen örtlichen Feststellungen gaben Anlaß, auf die datenschutzrechtlichen Anforderungen bei der Verarbeitung personenbezogener Daten im Auftrag hinzuweisen. Zu beachten ist, daß die auftraggebende Stelle gem. § 4 LDSG für die Einhaltung der Bestimmungen dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich ist, der Auftraggeber mithin „Herr der Daten" bleibt. Für die beim nichtöffentlichen Auftragnehmer beschäftigten Personen gilt das Datengeheimnis gem. § 5 BDSG, sofern sie bei der Verarbeitung personenbezogener Daten in den Phasen der Datenverarbeitung tätig sind. Nach Auffassung des LfD ist die Beschäftigung freier Mitarbeiter als Subunternehmer (im vorliegenden Fall waren es „Werkvertrags-Studenten") der Privatfirma problematisch, weil die Frage der Zuverlässigkeit nur schwer zu beurteilen ist. Bei Zuwiderhandlungen gegen datenschutzrechtliche Vorschriften stellen sich Haftungsfragen. Grundsätzlich sollte also bei der Erfassung und Verarbeitung sehr empfindlicher Daten keine Beschäftigung von Personen, die an den Auftragnehmer nicht arbeitsvertraglich gebunden sind, in Betracht kommen. Vorliegend war es unschwer vorstellbar, daß Eintragungen in die Kataster für die Betroffenen mitunter existenzgefährdend sein können.

Sofern die Bestimmungen des LDSG, wie im vorliegenden Fall, auf die auftragnehmende Person oder Stelle (Privatfirma) keine Anwendung finden, ist die auftraggebende Stelle nach § 4 Abs. 1 Satz 2 LDSG verpflichtet sicherzustellen, daß die auftragnehmende Person oder Stelle die Bestimmungen dieses Gesetzes beachtet und sich der Kontrolle des LfD unterwirft. Weiterhin hat der LfD klargestellt, daß bei künftigen Auftragsvergaben die auftragnehmende Person oder Stelle möglichst unter mehreren Anbietern unter besonderer Berücksichtigung der Eignung der von ihr getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen ist. Daraus folgt, daß der Auftragnehmer, um seine Dienstleistungen für die Verarbeitung und Nutzung personenbezogener Daten anbieten zu können, ein gesetzeskonformes Datensicherungskonzept ausarbeiten muß. Dieses hat er als Anbieter dem Auftraggeber vorzulegen. Liegt es bei der Auswahl nicht vor, verstößt der Auftraggeber gegen die vorgenannte, zwingende Vorschrift des § 4 Abs. 2 LDSG (fehlerhaftes Auswahlermessen). Der Auftraggeber hat sich vor der Auftragserteilung ggf. zu erkundigen, ob das Unternehmen in der Vergangenheit vergleichbare Aufträge ordnungsgemäß abgewickelt hat. Er hat weiter zu prüfen, ob sich die Organisation und die Einrichtung des Unternehmens für eine Datenverarbeitung der vorgesehenen Art eignen. Handelt es sich – wie im vorliegenden Fall – um ein nichtöffentliches Unternehmen, ist zu prüfen, ob der Auftragnehmer seiner Meldepflicht nach § 32 Abs. 1 Nr. 3 BDSG nachgekommen ist. In diesem Zusammenhang sollte das Aktenzeichen, unter dem die Datenverarbeitung bei der zuständigen Aufsichtsbehörde registriert worden ist, bekannt sein. Grundlage für die zu regelnden technischen und organisatorischen Maßnahmen und damit für das allgemeine Sicherungskonzept des privaten Auftragnehmers ist § 9 BDSG (im wesentlichen inhaltsgleich mit § 9 LDSG). Diese Vorschrift deckt zum einen umfassend alle gesetzlichen Anforderungen in diesem Bereich ab, die bei der Verarbeitung personenbezogener Daten zu beachten sind. Zum anderen leitet sich hieraus zugleich die Grundlage für die Prüfungstätigkeit der Aufsichtsbehörden ab.

9.3 Sonderabfallentsorgung in Rheinland-Pfalz

Am 1. Januar 1994 hat die in Mainz ansässige Sonderabfall-Management-Gesellschaft Rheinland-Pfalz GmbH (SAM) ihre Geschäftstätigkeit aufgenommen. Als „Zentrale Stelle" für Sonderabfälle übernimmt sie damit die Verantwortung für die rheinland-pfälzische Sonderabfallentsorgung.

Noch vor dem Inkrafttreten des neuen LDSG wurde der LfD mit der Frage befaßt, ob es zulässig ist, daß öffentliche Stellen personenbezogene Daten aus dem Bereich Abfallwirtschaft an die SAM GmbH übermitteln.

Maßgeblich war zunächst, ob die SAM GmbH im Sinne des Datenschutzrechts als öffentliche Stelle oder als eine Stelle außerhalb des öffentlichen Bereichs anzusehen ist. Die Gesellschafter der SAM sind die „Vereinigung privater Entsorgungsbetriebe der Sonderabfallentsorgung Rheinland-Pfalz GmbH" (VPE) mit einer Beteiligung am Stammkapitel von 25,1 Prozent, die

„Vereinigung mittelständischer Entsorgungsbetriebe der Sonderabfallentsorgung Rheinland-Pfalz GmbH" (VME) mit einer Beteiligung von 23,9 Prozent und das Land Rheinland-Pfalz mit einer Beteiligung von 51 Prozent. Dem Land Rheinland-Pfalz wurde an der SAM GmbH damit ein bestimmender Einfluß auf den Geschäftsbetrieb eingeräumt.

Der LfD hat für die Beantwortung der Frage, ob es sich bei der SAM GmbH um eine öffentliche Stelle im Sinne des Datenschutzrechts handelt, bereits die einschlägigen Bestimmungen des Gesetzentwurfs zur Novellierung des Landesdatenschutzgesetzes (LDatG-E) herangezogen. Mit der Neuregelung in § 2 Abs. 1 Satz 1 LDatG-E wurde deutlich, daß der Begriff der „öffentlichen Stelle" nicht nur für die öffentlich-rechtlich organisierten Stellen des Landes einschließlich ihrer Vereinigungen gelten soll, sondern auch für deren in Privatrechtsform errichtete juristische Personen oder Vereinigungen. Hierzu rechnen insbesondere auch in der Rechtsform einer Gesellschaft mit beschränkter Haftung (GmbH) geführte Einrichtungen. Gem. § 2 Abs. 1 Satz 2 LDatG-E sollten als öffentliche Stellen auch diejenigen juristischen Personen und sonstigen Vereinigungen des privaten Rechts gelten, an denen neben nichtöffentlichen Stellen die in Satz 1 genannten öffentlichen Stellen beteiligt sind, wenn ihnen allein oder gemeinsam mit anderen in Satz 1 genannten Stellen die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

Mithin hatte der LfD im vorliegenden Fall keine Bedenken, von einer Datenübermittlung an Stellen innerhalb des öffentlichen Bereichs im Sinne von § 6 LDatG auszugehen. Was die Erforderlichkeit anbelangte, waren die aufgrund der Verordnungsermächtigung in § 8 b Landesabfallwirtschafts- und Altlastengesetz (LAbfWAG) geschaffenen Regelungen des § 2 der Landesverordnung über die Andienung von Sonderabfällen vom 2. Dezember 1993 zu beachten. Danach werden der Zentralen Stelle (SAM GmbH) die Aufgaben übertragen, die der für die Entsorgungs- oder Verwertungsanlage zuständigen Behörde bei der Durchführung des Nachweisverfahrens über die Zulässigkeit der vorgesehenen Entsorgung oder Verwertung sowie bei der Durchführung des Nachweisverfahrens über entsorgte Abfälle oder verwertete Reststoffe nach der Abfall- und Reststoffüberwachungs-Verordnung vom 3. April 1990 obliegen, wobei Satz 1 des Abs. 2 auch für dem Nachweisverfahren unterliegende Abfälle gilt, die nicht andienungspflichtig sind. Fernerhin wurden der SAM GmbH gem. § 2 Abs. 3 der vorgenannten Verordnung die Aufgaben der zuständigen Behörde nach § 13 des Abfallgesetzes (AbfG) vom 27. August 1986 übertragen, soweit es sich um gefährliche Abfälle im Sinne des § 5 der Abfallverbringungsverordnung vom 18. November 1988 handelt.

Nach allem bestanden aus datenschutzrechtlicher Sicht keine Bedenken gegen die Datenübermittlung, soweit sie sich im Rahmen der Aufgabenübertragung nach § 2 der Landesverordnung über die Andienung von Sonderabfällen vom 2. Dezember 1993 bewegt.

9.4 Daten aus dem Ablagerungs- und Verdachtsflächenkataster

In einer Eingabe beklagte ein Naturschutzverband, daß ihm das Ministerium für Umwelt die erforderlichen Angaben für den Aufbau eines eigenen Ablagerungs- und Verdachtsflächenkatasters nicht zur Verfügung stelle. Für ihn sei es von Wichtigkeit, den genauen Standort der Altlasten- und Verdachtsflächen (mit Parzellen-Nr.) in Erfahrung zu bringen, um daraus das betroffene Grundstück ableiten zu können.

Der LfD hat dem Petenten klargemacht, daß es aus der Sicht des Datenschutzes um die Sicherung des Rechts auf informationelle Selbstbestimmung geht. So können umweltbezogene Informationen sensible personenbezogene Daten enthalten. Das Bundesverfassungsgericht hat in seiner grundlegenden Entscheidung zum Grundrecht auf informationelle Selbstbestimmung – Volkszählungsurteil – aus dem mit Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 Grundgesetz gewährleisteten Recht die Befugnis des einzelnen abgeleitet, über die Preisgabe und Verwendung seiner persönlichen Daten grundsätzlich selbst zu bestimmen. Eine Beschränkung dieses informationellen Selbstbestimmungsrechts ist nur bei überwiegendem Allgemeininteresse zulässig und bedarf einer verfassungsmäßigen gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem Rechtsstaatgebot der Normenklarheit entspricht. Einschränkungen des Rechts auf informationelle Selbstbestimmung sind zulässig, weil das Recht im Hinblick auf die Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person nicht schrankenlos gewährleistet ist. Die Frage, ob personenbezogene Umweltdaten offenbart werden dürfen, richtete sich im vorliegenden Fall nach den speziellen Regelungen im Abfallwirtschafts- und Altlastengesetz (LAbfWAG), das die Einrichtung und den Betrieb der angesprochenen Kataster regelt. Es handelt sich um Verzeichnisse, in denen unter Einsatz der automatisierten Datenverarbeitung unter anderem Informationen über Altablagerungen erfaßt und verarbeitet werden. Erfaßt werden auch die räumliche Lage einer Fläche und die gegenwärtige Nutzung. Dabei fallen personenbezogene Daten an; denn die gespeicherten Daten sind Einzelangaben über persönliche und sachliche Verhältnisse. Die Grundstücksbezogenheit führt in der Regel dazu, daß eine bestimmte oder bestimmbare natürliche Person betroffen ist. Die Daten fallen demzufolge in den Schutzbereich des Rechts auf informationelle Selbstbestimmung. Gemäß § 27 Abs. 2 LAbfWAG erstellt die zuständige Behörde (Bezirksregierung) für ihren Bezirk das Verdachtsflächen- und Altlastenkataster. Nach Absatz 5 dieser Regelung teilt sie die Tatsache der Aufnahme des Grundstücks in das Verdachtsflächen- und Altlastenkataster dem Grundstückseigentümer mit. Dem Nutzungsberechtigten und den Eigentümern von Nachbargrundstücken ist nach § 27 Abs. 6 LAbfWAG auf Antrag Auskunft über die im Verdachtsflächen- und Altlastenkataster gespeicherten Daten zu gewähren. An sonstige Behörden und Einrichtungen des Landes, der Gemeinden, der Kreise und kreisfreien Städte können Auskünfte aus diesem Kataster ausschließlich zur Wahrung der diesen Stellen auf dem Gebiet der Gefahrenermittlung, Ge-

fahrenabwehr, Überwachung und Planung gesetzlich obliegenden Aufgaben übermittelt werden. Der Naturschutzverband kam mithin als Übermittlungsempfänger nicht in Betracht; es sei denn, er wäre im Einzelfall Nutzungsberechtigter oder Eigentümer eines Nachbargrundstücks. Soweit Informationen der Öffentlichkeit zugänglich gemacht werden sollen, darf die Bekanntgabe nach der Regelung in § 27 Abs. 7 LAbfWAG keine personenbezogenen Daten enthalten.

Da es sich bei den gespeicherten Flächen um Verdachtsflächen handelt – es steht also gegenwärtig noch nicht fest, ob die Fläche letztlich als Altlast eingestuft wird – sind die schutzwürdigen Interessen der Grundstückseigentümer in den Vordergrund zu stellen. So können beispielsweise falsche Auskünfte über Grundstücke, bei denen sich im Laufe der Untersuchung herausstellt, daß es sich nicht um Altlasten handelt, unter Umständen für den Grundstückseigentümer oder Nutzungsberechtigten existenzgefährdend sein.

Schließlich sprachen aus Sicht des LfD auch praktische Überlegungen dagegen, dem Anliegen nachzukommen. Es darf nämlich nicht übersehen werden, daß damit ein Zweitkataster entstehen würde, das in sehr kurzer Zeit veraltete Informationen enthielte.

9.5 Auslagerung von Tätigkeiten an ein privates Unternehmen

Der Eigenbetrieb Abfallwirtschaft eines Landkreises hatte in Erwägung gezogen, Verpackung und Versand der Gebührenbescheide des Bereichs Abfallwirtschaft an ein privates Unternehmen zu übertragen. Der LfD hat die Kreisverwaltung auf folgendes aufmerksam gemacht:

Werden für eine öffentliche Stelle personenbezogene Daten nicht durch diese, sondern in deren Auftrag durch andere Personen oder Stellen verarbeitet, handelt es sich um eine Datenverarbeitung im Auftrag gem. § 4 LDSG.

In diesem Fall ist die auftraggebende Stelle – trotz der Verlagerung der Arbeiten – für die Einhaltung der datenschutzrechtlichen Bestimmungen durch den Auftragnehmer verantwortlich. Um dem Rechnung zu tragen, sollten für eine datenschutzgerechte Ausgestaltung des (schriftlichen) Vertrages grundsätzlich die folgenden Empfehlungen berücksichtigt werden:

- möglichst konkrete Bezeichnung des Gegenstands des Vertrages, Umfang und Grenzen der übertragenen Tätigkeiten;
- Vereinbarungen hinsichtlich erforderlicher Nachweise über erbrachte Vertragsleistungen;
- Regelungen zur Vertragsänderung und -verlängerung, insbesondere hinsichtlich vertraglicher Nebenpflichten oder über ein Vertragsende hinaus sicherzustellender Leistungen;
- Regelungen hinsichtlich eventueller Unterauftragsverhältnisse;
- Verpflichtung auf die maßgebenden datenschutzrechtlichen Bestimmungen – Weisungs-, Prüfungs- und Kontrollrechte des Auftraggebers;
- Prüfungs- und Kontrollrechte des für den Auftraggeber zuständigen Datenschutzbeauftragten;
- Sicherstellung technisch-organisatorischer Maßnahmen seitens des Auftragnehmers nach § 9 BDSG;
- Festlegung derjenigen (formalen) Pflichten, die sich aus den für den Auftraggeber geltenden datenschutzrechtlichen Vorschriften ergeben;
- Regelungen über gegenseitige Hinweispflichten (Anzeige von Veränderungen);
- unter Berücksichtigung der zu erwartenden Risiken Regelungen über Konsequenzen bei Nichterfüllung vertraglicher Leistungen (z. B. Konventionalstrafen, Ersatzvornahme);
- Haftungsregelungen.

Vorliegend war schließlich darauf hinzuweisen, daß mit der vorgesehenen Auslagerung auf eine Privatfirma das Steuergeheimnis berührt wird. Dies ergibt sich aus § 39 Abs. 1 Nr. 1 Kommunalabgabengesetz (KAG) i. V. m. § 30 Abgabenordnung (AO). Vorgänge, die dem Steuergeheimnis unterliegen, sollten indes nur ausnahmsweise Privaten übertragen werden. Es ist in solchen Fällen zu prüfen, ob die Beauftragung einer Privatfirma als unabdingbar anzusehen ist. Der LfD vertritt grundsätzlich die Auffassung, daß Anstrengungen unternommen werden sollten, um ohne eine Beauftragung Privater in diesem Zusammenhang auskommen zu können.

Daraufhin hat die Kreisverwaltung von einer Auslagerung der Verpackung und Versendung der Gebührenbescheide Abstand genommen.

9.6 Öffentlichkeit und Erörterungstermin im abfallrechtlichen Planfeststellungsverfahren

Ein Petent wandte sich gegen den nach seiner Meinung verspäteten Ausschluß der Öffentlichkeit während des Erörterungstermins im Rahmen des Planfeststellungsverfahrens zur Errichtung einer Mülldeponie. Im konkreten Fall ergaben sich aus dem beigezogenen Wortprotokoll des Erörterungstermins aus der Sicht des LfD keine Anhaltspunkte für eine datenschutzrechtlich zu beanstandende Vorgehensweise der als Anhörungsbehörde zuständigen Bezirksregierung.

Gleichwohl wurde deutlich, daß der Schutz des Persönlichkeitsrechts in Massenverfahren – nicht nur im abfallrechtlichen Bereich – durchaus problematisch ist. Was den Erörterungstermin anbelangt, so dient die Regelung in § 68 Abs. 1 VwVfG, wonach die mündliche Verhandlung nicht öffentlich ist, dem Schutz der Persönlichkeitsrechte der Verfahrensbeteiligten und konkretisiert deren Recht auf informationelle Selbstbestimmung. Das gesetzgeberische Motiv der genannten Vorschrift liegt darin, den Beteiligten eine ungestörte und unbeeinflußte Wahrung ihrer Interessen zu ermöglichen. Den Beteiligten soll die Befürchtung genommen werden, ihre Angaben könnten in falsche Hände gelangen. Damit kommt aber auch zum Ausdruck, daß von einem Eingriff in die Persönlichkeitsrechte erst dann gesprochen werden sollte, wenn es um die Erörterung von Sachfragen geht. In dem angesprochenen Fall war auch zu berücksichtigen, daß es sich um ein abfallrechtliches Massenverfahren zum Bau und Betrieb einer Abfallentsorgungsanlage handelte. Hier findet erfahrungsgemäß bereits im Vorfeld des Erörterungstermins eine Mobilisierung der Öffentlichkeit statt, die dazu führt, daß zumindest die Namen der führenden Repräsentanten aus dem Kreis der Einwender bekannt sind.

In diesem Zusammenhang hat der LfD ferner darauf hingewiesen, daß die Einwender-Öffentlichkeit sich in Massenverfahren erfahrungsgemäß als „Quasi-Öffentlichkeit" auswirkt. Wenn nämlich eine Vielzahl von Einwendern Zutritt beanspruchen kann, sind unter diesen Einwendern nach allgemeiner Lebenserfahrung oft auch Journalisten, die Einwendungen erheben. Befürworter von Anlagen erheben bisweilen aus taktischen Gründen Einwendungen, um den Termin beobachten zu können, wobei Einwender aus diesen Personengruppen sich u. U. wiederum vertreten lassen.

In den tatsächlichen Geschehensabläufen dieser Verhandlungen zeigt sich, daß entgegen dem gesetzgeberischen Motiv der Regelung in § 68 VwVfG (Grundsatz der Nichtöffentlichkeit der mündlichen Verhandlung) eine ungestörte und unbeeinflußte Erörterung privater Belange nicht mehr möglich ist. Dies ist eine aus der Sicht des LfD bedauernswerte Entwicklung, deren Ursache in einem Systemfehler des Erörterungstermins im Massenverfahren liegt. Ein Verhandlungsleiter indes kann daran nichts ändern. Vielmehr ist hier der Gesetzgeber gefordert, neue – problemgerechte und an der Verfahrenswirklichkeit orientierte – Wege der Konfliktlösung zu beschreiten.

In der Literatur sind übrigens Ansätze zu neuen Wegen erkennbar (vgl. z. B. den Aufsatz „Kommunikative Problembewältigung bei umweltrelevanten Großvorhaben" von Univ.-Prof. Dr. Hermann Hill, veröffentlicht in DÖV 1994, S. 279 ff.).

9.7 Erfassungsblatt zum Zwecke der Veranlagung von Weinbaubetrieben zur Schmutzfrachtgebühr

Für die bei der Abwasserreinigung aus dem Bereich der Weinbaubetriebe verursachten Mehrkosten mußten die Träger der Abwasserbeseitigung eine Zusatzgebühr gem. § 15 Abs. 3 Kommunalabgabenverordnung (KAVO) erheben, die sog. Schmutzfrachtgebühr. Dabei wurde das Schmutzwasser der Weinbaubetriebe nicht gewichtet, sondern die im Ertrag stehende Fläche und die Zukaufsmenge für Most oder Wein als Verteilungsmaßstab der Gebührenberechnung zugrunde gelegt. Für die Ermittlung und Festsetzung der Gebühren diente ein Erfassungsblatt, dessen Ausgestaltung Gegenstand einer Eingabe war. Ein Großteil der in diesem Zusammenhang anstehenden Fragen im Hinblick auf möglicherweise datenschutzrechtlich unzulässige Erhebungen (so z. B. geforderte Angaben zur Person des Verpächters; Vorlage der Traubenerntemeldung und damit Angaben über die Menge an Qualitätswein/Tafelwein, die für eine flächenabhängige Gebührenberechnung unerheblich waren) hat sich zwischenzeitlich erledigt. Denn aufgrund der Neufassung des Kommunalabgabengesetzes (KAG) in Verbindung mit dem geänderten Landeswassergesetz ist es künftig erlaubt, die Weinbauabwässer in die Weinberge zu verbringen. Damit sind die Kommunen von der Entsorgungspflicht befreit, so daß die Schmutzfrachtgebühr entfallen kann.

Die Einwilligungserklärung lautete wie folgt:

„Ich bin damit einverstanden, daß der ... (Entsorgungsbetrieb) in die alljährlich bei der ... (Kommunalverwaltung) bzw. bei der Landwirtschaftskammer – Weinbauamt – abzugebende Traubenernte- bzw. Weinerzeugermeldung sowie in weitere Statistiken und Unterlagen, aus denen insbesondere die Weinbauertragsfläche hervorgeht, zum Zwecke der Veranlagung Einblick nehmen darf. Der letzte Absatz dieser Erklärung ist freiwillig und kann gestrichen werden."

Anläßlich des Schriftwechsels hat der LfD gefordert, die Einwilligungserklärung den gesetzlichen Anforderungen anzupassen. Er hat ausgeführt, daß die Datenverarbeitung zwar grundsätzlich ohne weitere gesetzliche Grundlage zulässig ist, wenn die Betroffenen einwilligen. Die Betroffenen sind jedoch über die Bedeutung der Einwilligung, den Verwendungszweck der Daten und den möglichen Empfängerkreis aufzuklären. Sie sind gem. § 5 Abs. 2 und 3 LDSG unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß sie die Einwilligung verweigern oder mit Wirkung für die Zukunft widerrufen können. Eine öffentliche Stelle darf aber auch auf der Basis der Einwilligung Daten nicht im beliebigen Umfang erheben und speichern. Im vorliegenden Fall war die Formulierung in bezug auf die Einsichtnahme „in weitere Statistiken und Unterlagen" aus Sicht des LfD viel zu unbestimmt. Er hat darauf hingewiesen, daß die allgemeinen Voraussetzungen allen behördlichen Tätigwerdens auch hier vorliegen müssen; dazu gehört insbesondere, daß die Datenerhebung und -verarbeitung im Rahmen der Aufgaben der öffentlichen Stelle liegen muß. Dies bedeutet, daß überflüssige Informationen auch nicht auf der Basis der Einwilligung verarbeitet werden dürfen.

Das Antwortschreiben enthielt den Hinweis, der nunmehr entsprechend korrigierte, in Rede stehende Absatz des Erfassungsblattes hätte in der Vergangenheit lediglich der „Abschreckung" gedient und sei bisher noch nie angewandt worden. Dies spricht indessen nicht gerade für eine besondere Aufgeschlossenheit gegenüber Datenschutzfragen.

10. Gesundheitswesen

10.1 Statistik und wissenschaftliche Forschung mit medizinischen Daten

10.1.1 Meldungen und Statistik nach dem Bundesseuchengesetz

Nach § 1 Abs. 3 der Verordnung über die Ausdehnung der Meldepflicht auf die humanen spongiformen Enzephalopathien vom 1. Juli 1994 müssen die Meldungen über die zuständigen Landesbehörden an das Robert-Koch-Institut anonym sein. Für die Meldungen wurde ein Vordruck eingeführt, der die Anonymität nicht ausreichend sicherstellt: Aus den nicht durch einen Schlüssel vorgegebenen, sondern als Freitext einzutragenden Angaben zum Beruf i. V. m. den ersten drei Stellen der Postleitzahl, Geburtsmonat und Jahr sowie aus seltenen Staatsangehörigkeiten können sich in Einzelfällen, bei entsprechendem Zusatzwissen, Hinweise auf bestimmte bzw. bestimmbare natürliche Personen ergeben.

Der LfD empfahl, bei der Verwendung des Formblattes vor allem darauf zu achten, daß die Angabe zum Beruf i. V. m. den anderen Angaben keine Reidentifizierungsrisiken enthält.

Das Ministerium für Arbeit, Soziales und Gesundheit entsprach dieser Empfehlung und unterrichtete die Bezirksregierungen.

10.1.2 Verwendung von Leichenschauscheinen für wissenschaftliche Zwecke

Den LfD erreichen immer wieder Anfragen von Gesundheitsämtern und Hochschulen, die wissen wollen, ob der Inhalt von Leichenschauscheinen für wissenschaftliche Zwecke verwendet werden darf. Die Rechtslage ist folgende:

§ 4 Abs. 3 der LVO zur Durchführung des Bestattungsgesetzes vom 20. Juni 1983, GVBl. S. 133, BS 2127-1-1, bestimmt, daß der Leichenschauschein von den Behörden der Versorgungsverwaltung und den Trägern der gesetzlichen Unfallversicherung eingesehen werden kann. Diese derzeit geltende Regelung ist abschließend; eine Datenübermittlung für wissenschaftliche Zwecke kommt danach nicht in Betracht.

Das Ministerium für Arbeit, Soziales und Gesundheit beabsichtigt, im Anschluß an die Novellierung des Bestattungsgesetzes auch die obige LVO zu ändern. In einer Stellungnahme zu dem Verordnungsentwurf wies der LfD darauf hin, daß sich diese Regelung in der Vergangenheit sowohl im Blick auf berechtigte Informationsansprüche von Hinterbliebenen wie auch im Blick auf die Interessen der wissenschaftlichen Forschung als sehr eng erwiesen hat. Dabei ist zu berücksichtigen, daß auch der Inhalt der beim Arzt verbleibenden Ausfertigung der Todesbescheinigung nicht offenbart werden darf. Ob eine Offenbarung aufgrund einer zu Lebzeiten vom Betroffenen erklärten Einwilligung zulässig ist, ist unklar. Der LfD empfahl deshalb zu prüfen, ob die Regelung in der bisherigen engen Fassung beibehalten werden muß. Gegen die angemessene Berücksichtigung von Informationsinteressen der Hinterbliebenen oder von Forschungseinrichtungen für Zwecke der Wissenschaft wären jedenfalls aus seiner Sicht keine Bedenken zu erheben.

10.1.3 Erfassungsprogramm für angeborene Fehlbildungen bei Neugeborenen (Mainzer Modell)

Ziel des Erfassungsprogramms ist es, zuverlässige Informationen über Art und Häufigkeit angeborener Fehlbildungen zu gewinnen. Projektbeteiligte sind die Universitätskinderklinik und das Institut für Medizinische Statistik und Dokumentation der Johannes Gutenberg-Universität Mainz sowie die Abteilung für Epidemiologie des Deutschen Krebsforschungszentrums Heidelberg. Für die Datenerfassung wurde ein projektbezogener dreiteiliger Erhebungsbogen in Anlehnung an den Perinatologischen Basiserhebungsbogen entwickelt. Angaben zur Mutter des Kindes, zum Vater, zur Familienanamnese, zum Schwangerschaftsverlauf, zur Geburt und zum Neugeborenen selbst sowie allgemeine Expositionsdaten werden den vorhandenen gynäkologischen Patientenakten bzw. dem Perinatologischen Basiserhebungsbogen entnommen und anonymisiert dokumentiert. Neben den anamnestischen Daten werden die Untersuchungsbefunde in verschlüsselter Form dokumentiert.

Das Mainzer Modell war im Deutschen Bundestag Gegenstand einer Kleinen Anfrage – Drucksache 12/7377 –. Der Antwort der Bundesregierung – Drucksache 12/7716 – ist unter Tz. 5 und 6 auch Näheres über die datenschutzrechtliche Beurteilung zu entnehmen. Um Fehlbildungen in Deutschland systematisch zu erfassen, hat der Wissenschaftliche Beirat der Bundesärztekammer in einer Empfehlung „Erhebung von Fehlbildungen" ein Verbundkonzept vorgeschlagen. Dieses sieht das Zusammenführen der Daten aus den flächendeckenden bundesweiten Informationen der Perinatalstudien, aus koordinierten Fehlbildungserhebungen in Perinatologischen Zentren, wie dem Mainzer Modell, sowie aus pränatalen Chromosomenuntersuchungen vor. Eine Realisierung dieser Zielsetzung ist jedoch in absehbarer Zeit nicht zu erwarten. Das Mainzer Modell wird – im wesentlichen unverändert – von der Ludwig-Maximilians-Universität München unter Einbeziehung anderer Geburtskliniken im Raum München übernommen. Projekte mit ähnlicher Aufgabenstellung bestehen auch in Magdeburg und Hamburg.

Der LfD wurde von den Projektverantwortlichen erst in der Einführungsphase des Modells informiert, nachdem in der Öffentlichkeit kritische Stimmen laut geworden waren, die eine schwerwiegende Beeinträchtigung von Datenschutzrechten befürchteten.

Die eingehende Prüfung der Verfahrensabläufe ergab, daß derartige Befürchtungen jedenfalls im gegenwärtigen Entwicklungsstadium unbegründet sind. Beteiligt sind drei geburtshilfliche Kliniken; von einer bundesweit flächendeckenden Erfassung kann keine Rede sein. Die Daten werden von einer Fachärztin, die in diesen Kliniken unabhängig von dem Mainzer Modell Untersuchungen an Neugeborenen vornimmt, erhoben und stehen damit unter dem Schutz der ärztlichen Schweigepflicht. Die Daten werden auf den Erfassungsbögen – und später im automatisierten Verfahren – anonymisiert gespeichert. Zuständig für die Datenverarbeitung ist das Krebsforschungszentrum Heidelberg als Auftragnehmer.

Die gespeicherten anonymisierten Einzeldatensätze können nur unter Mitwirkung der jeweiligen Geburtsklinik deanonymisiert werden. Sofern also ein wissenschaftliches Interesse beispielsweise an einer ergänzenden Datenerhebung zu einem in dem Register gespeicherten Fall besteht, muß die Geburtsklinik ersucht werden, die Identifizierung vorzunehmen. Mißverständliche Äußerungen eines Projektverantwortlichen in der Presse zu diesem Problem ließen den unzutreffenden Eindruck entstehen, eine Identifizierung sei gänzlich ausgeschlossen und die wissenschaftliche Arbeit damit unzumutbar behindert. Unter Datenschutzgesichtspunkten ist es freilich entscheidend, daß Informationen nach Herstellung des Personenbezugs bei den Ärzten verbleiben, die im Rahmen der Behandlung beratend tätig sind.

Die Anonymität der gespeicherten Daten wird auch dadurch gesichert, daß die regionalen Zuordnungen über Ziffern erfolgen, die nur sieben Ausprägungen wiedergeben.

Für die datenschutzrechtliche Beurteilung ist auch von Bedeutung, ob ausschließlich Behandlungsdaten verwendet oder ob ergänzend personenbezogene medizinische Daten, die für die Behandlung nicht erforderlich sind, nur für wissenschaftliche Zwecke erhoben werden. Im letztgenannten Falle wäre eine detaillierte Information der Betroffenen und deren Einwilligung Voraussetzung der Datenverarbeitung. Bei den sog. „großen Fehlbildungen" bestehen keine Zweifel an der Erforderlichkeit und Zulässigkeit der Erfassung aufgrund des Behandlungsvertrags. Der Katalog der „kleinen morphologischen Auffälligkeiten" wurde unter Berücksichtigung der datenschutzrechtlichen Gesichtspunkte überarbeitet. In der nunmehr vorliegenden Fassung entspricht er, so wurde dem LfD aus fachlicher Sicht vorgetragen, der Dokumentationspflicht bei Behandlungsfällen.

10.2 Öffentlicher Gesundheitsdienst

10.2.1 Landesgesetz über den öffentlichen Gesundheitsdienst

Die Arbeit der Gesundheitsämter in Rheinland-Pfalz stützt sich noch immer im wesentlichen auf das „Gesetz über die Vereinheitlichung des Gesundheitswesens" vom 3. Juli 1934 und die hierzu ergangene Durchführungsverordnung aus dem Jahre 1935. Diese Rechtsgrundlagen entsprechen nicht mehr den heutigen Anforderungen an eine moderne Gesundheitsverwaltung. In ihrem 12. Tätigkeitsbericht (Tz. 9.1) wies die DSK darauf hin, daß wesentliche datenschutzrechtliche Grundfragen ungeklärt sind und die Erfahrungen aus der Wahrnehmung von Kontrollaufgaben im Bereich der Gesundheitsverwaltung und aus der Bearbeitung von Eingaben die Forderung nach einer gesetzlichen Neuordnung dieses Bereichs unterstreichen. Normenklare Datenschutzregelungen hielt die DSK auch deshalb für dringend erforderlich, weil die Gesundheitsverwaltung in Rheinland-Pfalz an der Schwelle zum Einsatz autonomer automatisierter Verfahren für die Aufgabenerfüllung steht. Im Blick auf die außerordentlich hohe Sensitivität der Informationsverarbeitung im Gesundheitsbereich könne, so die DSK, ein Rechnereinsatz grundsätzlich nur dann akzeptiert werden, wenn die Aufgaben und Befugnisse der Gesundheitsverwaltung gegenüber den Bürgern und ihre Zusammenarbeit mit anderen Stellen normenklar geregelt sind und die Einhaltung dieser Regelungen durch organisatorische Vorkehrungen gesichert ist.

Im Anschluß an eine Initiative der Fraktion der CDU vom März 1995 für ein Landesgesetz über den öffentlichen Gesundheitsdienst (Drucksache 12/6230) wurde dem LfD im Mai 1995 ein Referentenentwurf zur Stellungnahme vorgelegt, der im Juni 1995 eingebracht wurde (ÖGdG, Drucksache 12/6841). Beide Gesetzentwürfe enthalten Datenschutzregelungen, die im Grundsatz angemessen, in den Details aber verbesserungsfähig sind. Die Empfehlungen des LfD zum Referentenentwurf wurden im wesentlichen berücksichtigt, so daß er sich im Anhörverfahren auf wenige Anmerkungen und Änderungsvorschläge beschränken konnte. Ein zentrales Anliegen, das beide Entwürfe betrifft, formulierte der LfD wie folgt:

Es gibt im öffentlichen Gesundheitsdienst im wesentlichen drei Bereiche, in denen personenbezogene Daten verarbeitet – erhoben, gespeichert, genutzt, übermittelt, gesperrt und gelöscht (§ 3 Abs. 2 LDSG) – werden:

- der Bereich der zwangsweise durchsetzbaren Untersuchungen (Beisp. §§ 32, 36 Bundesseuchengesetz, §§ 3, 4, 13 Geschlechtskrankheitengesetz);
- der Bereich, in dem Untersuchungen für die Betroffenen Obliegenheiten darstellen (Beisp. § 18 Bundesseuchengesetz, § 15 b Abs. 1 Straßenverkehrszulassungsordnung);
- der Bereich, in dem Untersuchungen und Beratungen auf freiwilliger Grundlage durchgeführt werden (Beisp. Schwangerenberatung, Beratungen für Krebskranke, freiwillige Impfungen, HIV-Tests).

In dem unter dem letzten Spiegelstrich angesprochenen Bereich unterscheidet sich die Tätigkeit von Ärzten im öffentlichen Gesundheitsdienst nicht oder nur ganz unwesentlich von der Tätigkeit eines niedergelassenen Arztes oder eines Arztes im

Krankenhaus. Voraussetzung für diese Leistungen, die freiwillig in Anspruch genommen, gleichwohl aber im öffentlichen Interesse erbracht werden, ist das Vertrauensverhältnis zwischen Patient und Arzt. Dieses bezieht sich nicht nur darauf, daß der Arzt fachlich qualifiziert ist, die Leistung zu erbringen, sondern auch darauf, daß er und seine Mitarbeiter Verschwiegenheit über das bewahren, was ihnen bei der Aufgabenwahrnehmung anvertraut worden oder sonst bekanntgeworden ist.

Dieses besondere Vertrauensverhältnis ist durch die Berufsordnung für die Ärzte (§ 2) und durch § 203 Abs. 1 und 3 StGB geschützt. Nach der letztgenannten Vorschrift wird der Arzt oder sein berufsmäßig tätiger Gehilfe bestraft, wenn er „unbefugt" Privatgeheimnisse offenbart. Zum Begriff der Befugnis i. S. d. § 203 StGB existiert umfangreiche Rechtsprechung und Literatur; in Betracht kommen die Einwilligung des Betroffenen und allgemeine Rechtfertigungsgründe (Gesetz, rechtfertigender Notstand, gesetzliche Anzeigepflichten).

In dieses vorhandene System des Vertrauensschutzes für das Arzt-/Patientenverhältnis würde durch das ÖGdG mit Datenverarbeitungsbestimmungen eingegriffen, die nicht nur in den unter den beiden ersten Spiegelstrichen genannten Fällen – wo sie im wesentlichen angemessen sind – sondern auch dann anzuwenden sind, wenn sich ein Betroffener ohne jede rechtliche Verpflichtung ratsuchend an Mitarbeiter des Gesundheitsamtes wendet. Auch die in diesem Zusammenhang erhobenen Daten dürften, bliebe der Entwurf unverändert, zur Erfüllung ganz anderer Aufgaben der Behörden des öffentlichen Gesundheitsdienstes gespeichert und genutzt (§ 11 Abs. 2 Nr. 1) oder nach § 11 Abs. 3 an andere öffentliche und nichtöffentliche Stellen übermittelt werden. Die Situation einer Person, die sich bei einem Gesundheitsamt einem freiwilligen HIV-Test unterzieht, würde sich von der einer Person, die einen niedergelassenen Arzt in Anspruch nimmt, dadurch unterscheiden, daß das Testergebnis im Rahmen des § 11 Abs. 2 verwendet und beispielsweise für die Durchführung von Organisationsuntersuchungen nach § 11 Abs. 3 oder für Zwecke der wissenschaftlichen Forschung nach § 11 Abs. 4 übermittelt wird. Diese Verarbeitungs- und Übermittlungsregelungen könnten, so ist zu befürchten, dazu führen, daß der öffentliche Gesundheitsdienst für derartige Leistungen, an deren Erbringung ein eminent starkes öffentliches Interesse besteht, nicht mehr in dem wünschenswerten Umfange in Anspruch genommen wird.

Der LfD empfahl, das Problem in der Weise zu lösen, daß in § 11 folgender neue Absatz 5 eingefügt wird:

„(5) Daten, die einem Mitarbeiter des öffentlichen Gesundheitsdienstes zum Zwecke der Beratung oder zu sonstigen Zwecken ohne gesetzliche Verpflichtung anvertraut worden sind, dürfen nur im Rahmen dieser Zweckbestimmungen gespeichert und genutzt oder beim Vorliegen der Voraussetzungen des § 203 Abs. 1 und 3 Strafgesetzbuch übermittelt oder offenbart werden."

Nach dem Verlauf der Beratungen im federführenden Sozialpolitischen Ausschuß ist davon auszugehen, daß der Vorschlag des LfD in einer leicht veränderten Fassung übernommen wird.

10.2.2 Was hat der Stuhlgang eines Polizeibeamten mit seinem verstauchten Finger zu tun?

Ein Polizeibeamter hatte sich beim Dienstsport einen Finger verstaucht und wurde deshalb angewiesen, sich zur Feststellung der Dienstfähigkeit bei einem Gesundheitsamt vorzustellen. Seitens des Gesundheitsamtes wurde ihm mit der Bitte um wahrheitsgemäße Beantwortung ein Fragebogen ausgehändigt, der sowohl die gesundheitliche Familienvorgeschichte wie auch eigene Vorerkrankungen betraf. Es wurde u. a. gefragt, wer in der Familie an einem Schlaganfall oder an Krebs erkrankt war und ob Geisteskrankheiten oder Geschlechtskrankheiten vorlagen. Ferner sollte der Beamte Beschwerden oder Veränderungen beim Stuhlgang offenbaren und mitteilen, ob und ggf. in welchem Umfange er Drogen konsumiere. Insgesamt wurden 83 Fragen gestellt, die zum weitaus größten Teil mit dem verstauchten Finger des Beamten nicht das geringste zu tun hatten. Das Ministerium für Arbeit, Soziales und Gesundheit stimmte dem LfD in der Auffassung zu, daß der Fragebogen inhaltlich weit über das hinausging, was zur Aufgabenerfüllung erforderlich war. Eine Datenerhebung durch Gesundheitsämter, die über das im Einzelfall erforderliche Maß hinausgeht, ist datenschutzrechtlich nicht zulässig. Das Ministerium forderte die Bezirksregierungen auf, die Gesundheitsämter über den geschilderten Fall zu informieren und sicherzustellen, daß – auch bei Verwendung von Fragebögen – die Datenerhebung der Gesundheitsämter auf das zur konkreten Aufgabenerfüllung Erforderliche beschränkt wird.

Datenschutzrelevant sind aber auch folgende Gesichtspunkte: Im Einleitungsteil des Fragebogens war aufgrund der mißverständlichen Formulierung „Wir bitten Sie deshalb, diesen Fragebogen gewissenhaft zu beantworten ..." nicht erkennbar, daß keine Antwortpflicht besteht. Jedenfalls erfüllt diese Formulierung nicht die an eine Einwilligungserklärung nach Datenschutzrecht zu stellenden formalen und inhaltlichen Anforderungen. Dessenungeachtet ist auch zu berücksichtigen, daß die Qualität einer Einwilligung als freier, durch keine sachfremden Erwägungen beeinträchtigter Willensakt jedenfalls in solchen Fällen in Frage zu stellen wäre, in denen der Betroffene befürchtet, durch die Verweigerung ein für ihn ungünstiges Klima zu erzeugen. Ein Problem dürfte auch sein, daß der Betroffene kaum in der Lage ist, die untersuchungsrelevanten Informationen von solchen abzugrenzen, die im konkreten Falle ohne jede Bedeutung sind.

Der LfD strebt an, daß das Fragebogenverfahren mit seinen beschriebenen Inhalten und der beschriebenen Form durch eine Befragung ersetzt wird, die vom Arzt selbst im Blick auf die anstehende Untersuchung unter besonderer Berücksichtigung der Erforderlichkeit durchgeführt wird. Bei örtlichen Feststellungen in Gesundheitsämtern wird dies ein Prüfungsschwerpunkt sein.

10.2.3 Tonbandaufzeichnungen bei Prüfungsgesprächen

Die Prüfung von Anträgen auf Erteilung der Erlaubnis zur Ausübung der Heilkunde nach dem Heilpraktikergesetz, beschränkt auf das Gebiet der Psychotherapie, ist mit einem Prüfungsgespräch verbunden. In einem Gesundheitsamt wurde zu Protokollzwecken bei diesen Prüfungsgesprächen ein Tonband eingesetzt, d. h. die Fragen des Prüfers und die Antworten des Prüflings wurden aufgezeichnet.

Zur Begründung der Erforderlichkeit der Tonbandaufzeichnungen wurde vorgetragen, daß diese vor dem Hintergrund einer besonderen Problematik gesehen werden müsse: Im Heilpraktikerrecht existierten weder staatlich geregelte Ausbildungs- oder Prüfungsvorschriften, noch seien die Prüfungsinhalte vorgegeben. Lediglich die im Heilpraktikergesetz vorgegebene Formulierung, daß der Amtsarzt in einer Überprüfung festzustellen habe, ob aufgrund der Kenntnisse und Fähigkeiten des Antragstellers eine Gefahr für die Volksgesundheit ausgehen könne, diene als Beurteilungskriterium für die Erlaubniserteilung. Um auf dem Boden dieser relativ unscharfen rechtlichen Vorgaben eine möglichst hohe Objektivität und Chancengleichheit für alle Antragsteller zu erreichen, werde auf Tonbandaufzeichnungen zurückgegriffen. Eine wortgetreue Aufzeichnung des Überprüfungsgesprächs sei notwendig, damit in einem nachfolgenden Widerspruchsverfahren eine eindeutige Klärung erfolgen könne. Auf die Zustimmung zu den Tonbandaufzeichnungen werde verzichtet, weil davon auszugehen sei, daß ein Antragsteller vor der Überprüfung kaum eine freie Willensentscheidung treffe, d. h. unter der Erwartung, sein Überprüfungsergebnis nicht negativ zu beeinflussen, werde er wahrscheinlich der Aufzeichnung zustimmen. Das Aufzeichnungsgerät stehe während des Überprüfungsgesprächs offen sichtbar auf dem Tisch, so daß für den Probanden erkennbar sei, daß dieses Hilfsmittel eingesetzt werde.

Unter datenschutzrechtlichen Gesichtspunkten war die Frage zu beurteilen, ob es sich bei der Anfertigung von Tonbandaufzeichnungen in der beschriebenen Weise um einen Informationseingriff handelt, der ohne ausdrückliche gesetzliche Eingriffsbefugnis zulässig ist.

§ 201 Abs. 1 Nr. 1 StGB schützt das Verfügungsrecht des Betroffenen über sein nichtöffentlich gesprochenes Wort: Die Aufnahme des nichtöffentlich gesprochenen Wortes eines anderen auf einen Tonträger ist strafbedroht, wenn sie unbefugt erfolgt. Für die Befugnis gilt das gleiche wie für die Offenbarung von Informationen, die den besonderen Berufsgeheimnissen des § 203 Abs. 1 StGB unterliegen; sie kann, von Fällen des rechtfertigenden Notstands abgesehen, nur aus einer gesetzlichen Eingriffsbefugnis oder aus der Zustimmung der Betroffenen hergeleitet werden. Aus der Teilnahme eines Probanden an der Prüfung trotz der für ihn erkennbaren Verwendung eines Tonbandgeräts zu Aufzeichnungszwecken kann nicht auf das Vorliegen einer Zustimmung geschlossen werden.

Hinweise auf die Qualifizierung der Tonbandaufzeichnungen als Informationseingriffe gibt das Urteil des Bundesverwaltungsgerichts vom 3. August 1990 – 7 C 14/90 – (NJW 1991, 118), das den Tonbandmitschnitt einer öffentlichen Gemeinderatssitzung durch Pressevertreter untersagt. In dieser Entscheidung wird hervorgehoben, daß das Recht des Ratsmitglieds auf freie Rede zwar nicht in der höchstpersönlichen Rechtssphäre gründet, aber durch die Aufzeichnung auf Tonband faktisch empfindlich tangiert werden kann. Ein gleichartiger Befund habe den Gesetzgeber sogar veranlaßt, die Verhandlung im Gerichtsverfahren, dort allerdings zum Schutz anderer Rechtsgüter, von Fernseh- und Rundfunkaufnahmen sowie von Ton- und Filmaufnahmen mit dem Ziel ihrer Veröffentlichung ganz freizustellen (§ 169 GVG). Tonbandaufzeichnungen zeitigten für das Verhalten der Betroffenen erhebliche Wirkung, weil sie jede Nuance der Rede, einschließlich der rhetorischen Fehlleistungen, der sprachlichen Unzulänglichkeiten und der Gemütsbewegungen des Redners dauerhaft und ständig reproduzierbar konservierten. Soweit im Einzelfall ein Interesse an der wortgetreuen Wiedergabe von Redepassagen bestehe, eröffneten die Mittel der Schrift genügend Möglichkeiten, exakt zu berichten.

Zusammenfassend vertrat der LfD die Auffassung, daß gegen eine gesetzgeberische Entscheidung, Tonbandaufnahmen in Prüfungsverfahren zu verwenden, keine durchgreifenden verfassungsrechtlichen Bedenken bestünden. Dies insbesondere dann nicht, wenn die gesetzgeberische Grundentscheidung durch verfahrenssichernde Maßnahmen (Zweckbindung, gesicherte Aufbewahrung, Löschung) flankiert würde. Ohne ausdrückliche gesetzliche Eingriffsbefugnis halte er die Tonbandaufzeichnungen aber für unzulässig.

Diese Rechtsauffassung wurde von der Gesundheitsverwaltung anerkannt; Tonbandaufzeichnungen werden bei den Prüfungsgesprächen nicht mehr angefertigt.

10.2.4 Unterrichtung von Straßenverkehrsbehörden durch die Gesundheitsämter

Ein Gemeinsames – nicht veröffentlichtes – Rundschreiben des Ministeriums für Soziales und Familie, des Ministeriums für Umwelt und Gesundheit, des Ministeriums für Wirtschaft und Verkehr sowie des Ministeriums des Innern und für Sport vom 25. Januar 1988 (s. Heft 5, S. 75 f.) regelt die Unterrichtung der Straßenverkehrsbehörde über Maßnahmen nach dem Unterbringungsgesetz. Es sieht vor, daß das Gesundheitsamt, wenn ihm von dem behandelnden Klinikarzt Bedenken hinsichtlich der Eignung eines Patienten zur Führung eines Kraftfahrzeugs mitgeteilt werden, in der Weise tätig wird, daß es ein Gespräch mit dem Patienten führt und versucht, ihn vom Führen eines Kraftfahrzeuges abzuhalten. Zeigt sich der Patient uneinsichtig,

so benachrichtigt das Gesundheitsamt die zuständige Straßenverkehrsbehörde. Zuvor hat es den Patienten hierüber zu unterrichten.

Diese Regelung hat sich aus der Sicht des LfD bewährt; sie konnte indessen nur für eine Übergangszeit bis zur Schaffung einer normenklaren Rechtsgrundlage Bestand haben. Der LfD begrüßt es, daß der in der parlamentarischen Beratung befindliche Entwurf eines Landesgesetzes für psychisch kranke Personen (PsychKG) – Drucksache 12/6842 – in § 33 die Problematik aufgreift und, soweit die Gesundheitsämter betroffen sind, einer Lösung zuführt.

Für den allgemeinen ärztlichen Bereich – außerhalb des öffentlichen Gesundheitsdienstes – ist auf die Rechtsprechung und Kommentierung von § 203 StGB zu verweisen.

Der Bundesgerichtshof hat mit Urteil vom 8. Oktober 1968 – VI ZR 168/67 – (NJW 1968, 2288) Mitteilungen des Arztes in Fällen der oben geschilderten Art wie folgt für zulässig gehalten: „Ein Arzt kann trotz seiner grundsätzlichen Schweigepflicht nach den Grundsätzen über die Abwägung widerstreitender Pflichten oder Interessen berechtigt sein, die Verkehrsbehörde zu benachrichtigen, wenn sein Patient mit einem Kraftwagen am Straßenverkehr teilnimmt, obwohl er wegen seiner Erkrankung nicht mehr fähig ist, ein Kraftfahrzeug zu führen, ohne sich und andere zu gefährden."

Die Strafrechtsliteratur hält eine Durchbrechung der ärztlichen Schweigepflicht für zulässig, „soweit die Tat nach den Grundsätzen der Güter- und Interessenabwägung ein angemessenes Mittel ist ... Der Arzt darf erforderlichenfalls Angehörige warnen oder den zuständigen Behörden von epileptischen Anfällen seines Patienten beim Autofahren oder sonstigen die Fahrtüchtigkeit aufhebenden Krankheiten berichten." (Dreher/Tröndle, StGB, RdNr. 31 zu § 203 m. w. N.).

10.2.5 Übermittlung von Gesundheitsdaten durch die Gesundheitsämter an Sozialleistungsträger

Sozialleistungsträger benötigen im Zusammenhang mit der Entscheidung über die Gewährung von Sozialleistungen, die vom Gesundheitszustand der Betroffenen abhängen, in bestimmten Fällen ein amtsärztliches Gutachten des zuständigen Gesundheitsamtes; dies gilt insbesondere bei der Leistungsgewährung nach den Vorschriften des Bundessozialhilfegesetzes. In mehreren Dienstbesprechungen von Amtsärzten, an denen Vertreter des LfD teilnahmen, wurde deutlich, daß bezüglich der Übermittlungsvoraussetzungen für derartige amtsärzliche Gutachten bei den Gesundheitsämtern eine verbreitete Rechtsunsicherheit bestand. Das Ministerium für Arbeit, Soziales und Gesundheit entsprach der Anregung von Gesundheitsämtern und des LfD, „Hinweise für die Übermittlung von Gesundheitsdaten durch die Gesundheitsämter an Sozialleistungsbehörden" herauszugeben.

Die Hinweise gehen davon aus, daß in der Regel die Sozialleistungsbehörden bereits bei der Antragstellung auf eine Sozialleistung eine Erklärung über die Schweigepflichtentbindung von der betroffenen Person oder ihrer gesetzlichen Vertreterin oder ihrem gesetzlichen Vertreter unterzeichnen lassen. Unterrichtet die Sozialleistungsbehörde das Gesundheitsamt über die erfolgte Schweigepflichtentbindung, so kann ärztlicherseits davon ausgegangen werden, daß eine wirksame Schweigepflichtentbindungserklärung vorliegt und eine Befugnis besteht, der Sozialleistungsbehörde die im Einzelfall benötigten Gesundheitsdaten zu übermitteln. Darüber hinaus besteht die Möglichkeit, daß die Amtsärzte selbst die Schweigepflichtentbindungserklärung einholen; auch hierzu werden Hinweise gegeben. Auf Wunsch des LfD wurde ferner ein Muster für eine Schweigepflichtentbindungserklärung angefügt.

Die Gesundheitsämter in Rheinland-Pfalz wurden durch Rundschreiben des Ministeriums vom 19. Dezember 1994 informiert.

10.3 Übersendung von Arztbriefen durch Krankenhausärzte

Der Chefarzt eines Krankenhauses in der Trägerschaft des Landes fragte an, unter welchen gesetzlichen Voraussetzungen Arztbriefe nach der Entlassung eines Patienten aus dem Krankenhaus an weiterbehandelnde Ärzte übermittelt werden dürfen. Sein besonderes Interesse galt auch der Frage, ob alleine die Erklärung des ärztlichen Kollegen, daß er Informationen für die Weiterbehandlung benötige, als Übermittlungsgrundlage ausreiche oder ob die Vorlage einer Erklärung über die Entbindung von der Schweigepflicht unabdingbar sei.

Ärzte eines Krankenhauses haben ebenso wie freipraktizierende Ärzte besondere Verschwiegenheitspflichten zu beachten. Rechtsgrundlage dieses sog. Arztgeheimnisses ist § 2 der Berufsordnung für die Ärzte; strafbewehrt ist die Verletzung des Arztgeheimnisses durch § 203 Abs. 1 Nr. 1 StGB. Eine Durchbrechung des Arztgeheimnisses ist, von Sonderfällen wie z. B. dem rechtfertigenden Notstand (§ 34 StGB) abgesehen, nur dann zulässig, wenn der Patient seine Einwilligung erteilt hat oder wenn die Offenbarung gesetzlich zugelassen ist.

Gesetzliche Übermittlungsregelungen sind § 36 Abs. 3 des Landeskrankenhausgesetzes (LKG) zu entnehmen. Nummer 2 dieser Vorschrift bestimmt, daß eine Übermittlung zulässig ist, soweit sie zur Durchführung des Behandlungsvertrages einschließlich der Nachbehandlung erforderlich ist und der Patient nach Hinweis auf die beabsichtigte Übermittlung nicht etwas anderes bestimmt.

Dieser Vorschrift entsprechend werden Krankenhauspatienten vor der Entlassung üblicherweise gefragt, an welchen nachbehandelnden Arzt der Entlassungsbericht übermittelt werden soll. Nennt der Patient einen nachbehandelnden Arzt und widerspricht er nicht der Übermittlung, so ist die mit der Übermittlung verbundene Durchbrechung des Arztgeheimnisses nach § 36 Abs. 3 Nr. 2 LKG zulässig.

Selbstverständlich ist es zulässig, dieses Verfahren auch noch nach der Entlassung des Patienten aus dem Krankenhaus durchzuführen. Wenn also ein Arzt den Entlassungsbericht anfordert, wäre der Patient über die beabsichtigte Übermittlung zu unterrichten; trifft er keine andere Bestimmung (z. B. Widerspruch oder Benennung eines anderen nachbehandelnden Arztes) so ist die Offenbarung zulässig. Die Unterrichtung bedarf nicht der Schriftform; sie könnte, wenn die Identität des Patienten zweifelsfrei feststellbar ist, auch fernmündlich erfolgen. Im Blick auf die Strafrechtsrelevanz dürfte es sich jedoch empfehlen, die Informations- und Übermittlungsvorgänge in der Patientenakte zu dokumentieren.

Die Erklärung des ärztlichen Kollegen, der sich als weiterbehandelnder Arzt bezeichnet, reicht für die Übersendung des Entlassungsberichts nicht aus. Entweder muß das oben beschriebene Verfahren durchgeführt oder der ärztliche Kollege aufgefordert werden, eine Schweigepflichtsentbindung des Patienten vorzulegen (Einwilligung i. S. von § 36 Abs. 3 Satz 2 LKG). Bezüglich der Formerfordernisse ist § 36 Abs. 2 Satz 2 bis 4 LKG zu beachten.

Auf den einweisenden Arzt bezieht sich § 36 Abs. 3 Nr. 2 LKG nur dann, wenn er auch nachbehandelnder Arzt ist. Im übrigen ist eine Übermittlung von Patientendaten an den einweisenden Arzt nur zulässig, wenn der Patient seine Einwilligung (§ 36 Abs. 3 Satz 2 i. V. m. § 36 Abs. 2 Satz 2 bis 4 LKG) erteilt hat.

10.4 Die Befreiung vom ärztlichen Notfalldienst – ein Datenschutzproblem

Ein niedergelassener Arzt konnte nach einer schweren Erkrankung seine Praxis nur noch in eingeschränktem Umfange weiterführen. Weil es ihn besonders belastete, daß er zum ärztlichen Notfalldienst – mit Sonntags- und Nachtdienst – herangezogen wurde, beantragte er beim Kreisobmann der Ärzteschaft die Freistellung. Mit dem Antrag legte der Arzt die Bescheinigung eines Facharztes über die eingeschränkte Leistungsfähigkeit vor, die indessen dem Kreisobmann als Beweismittel nicht ausreichte. Er verlangte ergänzend Auskunft über die Zahl der Krankenscheine, die im vorangegangenen Quartal bei der Kassenärztlichen Vereinigung für Abrechnungszwecke eingereicht wurden. Der betroffene Arzt sah sich durch dieses Verlangen in seinen Datenschutzrechten beeinträchtigt und beschwerte sich beim LfD.

Die von der Vertreterversammlung der zuständigen Bezirksärztekammer erlassene Notfalldienstordnung sieht vor, daß der Kreisobmann der Ärzteschaft im Auftrag der Bezirksärztekammer für die Organisation des Notfalldienstes verantwortlich ist. Sie bestimmt ferner, daß eine Freistellung vom Notfalldienst auf Antrag erfolgen kann, wenn ein Arzt durch Alter oder Krankheit in seiner täglichen Leistungsfähigkeit wesentlich beeinträchtigt ist.

Die Entscheidung über die Freistellung steht nicht im Belieben des Obmannes, sondern ist von diesem nach pflichtgemäßem Ermessen zu treffen. Der Arzt hat seinen Freistellungsantrag nach der Notfalldienstordnung schriftlich zu begründen. Die Bezeichnung von Beweismitteln oder die Vorlage von Beweisurkunden ist im Grundsatz sachdienlich.

Die mit dem Antrag vorgelegte Bescheinigung des Facharztes ist als Privaturkunde im Sinne von § 416 ZPO anzusehen. Nach dieser Regelung, die auch für das Verwaltungsverfahren von Bedeutung ist, begründet ein solches ärztliches Attest vollen Beweis nur dafür, daß die in der Bescheinigung enthaltene Erklärung vom Arzt abgegeben worden ist. Für die Richtigkeit dieser Erklärung gilt demgegenüber die Regelung der freien Beweiswürdigung: Dies bedeutet, daß der Obmann alle für den Einzelfall bedeutsamen Umstände zu berücksichtigen und nach freier Überzeugung zu entscheiden hat, ob er eine darin enthaltene tatsächliche Behauptung für wahr hält. Er kann sich zwar an den Inhalt eines solchen Attestes halten; ist er jedoch von der Wahrheit und Vollständigkeit nicht überzeugt, so kann er weiter ermitteln.

Eine Notwendigkeit, in der Sache weiter zu ermitteln, kann beispielsweise dann bestehen, wenn das ärztliche Attest inhaltlich so verkürzt ist, daß es für die Beurteilung, ob die Voraussetzungen des § 3 Notfalldienstordnung vorliegen, nicht tauglich ist. Der Beweiswert ärzlicher Bescheinigungen läßt sich nur feststellen, wenn sich aus dem vorgelegten Attest mindestens Art und Umfang der vom Arzt aufgrund eigener Wahrnehmung getroffenen Tatsachenfeststellungen ergeben und nicht erkennbar ist, daß der Arzt bei seiner Beurteilung Rechtsbegriffe verkannt hat. So muß aus dem Attest zu ersehen sein, ob es sich beispielsweise um ein Dauerleiden oder um eine vorübergehende Erkrankung handelt. Nähere Angaben über die Art der Erkrankung ermöglichen es, die Beeinträchtigung der Leistungsfähigkeit im Sinne der Notfalldienstordnung zu beurteilen.

Nach Auffassung des LfD gehört es aber nicht zu den Obliegenheiten des Arztes, der eine Freistellung beantragt, den Nachweis einer Beeinträchtigung der Leistungsfähigkeit indirekt, nämlich durch nähere Angaben über die Zahl der abgerechneten Krankenscheine, zu führen. Bedenken bestehen insbesondere bezüglich der Geeignetheit derartiger Informationen. Einerseits kann ein Rückgang der Abrechnungszahlen auf anderen Ursachen als einer Erkrankung beruhen, andererseits ist nicht auszuschließen, daß sich eine krankheitsbedingte Leistungsbeeinträchtigung erst mit einiger Verzögerung auf die Abrechnung aus-

wirkt, etwa weil der Arzt seine Patienten, zu denen ein Vertrauensverhältnis besteht, nicht abweisen will, aber keine neuen Patienten mehr annimmt.

Im konkreten Falle empfahl der LfD, von der in der Notfalldienstordnung eingeräumten Möglichkeit Gebrauch zu machen und gegen die Entscheidung des Kreisobmannes Widerspruch einzulegen.

10.5 Der „schusselige" Zahnarzt

Zahnärzte melden ihrer Kassenzahnärztlichen Vereinigung monatlich die Zahl der behandelten, bei Primärkassen und Ersatzkassen versicherten Patienten. Diese Meldungen dienen als Grundlage für die Berechnung und Zahlung von Abschlägen auf die Quartalsabrechnung.

Nun kommt es gelegentlich vor, daß einzelne Zahnärzte vergessen, diese sog. Fallmeldungen mit ihrem Praxisstempel zu versehen; die Mitarbeiter der Kassenzahnärztlichen Vereinigung haben dann erhebliche Probleme, eine Zuordnung aufgrund der schwer lesbaren Unterschrift vorzunehmen. Bisweilen ist diese Zuordnung völlig unmöglich; eine Abschlagszahlung kann dann nicht geleistet werden.

Es liegt im Interesse der Kassenzahnärztlichen Vereinigungen, derartige Erschwernisse ihrer Arbeit zu vermeiden, und so ist nichts dagegen einzuwenden, daß eine dieser Körperschaften in einem Rundschreiben auf das Problem hinwies und an die Zahnärzte appellierte, in den Fallmeldungen doch bitte den Absender anzugeben. Sie tat aber noch ein übriges und lichtete drei mit unleserlicher Unterschrift versehene Fallmeldungen in dem Rundschreiben ab.

Einer der betroffenen Zahnärzte war der Meinung, daß die Kassenzahnärztliche Vereinigung personenbezogene Daten veröffentlichte, denn seine für deren Mitarbeiter unleserliche Unterschrift sei Kollegen und anderen Beziehern des Rundschreibens durchaus bekannt, eine Zuordnung der gemeldeten Fallzahlen zu seiner Praxis also möglich. Es handele sich auch um sensible Daten, denn aus den Fallzahlen ergebe sich die Praxis- und Umsatzgröße in hinreichender Genauigkeit.

Der LfD beurteilte dies ebenso, stieß indessen mit seiner Stellungnahme auf das völlige Unverständnis der Kassenzahnärztlichen Vereinigung, die bestritt, daß die Voraussetzungen für die Anwendung datenschutzrechtlicher Vorschriften vorlagen. Der LfD bekräftigte seine Rechtsauffassung unter Hinweis auf das Sozialgeheimnis, das auch die Praxisdaten von Ärzten schützt. Er wies darauf hin, daß die Fallmeldungen die sachlichen Verhältnisse von Ärzten betrafen, die, auch wenn die Unterschrift nicht lesbar war, durch Schriftvergleich oder aufgrund direkter Kenntnis des Schriftzuges jedenfalls für einzelne Empfänger des Rundschreibens identifizierbar waren.

In einem folgenden Rundschreiben berichtete die Kassenzahnärztliche Vereinigung über die Beschwerde des Zahnarztes und die Stellungnahme des LfD. Es sei ihr, so fügte sie an, aus der Kenntnis der inneren Zusammenhänge heraus nicht ersichtlich, welche besonderen betrieblichen oder persönlichen Rückschlüsse aus dem Inhalt der Veröffentlichung gezogen werden könnten, außer denen auf eine mögliche „Schusseligkeit" des Absenders. Um die Kollegen, die noch immer nicht wußten, um welchen Zahnarzt es sich handelte, nicht länger im unklaren zu lassen, wurde auch noch dessen frühere Gutachtertätigkeit erwähnt.

Hier schaltete sich nun das Ministerium für Arbeit, Soziales und Gesundheit als Aufsichtsbehörde ein. In einem Schreiben an die Kassenzahnärztliche Vereinigung bestätigte es die Rechtsauffassung des LfD in vollem Umfange und bezeichnete den Inhalt der Veröffentlichung, die in Kenntnis dieser Rechtsauffassung erfolgte, als schlechthin unvertretbar. Mit dem Wesen einer Kassenzahnärztlichen Vereinigung als Körperschaft des öffentlichen Rechts und deren mitgliederbezogenen Aufgaben sei es nicht vereinbar, daß anstelle eines Zeichens der Einsicht in den begangenen Rechtsverstoß oder eines Wortes des Bedauerns gegenüber dem Betroffenen diesem mit dem Vorwurf möglicher „Schusseligkeit" gewissermaßen die Verantwortung für die Rechtsverletzung zugeschoben werde.

10.6 Verwendung von Disketten mit Patientendaten für die Fehleranalyse

Niedergelassene Ärzte setzen für die Abrechnung mit den Kassenärztlichen Vereinigungen zunehmend die automatisierte Datenverarbeitung ein. Sie verwenden Softwareprodukte unterschiedlicher Hersteller. Gelegentlich treten Verarbeitungsfehler auf, die entweder vom Arzt unmittelbar oder von den Kassenärztlichen Vereinigungen nach Eingang der Abrechnungsdisketten bemerkt werden. Der LfD erhielt Hinweise auf Fälle, in denen Ärzte Disketten mit Patientendaten, bei deren Verarbeitung Fehler auftraten, zum Zwecke der Fehleranalyse an die Softwarehersteller weitergegeben haben.

Diese Verfahrensweise ist vor dem Hintergrund der gesetzlichen Bestimmungen zum Schutze des Patientengeheimnisses (§ 2 der Berufsordnung für die Ärzte, § 203 StGB) bedenklich, denn eine gesetzliche Offenbarungsbefugnis besteht nicht und eine Zustimmung der Patienten liegt in der Regel ebenfalls nicht vor. Die Kassenärztliche Bundesvereinigung hat bezüglich der vergleichbaren Problematik der Fernwartung in ihren „Empfehlungen zu Datenschutz und Schweigepflicht beim EDV-Einsatz

in der kassenärztlichen Praxis" vom 13. Oktober 1989 die Auffassung vertreten, daß die Fernwartung von EDV-Software in Arztpraxen unzulässig ist, wenn nicht ausgeschlossen werden kann, daß dabei auf patientenbezogene Daten zugegriffen wird (CuR 1990, 558). Keine Einwendungen bestehen gegen die Durchführung der Fehleranalyse in der Arztpraxis unter Aufsicht des Arztes oder seiner Mitarbeiter.

Durch Veröffentlichung der Stellungnahme im Ärzteblatt entsprach die Ärztekammer der Empfehlung des LfD, die Ärzte in geeigneter Weise über diese Rechtsauffassung zu informieren.

10.7 Aufbewahrung von Patientenunterlagen

Ein Arzt, der bis zu seinem Tod eine Privatklinik betrieb, hinterließ größere Mengen von Aufzeichnungen – Patientenakten, Röntgenbilder, Patientenkartei –. Diese Materialien verblieben in dem Gebäude der Klinik, das später als Altenheim genutzt wurde. Der LfD erfuhr hiervon durch einen früheren Patienten des verstorbenen Arztes, der sich beschwerte, weil er für einen Rechtsstreit dringend Röntgenaufnahmen benötigte, aber niemand bereit war, diese herauszusuchen und auszuhändigen.

Nach § 11 Abs. 4 der Berufsordnung soll der Arzt dafür Sorge tragen, daß seine ärztlichen Aufzeichnungen und Untersuchungsbefunde nach Aufgabe der Praxis in gehörige Obhut gegeben werden. Unter Hinweis auf die der Ärztekammer zustehende Regelungsbefugnis konnte der LfD bewirken, daß die zuständige Bezirksärztekammer nähere Bestimmungen zur weiteren sicheren Aufbewahrung der Materialien getroffen hat.

Das Ministerium für Arbeit, Soziales und Familie beabsichtigt, die Novellierung des Heilberufsgesetzes für eine Klarstellung zu nutzen. Die Ärztekammer soll verpflichtet werden, in der Berufsordnung für die Ärzte nähere satzungsrechtliche Regelungen über die Aufbewahrung und Weitergabe der in Ausübung des Berufes gefertigten Aufzeichnungen zu treffen.

Hinsichtlich der Aufbewahrung von Röntgenaufnahmen ist § 28 der Röntgenverordnung zu beachten. Absatz 4 Nr. 2 statuiert für Röntgenaufnahmen eine Aufbewahrungspflicht für die Zeitdauer von zehn Jahren. Die zuständige Behörde – dies ist in Rheinland-Pfalz das Gewerbeaufsichtsamt – kann verlangen, daß im Falle der Praxisaufgabe die Aufzeichnungen und Aufnahmen an einer von ihr bestimmten, der ärztlichen Schweigepflicht unterliegenden Stelle hinterlegt werden. Im konkreten Falle ist diese Aufgabe dem örtlich zuständigen Gesundheitsamt übertragen worden. Diesem obliegt nunmehr die Auskunftserteilung nach § 18 LDSG.

10.8 Datenschutz bei der Einführung und Verwendung einer Patientenchipkarte in Neuwied/Rhein

Im September 1995 begann in der Stadt Neuwied/Rhein der Modellversuch „Persönliche Patientenkarte". Die Projektverantwortung tragen die Kassenärztliche Vereinigung Koblenz, das Zentralinstitut für die kassenärztliche Versorgung und die Bundesvereinigung Deutscher Apothekerverbände. Sie bezwecken mit der Einführung der Patientenchipkarte eine Verbesserung der Informationsübermittlung zwischen den Ärzten sowie zwischen diesen und den Apothekern, die sich an dem Modellversuch beteiligen. So soll der Arzt beispielsweise auch ohne zeitaufwendiges Befragen eines Patienten über Vorerkrankungen oder Behandlungsrisiken informiert werden, er soll sehen können, welche Medikamente regelmäßig eingenommen werden und ob unerwünschte Wechselwirkungen mit Arzneimitteln bestehen, die bereits früher verschrieben wurden. Apotheker sollen sich beispielsweise über den Umfang der Selbstmedikation informieren können und in den Stand gesetzt werden, den Patienten über mögliche Unverträglichkeiten mit ärztlich verschriebenen Medikamenten zu unterrichten.

Die Besonderheit des Projekts besteht darin, daß auf einer Chipkarte sowohl Befunddaten wie auch Medikationsdaten gespeichert werden. Das Lesen des vollständigen Karteninhalts ist nur den Ärzten möglich; die Bediensteten in Apotheken können nur die Adreß- und Medikationsdaten zur Kenntnis nehmen und neue Medikationsdaten hinzufügen. Eine zentrale Speicherung von Daten der Karteninhaber erfolgt nicht.

Gespeichert werden auf der Karte die Adreßangaben, Befundangaben (Allergien, chronische Krankheiten, bösartige Neubildungen, chirurgische Eingriffe, Fehlbildungen, Transplantationen, kontinuierliche Behandlungsmittel, Blutgruppe, Impfstatus und Röntgenstatus) sowie alle Medikamente, die ein Patient über die Apotheke bezieht.

Grundsätzlich birgt die Verwendung von Chipkarten im allgemeinen und von Patientenchipkarten im besonderen eine Fülle datenschutzrechtlicher Probleme. Hierzu gehören

- die mögliche zweckwidrige Verwendung (z. B. Arbeitgeber und Lebensversicherung verlangen ihre Vorlage, um sich über die gesundheitliche Verfassung zu informieren),
- die möglicherweise nicht ausreichende Absicherung (bei unzureichender Zugangssicherung kann der Inhalt einer Chipkarte im Falle des Verlustes von Unbefugten gelesen werden),
- sozialer Druck zur Verwendung der Chipkarte (der Arzt oder Apotheker wünscht, daß sich seine Patienten oder Kunden der Chipkarte bedienen und seine Arbeit damit erleichtern) oder
- die Entstehung zentraler Datensammlungen bei den Stellen, die die Eintragungen auf den Chipkarten vornehmen.

Der LfD wurde bei der Entwicklung des Neuwieder Modellversuchs zu einem frühen Zeitpunkt beratend hinzugezogen. Seine Empfehlungen bezogen sich insbesondere auf die rechtlichen Voraussetzungen der Teilnahme: Unterrichtung der Betroffenen über den Zweck der Verwendung von Chipkarten sowie die Erhebung und weitere Verarbeitung ihrer Daten; Teilnahme nur mit schriftlicher Einverständniserklärung – und auf die technisch-organisatorische Verfahrenssicherung. In beiden Bereichen wurden Ergebnisse erzielt, die im Modellversuch akzeptabel sind.

Nach Abschluß der Versuchsphase kann die Anwendung aus der Sicht des LfD nur dann weitergeführt werden, wenn die technischen Schutzvorkehrungen noch weiter verbessert und wichtige gesetzgeberische Entscheidungen getroffen werden. So müßte der Gesetzgeber beispielweise regeln, daß die auf der Patientenchipkarte gespeicherten medizinischen Daten ebenso gegen Beschlagnahme und unbefugte Kenntnisnahme geschützt sind wie die beim Arzt gespeicherten Daten. Im Rahmen der Novellierung des Heilberufegesetzes hat der LfD empfohlen, in die Berufsordnung für die Ärzte nähere Bestimmungen über den Datenschutz bei der Einführung und Verwendung von Patientenchipkarten aufzunehmen.

In einer Pressemitteilung hat der LfD die Bevölkerung der Versuchsregion über die Bedingungen der Teilnahme und des Einsatzes der Patientenchipkarte wie folgt informiert:

- Die Teilnahme an dem Modellversuch ist völlig freiwillig. Aus einer Verweigerung der Einwilligung zur Teilnahme dürfen keine Nachteile entstehen. Ärzte oder Apotheker, die Gegenteiliges behaupten oder Patienten bedrängen oder nötigen, handeln pflichtwidrig.
- Sofern eine Persönliche Patientenkarte ausgestellt wurde, kann der Patient völlig frei darüber entscheiden, ob und ggf. welchen Ärzten oder Apothekern er diese vorlegen will. Wer auch immer nach dem Besitz der Persönlichen Patientenkarte fragt: Der Besitz der Karte braucht nicht offenbart zu werden.
- Patienten können jederzeit von ihren Ärzten oder Apothekern verlangen, daß sie ihnen zeigen, welche Daten gespeichert sind, und daß diese Daten ausgedruckt werden. Dabei ist freilich zu berücksichtigen, daß nur Ärzte in der Lage sind, den gesamten Speicherinhalt zu lesen; Apotheker haben nur Zugriff zu den Adreßdaten und zu den Aufzeichnungen über die Medikation.
- Die Projektverantwortlichen haben versichert, daß die auf der Persönlichen Patientenkarte gespeicherten Daten an keiner anderen Stelle zentral gespeichert werden. Auch die Adressen der Teilnehmer an dem Modellversuch werden nicht zentral gespeichert. Dies wird vom LfD überwacht.
- Wer der Ansicht ist, in seinen Datenschutzrechten verletzt zu sein, kann sich jederzeit an den LfD wenden.

11. Sozialdatenschutz

11.1 Krankenkassen, Kassenärztliche Vereinigungen

11.1.1 Rechtsfragen bei der Anwendung von Vorschriften des SGB V

Im Berichtszeitraum häuften sich Anfragen, die sich auf die Zusammenarbeit des Medizinischen Dienstes mit Ärzten und Krankenkassen nach § 276 SGB V und die Mitteilungspflichten des Medizinischen Dienstes nach § 277 SGB V bezogen. In einer Reihe von Fällen wurde beklagt, daß bei der Anforderung für den Medizinischen Dienst bestimmter Gutachten verlangt wurde, diese zunächst den Krankenkassen vorzulegen. Nach Erörterung mit der Geschäftsleitung des Medizinischen Dienstes nahm der LfD zu diesen Rechtsfragen wie folgt Stellung:

1. Nach § 276 Abs. 2 Satz 1 zweiter Halbsatz SGB V sind die Leistungserbringer in Fällen, in denen die Krankenkassen nach § 275 Abs. 1 bis 3 eine gutachtliche Stellungnahme oder Prüfung durch den Medizinischen Dienst der Krankenversicherung (MDK) veranlaßt haben, verpflichtet, Sozialdaten auf Anforderung des MDK unmittelbar an diesen zu übermitteln, soweit dies für die gutachtliche Stellungnahme und Prüfung erforderlich ist. Diese Regelung läßt keinen Raum für eine Übermittlung von Sozialdaten auf der Grundlage einer Einwilligung der Betroffenen.

2. Es sind aus der Sicht des Datenschutzes keine Einwendungen dagegen zu erheben, daß die Leistungserbringer von den Krankenkassen unmittelbar ersucht werden, die für die gutachtliche Stellungnahme und Prüfung des MDK erforderlichen Sozialdaten unmittelbar an den MDK zu übermitteln. Es ist die Aufgabe der Krankenkassen, die in Wahrnehmung eines Mandats des MDK tätig werden, die Anforderungen unter Beachtung des Erforderlichkeitsgrundsatzes inhaltlich zu konkretisieren.

3. Der Befugnis zur Datenerhebung und -erfassung nach § 284 Abs. 1 Satz 1 Nr. 4 SGB V kann eine Übermittlungspflicht der Leistungserbringer nicht entnommen werden.

4. § 276 Abs. 1 Satz 1 SGB V, der die Krankenkassen verpflichtet, dem MDK die für die Beratung und Begutachtung erforderlichen Unterlagen vorzulegen und Auskünfte zu erteilen, gibt den Krankenkassen keine Befugnis, Daten für diesen Zweck zu

erheben. Es dürfen nur die von den Krankenkassen aus anderer Veranlassung, beisp. nach § 284 SGB V, erhobenen und erfaßten Daten übermittelt werden.

5. § 276 Abs. 2 Satz 1 zweiter Halbsatz SGB V erlaubt nicht nur die Übermittlung vom Arzt selbst erhobener Daten/Berichte, sondern auch die Übermittlung von Fremdbefunden/Krankenhausberichten/Stellungnahmen von Kurkliniken usw.

6. Die Datenübermittlung des MDK an die Krankenkasse richtet sich nach § 277 Abs. 1 SGB V. Ob auch Anamnesen aus den Gutachten des MDK an die Krankenkasse übermittelt werden sollen, ist je nach Gutachtenauftrag an den MDK und der sich daraus ergebenden Erforderlichkeit für die Erfüllung von Aufgaben der Krankenkasse zu beurteilen.

7. Nach § 277 Abs. 1 Satz 3 SGB V hat der Versicherte ein Widerspruchsrecht gegen die Mitteilung des Befundes an die Leistungserbringer. Die Information über das Widerspruchsrecht erfolgt – wenn der Versicherte zur Begutachtung einbestellt wird – durch den MDK und wird dokumentiert.

8. § 276 Abs. 2 SGB V regelt auch die Datenübermittlung durch Krankenhäuser an den MDK.

Dieser in gleichlautenden Schreiben an den Medizinischen Dienst, die Kassenärztlichen Vereinigungen und die Krankenkassen-Landesverbände vertretenen Rechtsmeinung wurde nicht widersprochen; der LfD geht davon aus, daß sie in allen einschlägigen Verfahren beachtet wird.

11.1.2 Eingeschränkter Zugriff auf Versichertendaten bei landesweiten oder überregionalen gesetzlichen Krankenkassen

Die gesetzlichen Krankenkassen schließen sich zunehmend zu landesweiten oder überregionalen gesetzlichen Krankenkassen zusammen. So ist zum Beispiel die AOK – Die Gesundheitskasse – Rheinland-Pfalz 1994 aus dem Zusammenschluß von zuvor rund 30 selbständigen gesetzlichen Krankenkassen entstanden; weitere Zusammenschlüsse fanden im Bereich der Innungskrankenkassen statt.

Als Serviceleistung bieten die landesweiten oder überregionalen Kassen ihren Versicherten die Möglichkeit, Versichertenangelegenheiten bei jeder Geschäftsstelle (Regionaldirektion) bearbeiten zu lassen. Voraussetzung hierfür ist, daß jede dieser Stellen auf die zentral gespeicherten oder im Datenverbund verfügbaren Versichertendaten zugreifen kann.

Der LfD hält dies für datenschutzrechtlich bedenklich, sofern den Versicherten keine Gelegenheit gegeben wird, selbst zu bestimmen, welche Geschäftsstellen zugriffsberechtigt sein sollen.

Er hält in Übereinstimmung mit dem BfD und mit den LfD der übrigen Länder nur folgendes für vertretbar:

1. Geschäftsstellen einer Krankenkasse dürfen ohne schriftliches Einverständnis des Versicherten nur auf einen „Stammdatensatz" zugreifen. Dieser „Stammdatensatz" darf nur den Namen, das Geburtsdatum, die Anschrift, die Krankenversichertennummer und die betreuende Geschäftsstelle des Versicherten umfassen.

2. Lediglich eine einzige Geschäftsstelle kann umfassend auf den Datensatz eines Versicherten zugreifen, sofern der Versicherte nicht ausdrücklich und eindeutig schriftlich in derartige Zugriffsmöglichkeiten durch weitere Geschäftsstellen eingewilligt hat.

3. Vor der Einwilligung ist der Betroffene umfassend aufzuklären. Die Daten dürfen nur zweckgebunden verwendet werden.

Zum Zeitpunkt der Berichtserstellung läßt sich noch nicht absehen, ob die Krankenkassen diesen Empfehlungen folgen werden.

11.1.3 Vorlage eines polizeilichen Führungszeugnisses für die Zulassung als Kassenarzt

Ärzte, die eine Zulassung zur kassenärztlichen Tätigkeit bei den Kassenärztlichen Vereinigungen beantragen, haben ihrem Antrag nach § 18 Abs. 2 der Zulassungsordnung ein polizeiliches Führungszeugnis beizufügen. Hierbei kann es sich nicht um ein sog. Behördenführungszeugnis nach §§ 30 Abs. 5 und 31 BZRG handeln, denn dieses wird verfahrensmäßig anders behandelt als ein Führungszeugnis, das dem Betroffenen selbst erteilt wird. Ein Behördenführungszeugnis kann einem Zulassungsantrag nicht beigefügt werden; sein Inhalt gelangt auf andere Weise zur Kenntnis der Behörde oder sonstigen öffentlichen Stelle, für die es bestimmt ist.

Den Kassenärztlichen Vereinigungen war indessen daran gelegen, im Zusammenhang mit Zulassungsanträgen Behördenführungszeugnisse zu erhalten, weil diese auch solche Verurteilungen und Eintragungen ausweisen, die in ein dem Betroffenen selbst erteiltes Führungszeugnis nicht aufgenommen werden.

Der LfD vertrat die Auffassung, daß, falls für die Prüfung der Zulassungsvoraussetzungen ein Behördenführungszeugnis erforderlich ist, in § 18 der Zulassungsverordnung konkret die Verpflichtung der antragstellenden Ärzte aufgenommen werden muß, die Erteilung eines solchen Führungszeugnisses zu beantragen, wie dies z. B. in § 8 Abs. 3 StVZO geregelt ist. Nach der gegenwärtigen Rechtslage sei indessen die Anforderung eines Behördenführungszeugnisses nicht zulässig.

Die Rechtsauffassung des LfD wurde von den Kassenärztlichen Vereinigungen bzw. von deren Zulassungsausschüssen anerkannt.

11.1.4 Bekanntgabe von Patientendaten durch den Prüfarzt einer Kassenärztlichen Vereinigung

Bei den Kassenärztlichen Vereinigungen sind nach § 106 Abs. 4 SGB V Prüfungsausschüsse gebildet, die darüber entscheiden, ob ein Arzt oder eine ärztlich geleitete Einrichtung gegen das Wirtschaftlichkeitsgebot verstoßen hat und welche Maßnahmen zu treffen sind. Den Prüfungsausschüssen gehören Vertreter der Ärzte und der Krankenkassen in gleicher Zahl an. Bei der Wahrnehmung ihrer Aufgaben werden den Mitgliedern der Prüfungsausschüsse Sozialdaten bekannt, die von Mitgliedsärzten im Rahmen der Leistungsabrechnung an die Kassenärztlichen Vereinigungen übermittelt wurden.

Ein Arzt beschwerte sich beim LfD darüber, daß ein Prüfarzt Informationen, die ihm bei seiner Prüftätigkeit bekannt geworden waren, als Beweismittel in einem von ihm beantragten Strafverfahren gegen diesen Arzt wegen Abrechnungsbetrugs nutzte. Das Ermittlungsverfahren sei – so teilte der Arzt mit – von der Staatsanwaltschaft zwar nach § 170 Abs. 2 StPO eingestellt worden; unabhängig davon sei aber zu beklagen, daß durch die Übermittlung von Patientendaten an die Staatsanwaltschaft das Sozialgeheimnis verletzt worden sei.

Nach eingehender Sachverhaltsprüfung, die wegen der zögerlichen Bearbeitung durch die Kassenärztliche Vereinigung längere Zeit in Anspruch nahm, beurteilte der LfD den Vorgang wie folgt:

Die den Prüfgremien bei der KV für die Wahrnehmung ihrer Aufgaben zur Verfügung gestellten Daten sind als Sozialdaten durch das Sozialgeheimnis (§ 35 SGB I) geschützt. Eine Übermittlung, auch für Zwecke der Strafverfolgung, ist nur bei Vorliegen der Voraussetzungen der §§ 68 ff. SGB X zulässig.

Zwar könnte nach § 69 Abs. 1 SGB X eine Übermittlung von Sozialdaten für Zwecke der Strafverfolgung grundsätzlich zulässig sein. Voraussetzung hierfür wäre indessen, daß die für die KV insoweit entscheidungs- und handlungsbefugten Organe tätig werden. Dies war jedoch nicht der Fall, so daß bei objektiver Betrachtung von der Unzulässigkeit einer Übermittlung der Sozialdaten auszugehen war. Der LfD beanstandete dies nach § 25 LDSG als Verstoß gegen datenschutzrechtliche Bestimmungen und unterrichtete die zuständige oberste Aufsichtsbehörde.

11.1.5 Diagnoseangaben auf Hilfsmittelverordnungen

Zwischen einer Kassenärztlichen Vereinigung und einer Ersatzkasse wurde die Frage diskutiert, ob der Kassenarzt auf Hilfsmittelverordnungen die Diagnose anzugeben hat. Die Kassenärztliche Vereinigung vertrat die Auffassung, daß die Angabe der Diagnosen aus Datenschutzgründen nur dann zulässig sei, wenn diese für die Auswahl, Herstellung oder Anpassung von Hilfsmitteln relevant sind. Die Ersatzkasse hingegen meinte, daß eine grundsätzliche Verpflichtung zur Angabe der Diagnose bestehe.

Der LfD, um Stellungnahme gebeten, verwies auf die Heilmittel- und Hilfsmittel-Richtlinien, die in Nummer 25 die Regelung enthalten, daß der Kassenarzt die Diagnose angeben soll. Diese Sollbestimmung berücksichtigt nach seiner Auffassung, daß das SGB V keine ausdrückliche Befugnis zur Übermittlung der Diagnose enthält und durch Richtlinien des Bundesausschusses der Ärzte und Krankenkassen nicht in das informationelle Selbstbestimmungsrecht der Patienten eingegriffen werden kann. Demzufolge ist die Sollbestimmung dahin gehend auszulegen, daß die Angabe der Diagnose auf der Verordnung in solchen Fällen erfolgt, in denen es zu den Mitwirkungspflichten der Patienten i. S. der §§ 60 ff. SGB I gehört, der Angabe von leistungserheblichen Tatsachen zuzustimmen. Dies kann nur ausnahmsweise in den von der Kassenärztlichen Vereinigung genannten Fällen in Betracht kommen.

11.2 Sozialhilfe, Kinder- und Jugendhilfe

11.2.1 Offenbarung von Sozialdaten gegenüber den Rechnungsprüfungsausschüssen von Ortsgemeinden

Der zulässige Umfang der Sozialdatenübermittlung an Ortsgemeinden und insbesondere auch an Rechnungsprüfungsausschüsse von Ortsgemeinden ist immer wieder Gegenstand von Anfragen an den LfD. Er beurteilt die Zulässigkeit wie folgt:

Örtliche Träger der Sozialhilfe sind nach § 1 AGBSHG die kreisfreien Städte und die Landkreise; nach § 4 Abs. 1 AGBSHG können die Landkreise bestimmen, daß Verbandsgemeinden oder verbandsfreie Gemeinden Sozialhilfeaufgaben ganz oder teilweise durchführen und dabei in eigenem Namen entscheiden. Demnach sind Ortsgemeinden weder Sozialhilfeträger noch Delegationsträger. Sie sind lediglich zur Kostenerstattung in dem durch § 8 AGBSHG bestimmten Umfange verpflichtet.

Informationen über den Leistungsbezug (Sozialdaten) sind als Sozialgeheimnis durch § 35 SGB I geschützt. Die Weitergabe personenbezogener Daten über den Leistungsbezug durch die Verbandsgemeinde an die Ortsgemeinde stellt eine Übermittlung dar, die nur unter den Voraussetzungen des Zweiten Buchs des SGB X zulässig ist. Die in Betracht kommende Bestimmung ist § 69 Abs. 1 Nr. 1 SGB X, die eine Übermittlung zuläßt, wenn die Daten für die Erfüllung der Zwecke, für die sie erhoben worden sind oder für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach dem Sozialgesetzbuch oder einer solchen Aufgabe des Empfängers, wenn er eine in § 35 SGB I genannte Stelle ist, erforderlich sind. Zweck der Erhebung von Sozialdaten ist die Sozialhilfegewährung durch den Leistungsträger; eine Übermittlung an die Ortsgemeinde ist hierdurch nicht gedeckt. Die zweite Alternative läßt beispielsweise zu, daß Sozialdaten von der Verbandsgemeindeverwaltung an den Ortsbürgermeister übermittelt werden, damit dieser aufgrund seiner besonderen Kenntnisse der örtlichen Verhältnisse die Richtigkeit von Angaben prüft. Der Ortsbürgermeister darf diese ihm übermittelten Sozialdaten nach § 78 Abs. 1 SGB X nur zu dem Zweck verarbeiten oder nutzen, zu dem sie ihm befugt übermittelt worden sind. Er ist ebenso an das Sozialgeheimnis des § 35 SGB I gebunden wie die Verbandsgemeinde als Delegationsträger. Die letzte Alternative des § 69 Abs. 1 Nr. 1 SGB X scheidet als Übermittlungsgrundlage schon deshalb aus, weil die Ortsgemeinde kein Sozialleistungs- oder Delegationsträger ist.

Eine Übermittlung von personenbezogenen Daten über Leistungsempfänger zum Zwecke der Prüfung der Kostenerstattungspflicht nach § 8 AGBSHG kann unter keine Übermittlungsbestimmung des SGB X subsumiert werden, denn sie ist nicht erforderlich. In der Antwort auf eine Kleine Anfrage (Drucksache 9/2127) wies die Landesregierung darauf hin, daß den Ortsgemeinden zum Zwecke der Haushaltsplanung lediglich die Anzahl der Sozialhilfeempfänger aus der jeweiligen Ortsgemeinde, die Summe der bisher pro Haushalt geleisteten Zahlungen und die voraussichtliche Steigerungsrate mitgeteilt werden darf. Die Rechnungsprüfung auf der Ebene der Ortsgemeinde muß sich ebenfalls mit diesen Daten begnügen. Beim Ortsbürgermeister evtl. vorhandene weitere Informationen (s. oben) dürfen aus dem gleichen Grunde (fehlende Erforderlichkeit) nicht genutzt werden, der auch eine Übermittlung ausschließt.

11.2.2 Übermittlung von Kfz-Zulassungsdaten an Sozialämter

Im 14. Tätigkeitsbericht wurde unter Tz. 11.3.5 dargestellt, unter welchen gesetzlichen Voraussetzungen Sozialämter bei Kfz-Zulassungsstellen recherchieren dürfen, ob Kraftfahrzeuge auf Sozialleistungsempfänger zugelassen sind. Der LfD vertrat die Auffassung, daß Sozialleistungsträger nicht gehindert sind, den Sachverhalt in konkreten Verdachtsfällen zu ermitteln (§ 20 SGB X), und daß sie im Rahmen dieser Ermittlungen auch befugt sind, Einzelanfragen an die Kfz-Zulassungsstelle zu richten und damit die Tatsache des Sozialhilfebezugs zu offenbaren. Die Zulassungsstellen ihrerseits sind befugt, dem Sozialamt Auskünfte zu erteilen, wenn die Rückforderung von Sozialleistungen in Höhe von mehr als 1 000,– DM beabsichtigt ist (§ 39 StVG) oder wenn die Übermittlung zur Verfolgung von Straftaten oder von Ordnungswidrigkeiten erforderlich ist (§ 35 Abs. 1 Nr. 2 und 3 StVG). Die genannten Vorschriften boten also auch in der Vergangenheit schon hinreichende Möglichkeiten, nach Sachverhaltsaufklärung Strafverfolgungsmaßnahmen wegen Sozialhilfebetrugs einzuleiten.

Dennoch wurde durch das Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms vom 23. Juni 1993 eine Änderung des BSHG vorgenommen, die den Trägern der Sozialhilfe die Befugnis gibt „zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe Daten von Personen, die Leistungen nach diesem Gesetz beziehen, bei anderen Stellen ihrer Verwaltung, bei ihren wirtschaftlichen Unternehmen und bei den Kreisen, Kreisverwaltungsbehörden und Gemeinden zu überprüfen, soweit diese für die Erfüllung dieser Aufgaben erforderlich sind" (§ 117 Abs. 3 BSHG). Die Träger der Sozialhilfe dürfen für die Überprüfung nur die in § 117 Abs. 1 Satz 2 BSHG genannten Daten übermitteln. Die ersuchte Stelle darf ebenfalls nur ganz bestimmte, im Gesetz aufgezählte Daten übermitteln; sie ist zur Auskunft verpflichtet und hat die ihr im Rahmen der Überprüfung übermittelten Daten nach Erteilung der Auskunft unverzüglich zu löschen.

Auf der Grundlage der erwähnten Vorschrift nahmen mehrere größere Städte eines benachbarten Bundeslandes einen automatisierten Abgleich von Daten der Sozialämter und der Kfz-Zulassungsstellen vor. Dies wurde von dem zuständigen LfD mit dem Argument beanstandet, daß eine Überprüfung zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe nur erlaubt sei, soweit die zu überprüfenden Daten für die Erfüllung ihrer Aufgaben erforderlich sind. Der Erforderlichkeit begriffsimmanent sei die Einzelfallbezogenheit. Wenn also der Gesetzgeber die Überprüfung der Eigenschaft als Kraftfahrzeughalter an die Erforderlichkeit binde, so habe er damit eine Überprüfung nur im Einzelfall zulassen wollen. Ergänzend wurde diese Auffassung auf die unterschiedliche Formulierung der Absätze 1 und 2 des § 117 BSHG, die einen Datenabgleich in anderen Fällen zuläßt, im Vergleich zu der Formulierung in Absatz 3 gestützt.

Der LfD als die für Rheinland-Pfalz zuständige Kontrollbehörde vertritt die Auffassung, daß die fehlende Normenklarheit der genannten Vorschrift bezüglich des Datenabgleichs nicht zu Lasten der Sozialleistungsempfänger gehen darf. Auch bei einer engen Auslegung bietet die Vorschrift hinreichende Möglichkeiten, das gesetzgeberische Ziel zu erreichen.

Das Ministerium für Arbeit, Soziales und Gesundheit teilte auf Anfrage mit, daß § 117 BSHG in der Verwaltungspraxis in Rheinland-Pfalz allenfalls eine untergeordnete Rolle spiele. Ein automatisierter Datenabgleich finde „offenbar" nicht statt. Eine Nachfrage erfolge nur, wenn konkrete Anhaltspunkte dafür vorlägen, daß Leistungen nach dem BSHG zu Unrecht bezogen

würden. Angesichts dieser Sachlage und der Tatsache, daß die Sozialhilfebehörden über die Problematik mündlich in Dienstbesprechungen und Arbeitsgemeinschaften informiert worden seien, werde keine Notwendigkeit gesehen, den Sachverhalt in einem Rundschreiben erneut darzustellen.

11.2.3 Steuerliche Erfassung der ausgezahlten Mieten für Asylbegehrende und andere Sozialleistungsempfänger

Im 14. Tätigkeitsbericht nahm der LfD unter Tz. 11.3.4 zur Zulässigkeit der Offenbarung von Vermieteradressen an die Steuerfahndung Stellung. Er vertrat die Auffassung, daß es angesichts der höchstrichterlichen Rechtsprechung nicht durchsetzbar sein dürfte, Auskunftsersuchen der Steuerfahndung zu Vermieteradressen unter Berufung auf Datenschutzgründe abzulehnen. Das Ministerium der Finanzen konkretisierte auf Anfrage des Städtetages den Umfang der Auskunftserteilung und wies ergänzend darauf hin, daß dem Arbeitsaufwand der Kommunen dadurch Rechnung getragen werden könne, daß die notwendigen Ermittlungen durch Beamte der Steuerfahndungsstelle unterstützt werden. Der LfD stellte in einem ergänzenden Hinweis an den Städtetag und die zuständige oberste Landesbehörde klar, daß es mit den gesetzlichen Bestimmungen zum Schutze des Sozialgeheimnisses nicht zu vereinbaren ist, daß den Beamten der Steuerfahndungsstellen Sozialleistungsakten zur Einsichtnahme oder zur Durchsicht übergeben werden.

11.2.4 Übermittlung von Sozialdaten an Heimträger

Die ganz überwiegende Zahl der Sozialhilfeträger leitet bei Heimunterbringung die Rentenansprüche der Leistungsempfänger über und erteilt eine Übernahmeerklärung für die Unterbringungskosten in voller Höhe. In diesen Fällen ist es zur Aufgabenerfüllung des Sozialleistungsträgers nicht erforderlich und deshalb unzulässig, daß die Einkünfte des Hilfeempfängers gegenüber dem Heimträger offenbart werden.

Nur vereinzelt wird von einer Überleitung abgesehen und nur eine Kostenübernahmeerklärung für die verbleibenden Restkosten gegenüber dem Heimträger erteilt. Auch dieses Verfahren ist zulässig; es ist unvermeidbar, daß der Heimträger in solchen Fällen Kenntnis davon erhält, welche Eigenmittel dem Hilfeempfänger zur Verfügung stehen.

In mehreren Fällen, in denen die Heimträger routinemäßig über die Leistungsgewährung durch Übersendung einer Ablichtung des Leistungsbescheids unterrichtet wurden, führten die Empfehlungen des LfD zu einer Verfahrensänderung.

11.2.5 Sozialhilfe; Rechtswahrungsanzeige

Die Rechtswahrungsanzeige nach § 91 Abs. 3 BSHG bewirkt den Übergang von Unterhaltsansprüchen des Hilfeempfängers auf den Sozialhilfeträger. Voraussetzung dieses Übergangs ist, daß dem Unterhaltspflichtigen der Bedarf unverzüglich nach Kenntnis des Trägers der Sozialhilfe schriftlich mitgeteilt wurde. Von datenschutzrechtlicher Relevanz ist eine solche Rechtswahrungsanzeige deshalb, weil dem Adressaten die Gewährung von Sozialhilfe an eine bestimmte Person offenbart wird. In einem dem LfD bekanntgewordenen Fall war den Eltern einer schwangeren Hilfeempfängerin eine Rechtswahrungsanzeige zugestellt worden. Der LfD rügte dies als Verstoß gegen die gesetzlichen Bestimmungen zum Schutze des Sozialgeheimnisses mit folgender Begründung:

Mit der Bekanntgabe des Sozialleistungsbezugs an die Eltern der Hilfeempfängerin wurden Sozialdaten offenbart, die durch das Sozialgeheimnis (§ 35 SGB I) geschützt sind. Die Zulässigkeit der Offenbarung bestimmt sich nach §§ 67 ff. SGB X, konkret nach § 69 Abs. 1 Nr. 1. Sie könnte dann in Betracht kommen, wenn sie zur Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach dem SGB erforderlich ist.

Nach § 91 Abs. 1 BSHG ist der Übergang eines Anspruchs gegen Verwandte ersten Grades einer Hilfeempfängerin ausgeschlossen, wenn diese schwanger ist oder ihr leibliches Kind bis zur Vollendung seines sechsten Lebensjahres betreut. Eine Heranziehung, die diese Grenzen nicht beachtet, ist also unwirksam (Schellhorn/Jirasek/Seipp, Kommentar zum BSHG, RdNr. 55 zu § 91). Hieraus folgt, daß eine Rechtswahrungsanzeige zur Vorbereitung einer Überleitung von Unterhaltsansprüchen nicht erforderlich und die damit verbundene Offenbarung von Sozialdaten demzufolge unzulässig ist.

Eine (Rechtswahrungs-)Anzeige an die Unterhaltspflichtigen könnte aber auch zu dem Zweck erfolgen, diese auf die grundsätzlich bestehende Leistungspflicht gegenüber dem Unterhaltsberechtigten hinzuweisen mit dem Ziel, im Leistungsfalle dem Grundsatz des Nachranges der Sozialhilfe (§ 2 Abs. 1 BSHG) Geltung zu verschaffen. Hierzu wird in der Literatur (a. a. O., RdNr. 57) die Auffassung vertreten, daß bei der Gewährung von Sozialhilfe tatsächlich eingehende Unterhaltsleistungen von Unterhaltspflichtigen, die über § 91 hinausgehen, nur dann berücksichtigt werden dürften, wenn die Leistungen des Unterhaltsschuldners ohne ihr Zutun erbracht worden sind. Es wäre unzulässig, wenn der Träger der Sozialhilfe die Vorschrift, die der Gesetzgeber mit dem Ziel des Schutzes des Unterhaltsschuldners in § 91 eingefügt hat, durch andere von ihm veranlaßte oder geförderte Formen der Heranziehung unterlaufen würde. Im übrigen dürfte die Geltendmachung des nach § 91 Abs. 1 nicht überleitungsfähigen Teils des Unterhaltsanspruchs direkt durch den Hilfeempfänger regelmäßig schon deshalb nicht möglich

sein, weil ein Unterhaltsbedarf nicht mehr besteht, da er (in Höhe des nicht überleitungsfähigen Teils) durch die insoweit dem betreffenden Unterhaltsschuldner gegenüber vorrangige Sozialhilfe abgedeckt ist (a. a. O., RdNr. 59 m. w. N., insoweit enger die Rechtsprechung des BGH, die streng vom Nachrang der Sozialhilfe nach § 2 ausgeht und Rückwirkungen auf das Unterhaltsrechtverhältnis ausschließt). Eine Rechtswahrungsanzeige war also auch insoweit nicht erforderlich, die damit verbundene Offenbarung von Sozialdaten demnach nicht zulässig.

11.2.6 Sozialdatenschutz im gerichtlichen Verfahren

Ein Sozialamt versuchte, Ansprüche gegen den unterhaltspflichtigen Sohn einer Sozialleistungsempfängerin im gerichtlichen Verfahren durchzusetzen. Im Rahmen dieses Verfahrens wurde das Sozialamt als Kläger vom Gericht aufgefordert, die Leistungsakten vorzulegen, in denen die Einkommens- und Vermögensaufstellungen der übrigen Kinder enthalten sind. Der LfD wurde gebeten, die Zulässigkeit zu überprüfen.

Bei der Unterhaltsklage handelt es sich um ein sog. Zusammenhangsverfahren i. S. des § 69 Abs. 1 Nr. 2 SGB X. Ein Zusammenhangsverfahren liegt u. a. vor, wenn eine in § 35 SGB I genannte Stelle in Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch den Anstoß zu dem Verfahren gegeben hat – z. B. durch eine Klageerhebung – (Walloth in Hauck, SGB X 1, 2, K § 69 Rz. 26). Zur Durchführung eines solchen Verfahrens dürfen nach § 69 Abs. 1 Nr. 2 SGB X Sozialdaten im erforderlichen Umfange offenbart werden.

Nach herrschender Literaturmeinung liegt die Entscheidungskompetenz hinsichtlich des Vorliegens der Offenbarungsvoraussetzungen in erster Linie beim jeweiligen Gericht (a. a. O., Rz. 27). Die Leistungsträger haben, sofern das Gerichtsverfahren mit der Erfüllung ihrer Aufgaben nach dem SGB zusammenhängt, die Erforderlichkeit der Offenbarung nur einer kursorischen „Schlüssigkeitsprüfung" zu unterziehen (Haase in GK-SGB X 2, § 69 Rz. 98). Welche Informationen im einzelnen für die gerichtliche Entscheidung relevant sein könnten, ist von den Leistungsträgern nicht zu beurteilen, denn die Bedeutung der einzelnen Fakten, Informationen und Vorgänge hängt von der rechtlichen Bewertung des Verfahrensstands ab, die dem Gericht vorbehalten ist. Angeforderte Akten sind daher, sofern ein gegenständlicher Bezug zu dem anhängigen Verfahren gegeben ist, grundsätzlich vollständig zu übersenden (Haase, a. a. O., Rz. 99).

§ 78 Abs. 1 SGB X statuiert eine Geheimhaltungspflicht des Gerichts als Empfänger der übermittelten Daten. Gerichtliche Entscheidungen, die Sozialdaten enthalten, dürfen durch Gerichte nur dann weiter übermittelt werden, wenn eine in § 35 SGB I genannte Stelle zur Übermittlung an den weiteren Empfänger befugt wäre.

11.2.7 Sozialhilfestatistik

Anfang 1994 gingen örtliche Sozialhilfeträger dazu über, neben dem üblichen Fragebogen zur Ermittlung der für die Leistungsgewährung maßgeblichen Umstände einen Ergänzungsfragebogen für Zwecke der Sozialhilfestatistik zu verwenden. Als Rechtsgrundlage wurde auf dem Fragebogen das Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms genannt, das Vorschriften über die Sozialhilfestatistik in das Bundessozialhilfegesetz (§§ 127 bis 134) einfügte.

Auskunftspflichtig zu dieser Sozialhilfestatistik sind nach § 131 BSHG die zuständigen Sozialhilfeträger und nicht die Antragsteller auf Sozialleistungen oder die Leistungsempfänger. Hieraus folgt, daß die Sozialhilfestatistik nur die Verwendung vorhandener Verwaltungsdaten erlaubt, m. a. W., es dürfen keine Daten erhoben werden, die nur für die Statistik und nicht primär für Entscheidungen über die Leistungsgewährung erforderlich sind.

Der erwähnte Ergänzungsfragebogen enthielt indessen Merkmale, die nur in Ausnahmefällen für die Leistungsgewährung von Belang sind, wie beispielsweise der „Schulabschluß" sowie „Berufsbildungsabschluß" und Angaben, die das Vorliegen einer besonderen sozialen Situation (Freiheitsentzug, Haftentlassung, Suchtabhängigkeit) beschreiben. Sofern diese Merkmale für die Leistungsgewährung keine Rolle spielen und deshalb nach den gesetzlichen Bestimmungen über die Mitwirkung der Leistungsberechtigten (§§ 60 ff. SGB I) nicht erhoben werden dürfen, können die Sozialleistungsträger ihrer durch § 131 BSHG begründeten Auskunftspflicht gegenüber den Statistikbehörden nicht nachkommen.

Das Ministerium für Arbeit, Soziales und Gesundheit vertrat die Auffassung, daß die Verwendung von Zusatzerhebungsbögen speziell für die Sozialhilfestatistik nicht zulässig sei, und sprach sich für die Schaffung normenklarer rechtlicher Grundlagen aus. Der LfD teilte seine Rechtsauffassung den fachlich zuständigen Stellen mit; der Gemeinde- und Städtebund machte die Stellungnahme des LfD durch Veröffentlichung in den GStB-Nachrichten bekannt.

11.2.8 Beratung und Unterstützung bei der Ausübung der Personensorge

Mütter und Väter, die allein für ein Kind oder einen Jugendlichen zu sorgen haben oder tatsächlich sorgen, können nach § 18 Abs. 1 SGB VIII Beratung und Unterstützung bei der Ausübung der Personensorge einschließlich der Geltendmachung von Unterhalts- oder Unterhaltsersatzansprüchen des Kindes oder Jugendlichen beanspruchen. Nach Bevollmächtigung können

die Jugendämter auch Unterhaltsansprüche geltend machen und die hierzu erforderlichen Auskünfte einholen. Der LfD hatte sich wiederholt mit Eingaben zu befassen, in denen beklagt wurde, daß die Ergebnisse derartiger Feststellungen durch Jugendämter an personensorgeberechtigte Mütter weitergegeben wurden.

Er vertrat die Auffassung, daß, sofern eine Auskunftspflicht nach § 1605 BGB besteht, die Jugendämter dem Grunde und dem Umfang nach Rechte in Anspruch nehmen, die den Kindern zustehen und die von den Personensorgeberechtigten als gesetzliche Vertreter in gleicher Weise hätten geltend gemacht werden können. Die Weitergabe der erlangten Informationen an die nach § 1605 BGB Berechtigten kann unter Datenschutzgesichtspunkten nicht beanstandet werden.

11.2.9 Datenübermittlung von Jugendämtern an Polizeibehörden

Ein Jugendamt bat um eine Stellungnahme des LfD zur Zulässigkeit der Übermittlung von Sozialdaten an eine Polizeibehörde. In dem der Anfrage zugrundeliegenden Fall sah sich das Jugendamt durch § 65 SGB VIII gehindert, das Geburtsdatum eines Jugendlichen weiterzugeben, weil dieses im Rahmen persönlicher und erzieherischer Hilfe bekanntgeworden war. Die Polizeibehörde behauptete, aus dem Melderegister sei das Geburtsdatum nicht zu entnehmen.

Der LfD wies in seiner Stellungnahme darauf hin, daß sich die Schutzwirkung des § 65 SGB VIII nicht auf alle dem Jugendamt im Rahmen der Aufgabenerfüllung bekanntgewordenen, sondern nur auf die einem Mitarbeiter anvertrauten Daten erstreckt. Die Verwendung des Begriffs „anvertraut" deutet darauf hin, daß dem Vertrauensverhältnis bei der Datenerhebung erhöhte Bedeutung zukommt (Hauck in Hauck/Haines, SGB VIII K § 65, Rz. 3). Durch die Vorschrift geschützt sind nur Daten, die im Rahmen besonders vertraulicher Beratungsgespräche anfallen und die ihrer Art nach besonders geheimhaltungsbedürftig sind.

Das Geburtsdatum unterliegt nicht dem besonderen Vertrauensschutz des § 65, auch wenn es im Zusammenhang mit der Gewährung persönlicher oder erzieherischer Hilfe bekanntgeworden ist.

Auch Geburtsdaten sind indessen Sozialdaten, die nur beim Vorliegen der Voraussetzungen der §§ 67 d bis 78 SGB X offenbart werden dürfen. Im konkreten Falle einschlägig ist § 68 SGB X, der u. a. die Übermittlung für Aufgaben der Polizeibehörden regelt.

Eine Übermittlung nach § 68 SGB X ist nur zulässig, soweit kein Grund zur Annahme besteht, daß dadurch schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Zwar ist auch das Geheimhaltungsinteresse des Betroffenen grundsätzlich schutzwürdig; überwiegend wird jedoch vertreten, das Geheimhaltungsinteresse des Betroffenen müsse „von der Rechtsordnung anerkannt sein", ein „zwingendes öffentliches Interesse" genieße Vorrang (Walz in GK SGB X 2, § 68 Rz. 70). Bei der Datenoffenbarung zu Strafverfolgungszwecken sei § 68 die Rolle eines Auffangtatbestandes einzuräumen (Bundesratsdrucksache 8/4022 zu § 70). Daraus ergebe sich, daß das Interesse des Betroffenen, sich einem Ermittlungsverfahren bzw. dem Zugriff der Strafverfolgungsbehörden zu entziehen, als solches nicht schutzwürdig sei (Walz a. a. O., Rz. 72, m. w. N.).

Die ersuchte Stelle ist freilich zur Übermittlung auch dann nicht verpflichtet, wenn sich die ersuchende Stelle die Angaben auf andere Weise beschaffen kann. Diese Formulierung stellt die Berufung auf die Nachrangigkeit der Offenbarung von Sozialdaten zwar in das Ermessen der ersuchten Stelle. Doch kann der Zweck dieser Übermittlungsbeschränkung, anfragende Stellen prinzipiell auf alternative Datenquellen zu verweisen, um den Schutz des Sozialgeheimnisses so effizient wie möglich auszugestalten, nur erreicht werden, wenn die Ablehnung der Datenoffenbarung im Fall einer anderweitigen Beschaffungsmöglichkeit grundsätzlich obligatorisch ist (Walz a. a. O., Rz. 82, m. w. N.). Da den Polizeibehörden in Rheinland-Pfalz auch der überregionale Zugriff auf Daten des Einwohnermelderegisters ermöglicht ist, begegnet die Einlassung, das Geburtsdatum sei nicht über EWOIS zu erlangen, erheblichen Zweifeln.

11.3 Datenschutz bei Adoptionen

11.3.1 Einladung zur Mütterberatung

Ein Caritasverband informierte den LfD über eine Verletzung des Adoptionsgeheimnisses in seinem Bereich: Eine Mutter hatte ihr Kind unmittelbar nach der Geburt zur Adoption freigegeben. Aufgrund der Meldung der Geburt nach § 99 der Dienstanweisung für die Standesbeamten wurde die Mutter von dem für ihren Wohnort zuständigen Gesundheitsamt zur Mütterberatung eingeladen. Die Einladung war adressiert: „An die Eltern des Kindes N. N.". Auf diese Weise erfuhren der Briefträger und die Vermieterin, der die Einladung übergeben wurde, von der Geburt – die nach dem Willen der Mutter geheimgehalten werden sollte – und von der Adoption.

Aus gegebener Veranlassung war bereits im Jahre 1987 zwischen dem Ministerium für Soziales und Familie, dem Ministerium des Innern und für Sport und der DSK ein Verfahren abgestimmt worden, das in Adoptionsfällen der beschriebenen Art eine Benachrichtigung der Meldebehörde des Wohnorts nach § 98 Abs. 1 Nr. 2 der Dienstanweisung für die Standesbeamten ausschließt (vgl. 11. Tb., Tz. 6.7). Statt dessen wird die Anmeldung des Neugeborenen durch die Adoptionspflegeeltern bei der für

ihren Wohnsitz zuständigen Meldebehörde vorgenommen. Diese für Geburtsmitteilungen an Meldebehörden getroffene Regelung für Fälle, in denen ein Kind unmittelbar nach der Geburt in Adoptionspflege gegeben wird, ist zwischenzeitlich in § 98 Abs. 1 Satz 2 der Dienstanweisung übernommen worden.

Der LfD empfahl dem Ministerium des Innern und für Sport, die Standesbeamten zu bitten, bei Mitteilungen an Gesundheitsämter im Vorgriff auf eine spätere Änderung des § 99 der Dienstanweisung ebenso zu verfahren. Das Ministerium hat dieser Empfehlung entsprochen.

11.3.2 Verwendung eines Motivationserfassungsbogens bei der Adoptionsvermittlung

Im 14. Tätigkeitsbericht äußerte sich der LfD ausführlich zur Absicht des Landesamtes für Jugend und Soziales, als Grundlage für die Erstellung von Eignungsberichten über potentielle Adoptions- und Pflegeeltern Daten zur Motivation unter Verwendung eines Fragebogens zu erfassen. Er erhob keine Bedenken dagegen, die für die Adoptionsvermittlung notwendigen Informationen, auch soweit sie sehr sensitiver Natur sind, in einem Gespräch mit den Adoptionsbewerbern zu erheben und die Folgerungen für die Antragsbearbeitung in einer Zusammenfassung aktenkundig zu machen, wandte sich aber gegen die routinemäßige Erfragung, Erfassung, Aufbewahrung (Speicherung) und sonstige Verarbeitung auch in solchen Fällen, in denen die Betroffenen ihre Zustimmung erklären.

Anfang 1994 wurde dem LfD die überarbeitete Endfassung des Motivationserfassungsbogens zugeleitet. In dieser Fassung waren einige wenige Fragen eliminiert; im übrigen war der Fragenteil aber inhaltlich unverändert. Eine Einwilligungserklärung für die Weitergabe von Akten an andere Adoptionsvermittlungsstellen war zwar vorgesehen, entsprach aber nicht den gesetzlichen Anforderungen. In einem Zuleitungsschreiben an die Jugendämter unterließ es das Landesamt freilich nicht, darauf hinzuweisen, daß der Fragebogen mit dem LfD abgestimmt sei.

Der LfD erklärte gegenüber dem Landesamt, daß er Fälle, in denen aufgrund der vorbezeichneten Einwilligungserklärung Akten und Arbeitshilfen weitergegeben werden, als Verstoß gegen die Vorschriften zum Schutze des Sozialgeheimnisses beanstanden werde. Im übrigen ist beabsichtigt, die Thematik im Rahmen örtlicher Feststellungen erneut aufzugreifen.

11.3.3 Überprüfung des Kindergeldanspruchs bei Adoptiveltern

Adoptionsdaten unterliegen einem besonderen Offenbarungs- und Ausforschungsverbot (§ 1758 BGB). Eingaben an den LfD machen immer wieder deutlich, daß die Eltern adoptierter Kinder besonders sensibel reagieren, wenn Tatsachen, die geeignet sind, die Adoption und ihre Umstände aufzudecken, erfragt werden.

Im Berichtszeitraum beklagten die Eltern eines adoptierten Kindes, daß in einer Erklärung aufgrund der Änderung des Bundeskindergeldgesetzes ab 1. Januar 1994 das Kindschaftsverhältnis in der Unterscheidung nach leiblichen Kindern und Adoptivkindern anzugeben war. Sie wiesen darauf hin, daß das Bundeskindergeldgesetz nur noch zwischen den Kindern des Berechtigten und ihnen gleichgestellten Kindern unterscheidet und zu den Kindern des Berechtigten auch die Adoptivkinder gehören.

Die im konkreten Falle zuständige Oberfinanzdirektion bestätigte, daß die Differenzierung in dem Vordruck auch aus ihrer Sicht entbehrlich war, wies zugleich aber darauf hin, daß der Erklärungsvordruck durch Erlaß des Bundesministeriums für Familie und Senioren und des Bundesministeriums des Innern vom 6. Januar 1994 eingeführt und bundesweit verwendet worden war.

Dem BfD, der den Vorgang ebenfalls aufgegriffen hatte, teilte das Bundesministerium für Familie und Senioren mit, daß es bei zukünftigen Angaben zum Kindschaftsverhältnis generell keine Unterscheidung zwischen leiblichen Kindern und Adoptivkindern mehr geben werde. Im übrigen erklärte es sein Einverständnis, daß, soweit ein Adoptivkindschaftsverhältnis bei Verwendung des Vordrucks erstmals offengelegt wurde, diese Informationen wieder gelöscht werden.

Die Oberfinanzdirektion wurde vom Ministerium der Finanzen angewiesen, dementsprechend zu verfahren. Auf nochmalige Rückfrage des LfD im März 1995 bestätigte das Ministerium, daß der aktuelle Datenbestand der Behörde keine Merkmale zur Unterscheidung zwischen leiblichen Kindern und Adoptivkindern mehr enthält.

11.4 Festsetzung von Elternbeiträgen zu den Kosten von Kindertagesstätten

Die Elternbeiträge für Kinderkrippen, Horte und altersübergreifende Gruppen sind nach den gesetzlichen Bestimmungen (Kindertagesstättengesetz) unter Berücksichtigung von Einkommen und Kinderzahl festzusetzen. Es ist also erforderlich, daß die Landkreise, Städte und Verbandsgemeinden als Träger solcher Einrichtungen von den Unterhaltspflichtigen Daten erfragen, die eine zutreffende Einstufung ermöglichen.

Eine Überprüfung durch den LfD ergab, daß einzelne Kindergartenträger weitaus mehr Daten erfragten, als zur Aufgabenerfüllung im Einzelfall erforderlich war. So sollten die Unterhaltspflichtigen beispielsweise angeben, wo sie krankenversichert sind, in welcher Zeit sie arbeitsunfähig erkrankt waren, welchen Einheitswert vorhandener Grundbesitz hat oder ob Vermögen innerhalb der letzten zehn Jahre verschenkt wurde. Kreditinstitute sollten von den Antragstellern ermächtigt werden, gegenüber den Behörden Auskünfte „insbesondere über den Kontostand und die Kontobewegungen" zu erteilen und eine Verbandsgemeinde wollte sich gar von der Verpflichtung befreien lassen, datenschutzrechtliche Bestimmungen beachten zu müssen.

Der LfD hat in Fällen, in denen Datenschutzbestimmungen verletzt wurden, Beanstandungen ausgesprochen. Das Ministerium für Kultur, Jugend, Familie und Frauen entsprach der Empfehlung des LfD, Richtlinien über die Vorgehensweise bei der Festsetzung von Elternbeiträgen zu erlassen. Ein Rundschreiben an die Jugendämter von Rheinland-Pfalz vom 1. Februar 1995 enthält folgende Hinweise:

a) Die in § 13 Abs. 3 Kindertagesstättengesetz vorgesehene Beitragsstaffelung sollte durch Satzung erfolgen.

b) Die im Einzelfall zu erhebenden Elternbeiträge sollten durch das zuständige Jugendamt festgesetzt und dem Träger der Einrichtung mitgeteilt werden.

c) Die Höhe des Einkommens ist nachzuweisen. Ein Einkommensnachweis ist entbehrlich, wenn nach den Angaben der Eltern der höchste in der Staffelung vorgesehene Elternbeitrag festzusetzen ist. Die Vorlage eines Einkommensnachweises kann von den Betroffenen abgelehnt werden mit der Folge, daß der höchste Elternbeitrag festgesetzt wird.

d) Ergänzende Angaben werden nur erhoben, wenn außergewöhnliche Belastungen geltend gemacht werden. Die Datenerhebung durch Vordrucke erfolgt unter strenger Beachtung des Erforderlichkeitsprinzips.

e) Bei der Vorlage von Einkommensnachweisen – Steuerbescheide, Verdienstbescheinigungen – bleibt es den Eltern bzw. Erziehungsberechtigten überlassen, für die Sachbearbeitung nicht relevante Daten unkenntlich zu machen (zu schwärzen).

f) Die Betroffenen werden durch die Herausgabe von Hinweisen über die Rechtsgrundlagen der Datenerhebung, die Staffelung der Elternbeiträge und die Modalitäten der Einkommensermittlung, insbesondere die in Buchst. c genannten Bedingungen, informiert.

11.5 Mitarbeiterinnen in Frauenhäusern haben Verschwiegenheitspflichten zu beachten

Frauen, die in Frauenhäusern Zuflucht suchen, befinden sich oft in einer persönlichen Gefährdungssituation. Dementsprechend besteht die Notwendigkeit, die Tatsache des Aufenthalts geheimzuhalten. Den Hilfesuchenden wird deshalb bei der Aufnahme Vertraulichkeit zugesichert. Unabhängig davon haben die Mitarbeiterinnen in Frauenhäusern als staatlich anerkannte Sozialarbeiterinnen oder Sozialpädagoginnen Verschwiegenheitspflichten zu beachten, deren Verletzung durch § 203 StGB strafbedroht ist.

Die Städte, in denen sich Frauenhäuser befinden, leisten den Trägerorganisationen institutionelle Förderung. Sie erwarten allerdings, daß die Umlandgemeinden, in denen Frauen vor ihrer Aufnahme in ein Frauenhaus gewohnt haben, ihre Aufwendungen ersetzen. In mehreren Fällen wurden die Trägerorganisationen deshalb aufgefordert, die Namen und Herkunftsgemeinden der Frauen mitzuteilen, die in Frauenhäusern wohnen.

Der LfD wies darauf hin, daß die Verschwiegenheitspflicht der in den Frauenhäusern Beschäftigten auch gegenüber den Trägern der Einrichtung besteht. Eine Bekanntgabe des Namens trotz der den Frauen zugesicherten Vertraulichkeit wäre unbefugt. Für unbedenklich hielt der LfD lediglich die Verwendung nichtpersonenbeziehbarer Daten für Abrechnungszwecke (Fallzahlen in der Gliederung nach Herkunftsgemeinden).

Für datenschutzrechtlich akzeptabel hielt der LfD die Lösung, die der Städtetag Rheinland-Pfalz gemeinsam mit dem Landkreistag gefunden und in der „Gemeinsamen Empfehlung über Hilfen an Frauen in Frauenhäusern einschließlich der institutionellen Förderung" bekanntgemacht hat. Danach wird eine Prüfung der institutionellen Förderung – bei der auch personenbezogene Daten von Bewohnerinnen der Frauenhäuser von dem Prüfer zur Kenntnis genommen werden können – nur durch das Rechnungsprüfungsamt der Stadt vorgenommen, die diese Förderung unmittelbar leistet. Die Herkunftsgemeinden erkennen die überprüfte Abrechnung von Kostenanteilen ohne die Übermittlung personenbezogener Daten an.

11.6 Archivierung von Akten einer Beratungsstelle für Kinder, Jugendliche und Erwachsene

Recht häufig wird der LfD um Beratung gebeten, wenn es zwischen Behörden um Kontroversen zu Datenschutzfragen kommt. Seltener sind Fälle, in denen sich Referate oder Abteilungen der gleichen Behörde streiten und den LfD als Sachverständigen anrufen. Auch in solchen Fällen kommt der LfD selbstverständlich den ihm durch § 24 Abs. 4 LDSG übertragenen Beratungsaufgaben nach; eine Pflicht zur Erstattung von Gutachten und Berichten besteht indessen nach § 24 Abs. 5 nur gegenüber dem Landtag, seinen Ausschüssen sowie der Landesregierung.

In einem konkreten Fall wurde die folgende Rechtsfrage zwischen dem Stadtarchiv und der Beratungsstelle für Kinder, Jugendliche und Erwachsene einer größeren Stadt kontrovers beurteilt: Das Stadtarchiv beanspruchte, gestützt auf die Anbietungspflicht des Landesarchivgesetzes (§ 7) die Herausgabe von Akten der Beratungsstelle. Diese war der Meinung, daß § 66 Abs. 1 SGB VIII i. V. m. § 84 SGB X einer solchen Herausgabe entgegensteht.

Der LfD vertrat folgende Auffassung:

Soweit die Daten dem allgemeinen Sozialgeheimnis unterfallen, ist gem. § 84 Abs. 6 i. V. m. § 71 Abs. 1 Satz 3 SGB X (i. d. F. vom 13. Juni 1994, BGBl. I, S. 1229) eine Offenbarung personenbezogener Daten zulässig, soweit sie erforderlich ist für die Erfüllung der gesetzlichen Pflichten zur Sicherung und Nutzung von Archivgut nach den §§ 2 und 5 des Bundesarchivgesetzes oder entsprechender gesetzlicher Vorschriften der Länder, die die Schutzfristen des Bundesarchivgesetzes nicht unterschreiten. Da die Schutzfristen des Landesarchivgesetzes Rheinland-Pfalz diejenigen des Bundesarchivgesetzes nicht unterschreiten, ist bezüglich dieser Daten eine Übermittlung nach dem Landesarchivgesetz nicht nur zulässig, es besteht die dort geregelte Anbietungspflicht.

Besonderes dürfte bezüglich derjenigen Daten gelten, die gem. § 65 Abs. 1 SGB VIII (Kinder- und Jugendhilfegesetz) dem Mitarbeiter eines Trägers der öffentlichen Jugendhilfe zum Zweck persönlicher und erzieherischer Hilfe anvertraut worden sind. Diese Formulierung erfaßt nur Daten, die im Rahmen besonders vertraulicher Beratungsgespräche anfallen und nicht auch Daten, die bei der Durchführung „anderer Aufgaben" der Kinder- und Jugendhilfe (etwa der Leistung finanzieller Zuwendungen) beschafft worden sind (so Hauck/Heines, Kommentar zum SGB VIII, Anm. 4 zu § 65).

Informationen über solche Beratungsgespräche werden im Regelfall wohl gar nicht aktenkundig gemacht. Wenn dies aber der Fall sein sollte, werden §§ 67 d bis 78 SGB X eingeschränkt. Eine Weitergabe solcher Unterlagen an das Archiv aufgrund des § 71 Abs. 1 Satz 3 SGB X dürfte also nicht zulässig sein.

11.7 Abrechnung der Kosten für die Schwangerenberatung

Die kommunalen Gebietskörperschaften in Rheinland-Pfalz leisten Zuschüsse für die institutionelle Förderung der Schwangerenberatung. Es versteht sich, daß sie hierzu nur insoweit bereit sind, als Frauen, die in ihrem Zuständigkeitsbereich wohnen, eine solche Beratung in Anspruch nehmen. Aus diesem Grunde übermitteln die Beratungsstellen die Fallzahlen in der Gliederung nach Jugendamtsbezirken an die Stadt- und Kreisverwaltungen.

Bei der Übermittlung dieser Fallzahlen soll es nach Meinung einer Kreisverwaltung gelegentlich zu Fehlern gekommen sein, weil die Beratungsstellen Wohngemeinden einem unzuständigen Jugendhilfeträger zuordneten mit der Folge, daß ein Jugendamt zuviel, ein anderes Jugendamt zuwenig zahlte. Die Kreisverwaltung verlangte deshalb, daß die Wohngemeinden der beratenen Frauen mitgeteilt werden.

Ein Träger von Schwangerenberatungsstellen hielt dies für bedenklich. Er vertrat die Auffassung, daß der Anonymitätsschutz der beratenen Frauen nach dem Schwangeren- und Familienhilfegesetz als Rechtsgut höher zu bewerten sei als die zweifelsfreie Klärung der Zuständigkeit kommunaler Zuschußgeber. Von diesen wurde eingewandt, die Anonymität sei nicht gefährdet, denn die Gruppe der möglichen Betroffenen sei selbst in kleinen Gemeinden so groß, daß eine Identifizierung mit Sicherheit ausgeschlossen werden könne.

Eine Auskunft des Statistischen Landesamtes, wie sie der LfD einholte, hätte die Zuschußgeber eines Besseren belehrt: in Rheinland-Pfalz existieren rund 130 Ortsgemeinden mit weniger als 100 Einwohnern. In einer dieser Gemeinden ist nur eine Frau der Altersgruppe von 15 bis 40 Jahren zugeordnet, eine Identifizierung wäre also problemlos möglich. In immerhin 17 Gemeinden leben höchstens fünf Frauen, die zu dieser Altersgruppe gehören. Beim Vorhandensein von Zusatzinformationen, die das soziale Umfeld betreffen, dürfte auch hier eine Identifizierung nicht allzu schwierig sein. Der Anonymitätsschutz von beratenen Frauen würde also durch die Angabe der Wohngemeinde erheblich reduziert. Schon aufgrund dieser Überlegung waren gegen die Angabe der Wohngemeinde datenschutzrechtliche Bedenken zu erheben. Die Angabe ist aber nach Auffassung des LfD auch nicht erforderlich, denn Zuordnungsfehler können zuverlässig vermieden werden, wenn den Beratungsstellen Listen zur Verfügung gestellt werden, aus denen die zu einem Jugendamtsbezirk gehörenden Wohngemeinden zu entnehmen sind.

11.8 Hilfe bei Schwangerschaftsabbrüchen

Ein Verband der freien Wohlfahrtspflege informierte den LfD über das ab Juni 1994 zu beachtende Kostenerstattungsverfahren der Schwangerschaftsabbrüche in den Fällen der §§ 37 und 37 a BSHG. Für die Leistungsabrechnung bei Schwangerschaftsabbrüchen, für die kein Leistungsanspruch gegenüber den gesetzlichen Krankenkassen besteht, wurde durch Rundschreiben des Ministeriums für Arbeit, Soziales, Familie und Gesundheit ein Antrags- und Abrechnungsverfahren eingeführt, das vier Stellen der öffentlichen Verwaltung beteiligte: die Krankenkasse, die Kassenärztliche Vereinigung, das Landesamt für Jugend und Soziales Rheinland-Pfalz und die örtlichen Sozialhilfeträger. Diese Stellen erhoben Daten über rechtswidrige straffreie

Schwangerschaftsabbrüche entweder unmittelbar oder es wurden ihnen derartige Daten übermittelt. Das Landesamt für Jugend und Soziales Rheinland-Pfalz hatte die Funktion einer zentralen Abrechnungsstelle. Da die Abrechnung personenbezogen erfolgte, entstand bei dieser Behörde eine besonders sensitive Datensammlung. Die Möglichkeit, sich zwecks Ausstellung eines Kostenübernahmescheins an die zuständige Krankenkasse zu wenden, wurde für die betroffenen Frauen deshalb geschaffen, weil ihnen der von vielen als diskriminierend empfundene Gang zum Sozialamt erspart werden sollte. Das Ministerium wies darauf hin, daß die Einbeziehung der Krankenkasse in das Antragsverfahren den Intentionen des Urteils des Bundesverfassungsgerichts entspreche, denn die gesetzlichen Krankenkassen seien in dieser Entscheidung ausdrücklich im Zusammenhang mit einer künftigen Verfahrensregelung zur Gewährung von Hilfen erwähnt. Die Übernahme von Aufgaben durch die Kassenärztlichen Vereinigungen sei durch § 75 Abs. 6 SGB V gedeckt. Nach dieser Vorschrift dürfen Kassenärztliche Vereinigungen mit Zustimmung der Aufsichtsbehörden weitere Aufgaben der ärztlichen Versorgung übernehmen. Die örtlichen Sozialhilfeträger seien an den Kosten beteiligt und ebenso wie das Landesamt als Leistungsträger anzusehen.

Der LfD hielt es unter Berücksichtigung der vom Ministerium genannten Zielsetzung – Vermeidung von Diskriminierung – unter Datenschutzgesichtspunkten für hinnehmbar, daß die Krankenkassen in das Antragsverfahren einbezogen werden. Er sprach sich aber mit aller Deutlichkeit dagegen aus, daß nur zu dem Zweck, die Abrechnung zu erleichtern, und zu Kontrollzwecken Daten an die Kassenärztliche Vereinigung und an das Landesamt für Jugend und Soziales übermittelt werden.

Das Ministerium folgte schließlich den Empfehlungen des LfD und änderte das Verfahren so, daß den Kassenärztlichen Vereinigungen und dem Landesamt nur noch anonyme Abrechnungsinformationen zugehen. Auch dieses Verfahren wird freilich nur von kurzer Dauer sein, denn ab 1996 werden die Leistungen nach § 3 des Gesetzes zur Hilfe für Frauen bei Schwangerschaftsabbrüchen in besonderen Fällen durch die gesetzliche Krankenkasse gewährt. Die Länder erstatten den gesetzlichen Krankenkassen die ihnen durch die Ausführung des Gesetzes entstehenden Kosten (§ 4). Der LfD wird sorgfältig darauf achten, daß die datenschutzrechtlichen Belange der betroffenen Frauen im Abrechnungsverfahren gewahrt bleiben. Er hofft, daß er vom zuständigen Ministerium rechtzeitig beteiligt wird.

11.9 Versorgungsverwaltung; Auskunftsansprüche eines Sozialleistungsempfängers gegen einen ärztlichen Gutachter

Die Wahrnehmung von Datenschutzrechten kann gelegentlich mit Ärger verbunden sein. Dies mußte auch ein Antragsteller auf Sozialleistungen erfahren, dem vom Leistungsträger – einem Versorgungsamt – aufgegeben worden war, sich zum Nachweis der Leistungsvoraussetzungen von einem Facharzt untersuchen zu lassen. Mit der Untersuchung war der Betroffene einverstanden, allerdings nur unter der Bedingung, daß ihm eine Kopie des Gutachtens ausgehändigt werde. Dies wiederum wurde von dem Arzt abgelehnt und so kam die Untersuchung nicht zustande.

Das Versorgungsamt und das Landesversorgungsamt, das schließlich ebenfalls mit der Sache befaßt wurde, vertraten die Auffassung, daß der Arzt, der kein Mitarbeiter des Versorgungsamtes ist, auch nicht darüber entscheiden könne, ob im Rahmen der Akteneinsicht nach § 25 SGB X eine Kopie des Gutachtens ausgehändigt werde. Die Gestattung der Akteneinsicht sei eine Verfahrenshandlung, zu deren Vornahme nach § 11 Abs. 1 SGB X nur die Behörde durch ihren Leiter, dessen Vertreter oder Beauftragten fähig sei.

Der LfD stimmte dem im Grundsatz zu, war aber der Meinung, daß die Information des Betroffenen, jedenfalls dann, wenn er dies wünscht, die Voraussetzung einer im Sinne des § 203 Abs. 1 StGB befugten Offenbarung ist. Es existiert nämlich keine gesetzliche Befugnis des Arztes zur Informationsweitergabe an die Versorgungsverwaltung; die Befugnis besteht also nur, wenn der Betroffene mit der Offenbarung von Untersuchungsdaten einverstanden ist. Verlangt er nähere Informationen über die Ergebnisse einer Untersuchung als Voraussetzung für seine Zustimmung, so kann der Arzt nicht darauf verweisen, daß diesem Verlangen durch den Empfänger des Gutachtens entsprochen werde. Der Arzt kann den Betroffenen durch Gewährung von Einsicht in das Gutachten oder mündlich unterrichten; er ist aber auch nicht gehindert, gewissermaßen außerhalb einer Rechtspflicht eine Kopie des Gutachtens zur Verfügung zu stellen.

12. Ausländerrecht

12.1 ASYLCARD u. a.

Im Oktober 1994 wurde der Zwischenbericht einer Bund-Länder-Arbeitsgruppe zur Harmonisierung des Asylverfahrens vorgelegt und auf Anfrage dem LfD von der Aufnahmeeinrichtung für Asylbegehrende Ingelheim – Außenstelle Worms – im Dezember zugeleitet.

Der Bericht weist zunächst auf eine Reihe von bundesweiten Mängeln im praktischen Ablauf des Verwaltungsverfahrens hin, insbesondere bei der Bereitstellung aktueller Daten an das Ausländerzentralregister (AZR), bei der Zuordnung einzelner Angaben zu bestimmten Asylbegehrenden sowie bei der Kommunikation der beteiligten Bundes- und Länderbehörden. Für die Behebung derartiger verwaltungstypischer Schwierigkeiten sind vorrangig die herkömmlichen organisatorischen und techni-

schen Möglichkeiten der Verwaltung zu nutzen, bevor über zusätzliche Eingriffe in das Recht auf informationelle Selbstbestimmung nachgedacht wird. Einem Großteil der bestehenden Schwierigkeiten könnte man bereits durch eine verbesserte Aktualität bei Bereitstellung und Abruf der im AZR gespeicherten Daten begegnen.

Im einzelnen wurde in diesem Bericht gefordert, daß zunächst innerhalb der Länder sog. „Datenführende Ausländerbehörden" zur Kommunikationsbündelung geschaffen werden. Abgesehen davon, daß von der funktionierenden Praxis her in Rheinland-Pfalz für eine derartige Einrichtung kein Bedarf besteht, und abgesehen von der Frage nach der Rechtsgrundlage, wäre es insbesondere unter Beachtung des Grundsatzes der Verhältnismäßigkeit unzulässig, vor dem Ausschöpfen bestehender Möglichkeiten einen weiteren zentralen Datenbestand zu schaffen, mit dem das Recht auf informationelle Selbstbestimmung der Betroffenen zusätzlich eingeschränkt wird.

Die Idee eines zumindest lesenden Zugriffs der beteiligten Stellen auf einen Teil der beim Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl.) geführten Daten – sog. „ASYLON-Fenster" –, die ebenfalls erheblichen Bedenken begegnet, scheint nach neuesten Erkenntnissen nur noch geringe Realisierungschancen zu haben.

Gegen die vorgeschlagene Verwendung des BAFl-Aktenzeichens als einheitliches Suchkriterium bestehen hingegen keine durchgreifenden Bedenken aus der Sicht des Datenschutzes.

Anders verhält es sich wiederum bei der auch öffentlich viel diskutierten ASYLCARD: Auf einer Chipkarte sollen danach Fingerabdruck und Lichtbild, Daten über das Asylverfahren, das Vorliegen einer Arbeitserlaubnis sowie über den Empfang von Sach- und Geldleistungen erfaßt werden. Auch hier ist stark zu bezweifeln, ob ein derart schwerwiegender Eingriff in Persönlichkeitsrechte, gemessen am Zweck der ASYLCARD, überhaupt verhältnismäßig sein kann. Die Einführung würde flächendeckende technische Infrastrukturen und erhebliche organisatorische Vorkehrungen erfordern, die ebenso für die beabsichtigte Manipulationsfestigkeit geboten wären, falls diese überhaupt erreichbar ist.

Schließlich bleibt zu bedenken: Je mehr Bereiche mit Kartenlösungen versehen werden, um so mehr wächst das Bedürfnis nach „praktischer und effizienter" Vereinheitlichung oder Zusammenführung. Hier entsteht die Gefahr der Rundumerfassung, die als Befürchtung schon am Anfang der Datenschutzdiskussion stand.

12.2 Ausländerzentralregistergesetz (AZRG)

Zu den Entwürfen des zwischenzeitlich in Kraft getretenen Ausländerzentralregistergesetzes hatte der LfD bereits in früheren Tätigkeitsberichten ausführlich Stellung genommen (s. 13. Tb. Tz. 12.1 und 14. Tb. Tz. 12.2). Auch in der Phase unmittelbar vor der Verabschiedung des Gesetzes hat der LfD die mit den anderen Landesbeauftragten für den Datenschutz abgestimmten Standpunkte gegenüber dem Ministerium des Innern und für Sport vertreten. Die von Anfang an erhobenen Bedenken gegen den automatisierten Zugriff der Nachrichtendienste gelten auch heute noch, auch wenn der entsprechende Datensatz reduziert wurde.

Für die Durchführungsverordnung des AZRG hatte der LfD Empfehlungen zum Inhalt der Datensätze, zur Bestimmtheit von Begründungstexten, zu den vorgesehenen Übermittlungssperren zu Gruppenauskünften an öffentliche Stellen sowie zur Stellung des Betroffenen bei Übermittlung seiner Daten an Behörden anderer Staaten und an zwischenstaatliche Stellen gegeben; sie konnten jedoch großteils bei der Endfassung nicht verwirklicht werden.

12.3 Auf Dauer keine Verwaltungsvorschrift zum Ausländergesetz?

Das Ausländergesetz sieht in § 104 vor: „Der Bundesminister des Innern erläßt mit Zustimmung des Bundesrates allgemeine Verwaltungsvorschriften zu diesem Gesetz ..." Dem Wortlaut nach ist dies nicht nur eine Ermächtigung, sondern ein gesetzliches Gebot. Schließlich werden die Vorschriften vor Ort benötigt.

Der LfD mahnte zum fünften Jahrestag des Inkrafttretens des Ausländergesetzes mit Unterstützung des Ministeriums des Innern und für Sport das Regelwerk beim Bundesministerium des Innern erneut an.

12.4 Übermittlung der Auslandsadresse durch die Ausländerbehörde

Ein Rechtsanwalt wollte eine höhere Gebührenforderung von einer Frau eintreiben, die sich im Bundesgebiet aufgehalten hatte, inzwischen aber wieder ausgereist ist; er wandte sich an die zuständige Ausländerbehörde, in deren Akten sich die Herkunftsadresse befindet, die vermutlich auch die gegenwärtige Anschrift ist.

Das Bundeszentralregistergesetz findet auf Übermittlungen vom und zum Register Anwendung, nicht aber – wie hier – auf Übermittlungen durch die Ausländerbehörde an nichtöffentliche Stellen. Das Ausländergesetz regelt den Fall nicht. Rechtsgrundlage bildet mithin § 16 Abs. 1 des LDSG, der die Übermittlung zuläßt, wenn der Empfänger ein rechtliches Interesse

glaubhaft macht und wenn zur Annahme entgegenstehender überwiegender schutzwürdiger Interessen des Betroffenen kein Anlaß besteht. Das rechtliche Interesse muß allerdings in geeigneter Weise glaubhaft gemacht werden. Im gegebenen Fall konnte nach Auffassung des LfD z. B. die Vorlage einer Gebührenrechnung zur Einsicht genügen oder das Erbringen vergleichbarer Nachweise.

Bei einer entsprechenden Anfrage zum Ausländerzentralregister müßte nach § 27 BZRG das rechtliche Interesse durch Vorlage eines nach deutschem Recht gültigen Vollstreckungstitels nachgewiesen werden. Diese Regelung mag sich aus der ungleich größeren Verwendbarkeit eines bundesweiten Personenregisters ergeben. Für die Übermittlung durch Landesbehörden, wie es Ausländerbehörden sind, erscheint die oben dargestellte Glaubhaftmachung angemessen und ausreichend.

Übrigens speichert das Bundeszentralregister nur den Wohnort im Herkunftsland, nicht die vollständige Anschrift.

12.5 Zwangsweise Vorführung Abzuschiebender beim Konsulat

Eines der Hauptprobleme bei der Abschiebung von Ausländern – insbesondere abgelehnter Asylbewerber – ist die Beschaffung der Heimreisedokumente, d. h. von Paßersatzpapieren. In über der Hälfte der Fälle wird dies nötig. Für Asylbewerber, die in einer Aufnahmeeinrichtung zu wohnen verpflichtet sind (in der Regel mit der Prognose „offensichtlich unbegründet"), bestimmt deshalb der im Jahre 1993 eingefügte § 43 b des Asylverfahrensgesetzes, daß die erforderlichen Maßnahmen zum frühestmöglichen Zeitpunkt zu treffen sind. Soweit hierbei nicht Bundesbehörden tätig werden, ist die Paßbeschaffung von der zuständigen Ausländerbehörde des Landes vorzunehmen.

Der Zeitpunkt, an dem mit der Paßersatzbeschaffung begonnen wird, bestimmt sich generell nach den Umständen des Einzelfalles, wobei allgemeine Erfahrungen sowie die übliche Dauer der Paßbeschaffung beim Herkunftsland eine Rolle spielen. Auf alle Fälle hat das Ministerium des Innern und für Sport die Ausländerbehörden angewiesen, die Heimatstaaten nicht über die Asylantragstellung zu informieren.

In der Berichtsperiode wurde bekannt, daß algerische Abschiebungsgefangene im Rahmen der Paßersatzbeschaffung auf Verlangen Algeriens zwangsweise den Konsulatsbeamten dieses Landes vorgeführt werden.

Hierzu ist übereinstimmend mit dem Ministerium des Innern und für Sport davon auszugehen, daß ohne die Zusammenarbeit mit den Heimatstaaten bei der Paßbeschaffung die gesetzlich vorgeschriebenen Abschiebungen praktisch nicht möglich sind.

Was den Zeitpunkt der Dokumentenbeschaffung angeht, so ist bei Asylbewerbern § 43 b AsylVerfG ohne Zweifel anzuwenden.

Soweit die Behörde vom Asylbewerber lediglich die Unterlagen ausfüllen läßt, ist die Eingriffstiefe äußerst gering und die Maßnahme insoweit durch die Mitwirkungspflicht des Asylbewerbers (§ 15 Abs. 2 Nr. 6 AsylVerfG) gedeckt. Dies gilt auch insoweit, als der Asylbewerber schon bei Antragstellung hierzu veranlaßt wird.

Es kann also letztlich nur um den Zeitpunkt der Übersendung der Unterlagen an die Auslandsvertretung des Asylbewerbers gehen. Hier läßt das gesetzliche Merkmal „frühestmöglicher Zeitpunkt" schon dem Wortsinne nach grundsätzlich keinen nennenswerten Interpretationsspielraum.

Bei alledem ist jedoch zu berücksichtigen, daß § 43 b AsylVerfG nur für solche Ausländer gilt, „die in einer Aufnahmeeinrichtung zu wohnen verpflichtet sind," also diejenigen, die nicht landesintern verteilt werden, sondern maximal drei Monate in der Aufnahmeeinrichtung verbleiben. In der Regel wird es sich um Fälle mit der Prognose „offensichtlich unbegründet" handeln.

Soweit die Beschaffung von Paßersatzpapieren die Übermittlung personenbezogener Daten an ausländische Konsularbehörden erfordert, findet sich im Ausländergesetz keine ausdrückliche spezielle Übermittlungsregelung. § 41 AuslG erlaubt jedoch, bei Identitätszweifeln die „erforderlichen Maßnahmen zu treffen", wenn es „zur Durchführung von Maßnahmen nach diesem Gesetz erforderlich" ist. Die Abschiebung wäre eine solche Maßnahme.

Als Übermittlungsgrundlage kommt § 17 Abs. 1 LDSG in Betracht. Danach ist die Übermittlung „nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen zulässig". Die genannten einschlägigen Bestimmungen des Asylverfahrensgesetzes und des Ausländergesetzes setzen die hier zur Paßbeschaffung erforderlichen Übermittlungen zwingend voraus. An inländische öffentliche Stellen läßt § 14 Abs. 1 Nr. 2 i. V. m. § 12 Abs. 4 Nr. 1 LDSG die Übermittlung zu, wenn sie zur rechtmäßigen Aufgabenerfüllung der übermittelnden Stelle erforderlich ist und eine Rechtsvorschrift dies zwingend voraussetzt. Danach kann davon ausgegangen werden, daß die Übermittlung nach Maßgabe des Ausländer- und des Asylverfahrensgesetzes erfolgt und damit zulässig ist.

Bei der Vorführung selbst werden seitens der durchführenden Behörden keine personenbezogenen Daten der Betroffenen erhoben oder gespeichert. Aus der Sicht des Datenschutzes ist dieser Vorgang somit nicht zu beurteilen. Hierbei dürften jedenfalls die gesetzlichen Mitwirkungspflichten der Betroffenen zur Anwendung gelangen.

Insgesamt hat der LfD jedoch zu diesem Komplex einige Empfehlungen gegeben:

- Die Behörden dürfen nur in den Fällen Heimreisedokumente unter Beteiligung der Heimatstaaten sofort beschaffen, in denen ein Asylantrag offensichtlich unbegründet ist.
- Die algerischen Konsulatsbehörden sind eindringlich auf die Verwendungsbeschränkungen des § 17 Abs. 4 LDSG hinzuweisen.
- Wie bereits vom Ministerium des Innern und für Sport angeordnet, ist besonders darauf zu achten, daß nur die für die Paßbeschaffung erforderlichen Daten übermittelt werden und keinerlei Hinweise auf die Asylantragstellung erfolgen.
- Die Betroffenen sind vor der Vorführung darauf hinzuweisen, daß sie keinerlei Angaben machen müssen, die zur Paßbeschaffung nicht erforderlich sind.
- Die algerische Konsularbehörde ist darauf hinzuweisen, daß sie darüber hinausgehende Fragen dementsprechend nicht stellen darf.
- Nach Möglichkeit sollte die die Vorführung veranlassende Behörde zur Überwachung einen Dolmetscher mitnehmen.

12.6 Ausländerbeiratswahlen

Nach § 46 a der Gemeindeordnung ist in Gemeinden, in denen mehr als 1 000 ausländische Einwohner ihre Hauptwohnung haben, ein Ausländerbeirat einzurichten, der die Interessen der ausländischen Einwohner gegenüber den gemeindlichen Organen und gegenüber allen Bürgern und Einwohnern der Gemeinde vertritt. Der LfD hatte wiederholt zu datenschutzrechtlichen Fragen Stellung zu nehmen, die mit der Vorbereitung und Durchführung der Ausländerbeiratswahlen zusammenhängen.

Zu klären war die Frage, ob es zulässig ist, Einwohnerdaten, die im Melderegister gespeichert sind, an einzelne Wählergruppen und Träger von Wahlvorschlägen sowie an die in der Ausländerarbeit tätigen anerkannten Organisationen für Zwecke der Wahlvorbereitung oder Wahlwerbung zu übermitteln. Es handelt sich hierbei um eine Datenübermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs, so daß § 34 Meldegesetz (MG) heranzuziehen ist. Absatz 3 dieser Vorschrift läßt die Erteilung einer Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Einwohner (Gruppenauskunft) zu, soweit sie im öffentlichen Interesse liegt. Durch die Übermittlung von Meldedaten für den genannten Zweck wird die Teilnahme an den Ausländerbeiratswahlen in erheblichem Maße gefördert, so daß vom Vorliegen dieser Übermittlungsvoraussetzung ausgegangen werden kann. Der LfD erhob also gegen die Erteilung einer Gruppenauskunft keine grundsätzlichen Bedenken.

Das Ministerium des Innern und für Sport stellte nach Abstimmung mit dem LfD in einem Rundschreiben vom 10. Oktober 1994 ergänzend fest, daß die Erteilung einer Gruppenauskunft auf ausländische Staatsangehörige beschränkt ist, die in den Gemeinden bzw. Landkreisen, in denen Ausländerbeiratswahlen durchgeführt werden, mit Hauptwohnung gemeldet sind. Sie darf nicht erteilt werden, wenn nach sorgfältiger Prüfung berechtigte Zweifel an der Seriosität oder der Zielsetzung einzelner Wählergruppen bestehen.

Ferner wies das Ministerium darauf hin, daß die Gruppenauskunft lediglich die Daten einer einfachen Melderegisterauskunft (§ 34 Abs. 1 Satz 1 MG) über Wahlberechtigte, für deren Zusammensetzung nur das Lebensalter der Betroffenen bestimmend ist, enthalten darf. Dementsprechend dürfen nur der Vor- und Familienname, akademische Grade und die Anschrift der Hauptwohnung des Wahlberechtigten mitgeteilt werden. Das Merkmal Staatsangehörigkeit darf weder übermittelt noch als Auswahlkriterium herangezogen werden. Unzulässig ist auch die Übermittlung der Geburtstage von Wahlberechtigten.

Außerdem hielt es das Ministerium für erforderlich, die Datenempfänger schriftlich darauf hinzuweisen, daß die übermittelten Daten nur zum Zwecke der Wahlwerbung im Zusammenhang mit Ausländerbeiratswahlen verwendet werden dürfen und spätestens einen Monat nach der Durchführung der Ausländerbeiratswahl zu löschen sind.

§ 35 Abs. 1 MG, der die Übermittlung von Meldedaten an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen im Zusammenhang mit Parlaments- und Kommunalwahlen regelt, kommt nach Auffassung des LfD als Rechtsgrundlage einer Weitergabe von Meldedaten für die vorgenannten Zwecke nicht in Betracht.

Wenige Tage vor der Ausländerbeiratswahl hatte sich der LfD mit einer Frage zu befassen, die das Wählerverzeichnis betraf. In Übernahme einer von der Arbeitsgemeinschaft der Kommunalen Spitzenverbände Rheinland-Pfalz ausgearbeiteten Mustersatzung (§ 9) hatten Städte und Gemeinden festgelegt, daß in das Wählerverzeichnis „alle wahlberechtigten Ausländerinnen und Ausländer, wozu auch Staatenlose gehören, mit Vor- und Familienname, Geburtstag, Anschrift und Nationalität eingetragen" werden und daß das Wählerverzeichnis an Werktagen vom 20. bis zum 16. Tag vor der Wahl öffentlich auszulegen ist. Der LfD verwies auf mögliche Gefährdungen von Ausländern durch eine gezielte Auswertung des Wählerverzeichnisses und vertrat die Auffassung, daß die Einbeziehung der Nationalität in den Datenkatalog zur Aufgabenerfüllung nicht erforderlich und daher

nicht zulässig ist. In Übernahme entsprechender Bestimmungen der Landeswahlordnung und der Kommunalwahlordnung empfahl er, ferner zuzulassen, daß auf Verlangen des Stimmberechtigten im Wählerverzeichnis während der Auslegungsfrist der Tag der Geburt unkenntlich gemacht wird.

13. Finanzverwaltung

13.1 Datenschutzrechtliche Ergänzung der Abgabenordnung

Die bereits im 14. Tätigkeitsbericht unter Tz. 13.1 näher erläuterte Sachlage in bezug auf die datenschutzrechtliche Ergänzung der Abgabenordnung ist nach wie vor unverändert. Das Bundesministerium der Finanzen hat sich nicht bewegt: Es stellt grundsätzlich die Erforderlichkeit solcher Ergänzungen in Frage.

Der LfD hält demgegenüber an seiner bereits vor zwei Jahren dargestellten Auffassung (die im wesentlichen von allen Datenschutzbeauftragten des Bundes und der Länder geteilt wird) fest.

13.2 Die Steuerdaten-Abrufverordnung: erforderlich, aber inhaltlich umstritten

Auch die Steuerdaten-Abrufverordnung (StDAV) kommt nicht voran. Ihre grundsätzliche Bedeutung wurde bereits im 11. Tätigkeitsbericht (Tz. 15.2.4) dargestellt. Immer wieder werden von verschiedenen Seiten Einwände erhoben. Nachdem die Frage der Befugnisse der Rechnungshöfe weitgehend einvernehmlich geklärt wurde, haben die Gemeinden Bedenken erhoben, ob sie durch die Verordnung nicht zu aufwendige Maßnahmen des technischen Datenschutzes treiben müßten. Nach Auffassung des LfD ist den berechtigten Anliegen der Gemeinden Rechnung zu tragen. Allerdings erfordert die Umsetzung der hier diskutierten Verordnung nach seiner Auffassung keinesfalls größere Aufwendungen, als sie ohnehin nach dem LDSG zu realisieren sind (§ 9 Abs. 2 LDSG). Der LfD appelliert eindringlich an das Ministerium, die Verabschiedung der VO, soweit es diesem möglich ist, zu fördern (vgl. hierzu auch 14. Tb., Tz. 18.6).

13.3 Dürfen die Ortsbürgermeister Listen mit Daten von Gewerbesteuerzahlern und Hundesteuerpflichtigen erhalten?

Eine Verbandsgemeinde hat sich mit folgenden Fragen an den LfD gewandt:

a) Ist es zulässig, daß die Verbandsgemeinde den Ortsbürgermeistern jeweils Übersichten über die Gewerbesteuerzahler in deren Ortsgemeinde zur Verfügung stellt?

b) Ist es zulässig, den Ortsbürgermeistern jeweils Listen der Hundesteuerzahler ihrer Ortsgemeinde zu übermitteln, damit die Ortsbürgermeister aufgrund ihrer örtliche Kenntnisse feststellen, wer Eigentümer bzw. Besitzer eines Hundes ist, damit seitens der Verbandsgemeindeverwaltung die notwendige Steuerveranlagung vorgenommen werden kann?

c) Inwieweit dürfen grundsätzlich Daten über Abgabenschuldner den Ortsbürgermeistern offenbart werden?

Der LfD hat diese Fragen wie folgt beantwortet:

a) Die Ortsgemeinde ist grundsätzlich Steuergläubigerin der Gewerbesteuern. Allerdings wird das Besteuerungsverfahren – soweit nicht die Finanzämter tätig werden – durch die Verbandsgemeinden durchgeführt. Auch bezüglich der Datenweitergaben von der Steuerverwaltung an den Steuergläubiger ist § 30 Abgabenordnung zu beachten. Danach dürfen nur diejenigen Personen bzw. Amtsträger Informationen aus einem Steuerverfahren erhalten, die selbst mit dem Steuerverfahren befaßt sind, sie dürfen nur insoweit Informationen erhalten, als dies der Durchführung des Besteuerungsverfahrens „dient" (§ 30 Abs. 4 Satz 1 Nr. 1 Abgabenordnung).

   Die Information des Ortsbürgermeisters über die konkrete Steuerlast des einzelnen Gewerbetreibenden dürfte der Durchführung des Besteuerungsverfahrens nicht in diesem Sinn „dienen". Entsprechenden Datenübermittlungen steht insofern § 30 Abgabenordnung entgegen.

   Der Gesichtspunkt, daß damit die Ortsgemeinde als Steuergläubigerin keine Kenntnis von den einzelnen gezahlten Steuerbeträgen erhält, hat demgegenüber zurückzutreten: Der Schutz des Steuergeheimnisses ist vorrangig.

b) Im Zusammenhang mit der Übermittlung von Listen von Hundesteuerzahlern an die Ortsbürgermeister kommt zu dem Gesichtspunkt, daß die Ortsgemeinden Steuergläubiger sind, hinzu, daß die Ortsbürgermeister insofern auch als Teil der steuererhebenden Verwaltung angesehen werden könnten. Wenn auch die Verwaltung der Steuern und Abgaben grundsätzlich der Verbandsgemeinde übertragen ist, so ist es nicht ausgeschlossen, daß die Ortsbürgermeister persönlich gewisse Aufgaben im Rahmen der Verwaltung selbst übernehmen. Vor diesem Hintergrund hat der LfD gegen die Übermittlung von Listen der Hundesteuerzahler an die Ortsbürgermeister keine durchgreifenden datenschutzrechtlichen Bedenken erhoben.

c) Entsprechende Überlegungen wären auch bei Informationen über andere gemeindliche Abgaben, für die § 30 Abgabenordnung ebenfalls maßgeblich ist, anzustellen.

13.4 Was darf das Finanzamt den Sozialämtern mitteilen?

Ein Beschwerdeführer hat vorgetragen, das Finanzamt habe rechtswidrig unter Verstoß gegen das Steuergeheimnis Angaben über sein Haus und seine Anwesenheitszeiten in diesem Haus an das Amt für Sozialwesen weitergegeben.

Als Rechtsgrundlage für diese Übermittlung kam ausschließlich § 21 Abs. 4 SGB X in Betracht. Danach haben die Finanzbehörden, soweit es in einem Sozialleistungsverfahren erforderlich ist, Auskunft über die ihnen bekannten Einkommens- oder Vermögensverhältnisse des Antragstellers oder der zum Haushalt rechnenden Familienmitglieder zu erteilen.

Diese Vorschrift ist nach ihrem Sinn und Zweck so auszulegen, daß auch die Angaben zu übermitteln sind, die die Beurteilung ermöglichen, ob ein bestimmtes Familienmitglied zum Haushalt des Antragstellers auf eine Sozialleistung rechnet.

Antragsteller auf Leistung nach dem Bundessozialhilfegesetz war der Bruder des Beschwerdeführers. Vor diesem Hintergrund waren die Angaben des Finanzamts zulässig, die die Beurteilung ermöglichten, ob der Beschwerdeführer zum Haushalt seines Bruders rechnete.

Die vom Finanzamt an das Sozialamt mitgeteilten Angaben entsprachen dieser Voraussetzung. Die Angaben über die Nutzungshäufigkeit des Gebäudes (drei- bis viermal im Jahr, verlassener Eindruck) waren dazu geeignet, die Frage zu beantworten, wo der Beschwerdeführer seinen Hauptwohnsitz hatte und dementsprechend dort Mitglied des Haushalts seines Bruders sein konnte.

Vor diesem Hintergrund bestand aus datenschutzrechtlicher Sicht kein Anlaß, die Auskunftserteilung durch das Finanzamt zu beanstanden.

13.5 Weitergabe von Steuerdaten durch das Finanzamt an die IHK zur Berechnung der Kammerbeiträge

In einer größeren Zahl von Eingaben wurde gefragt, ob die Datenerhebung der Industrie- und Handelskammern zum Zweck der Beitragserhebung zulässig ist. Insbesondere die Übermittlung von Steuerdaten durch das Finanzamt ist auf Bedenken der Betroffenen gestoßen.

Der LfD hat dies wie folgt beurteilt:

Die Industrie- und Handelskammern berechnen die Beiträge entsprechend ihrer Beitragsordnung. Maßgebliche Berechnungsgrundlage ist der Gewinn aus Gewerbebetrieb oder der Gewerbeertrag. Diese Regelung ist wirksam und verstößt nicht gegen höherrangiges Recht.

Es war zu fragen, ob die Industrie- und Handelskammern die maßgeblichen Informationen ohne vorherige Befragung der Beitragspflichtigen selbst unmittelbar beim Finanzamt erheben dürfen.

Nach dem LDSG ist die Datenerhebung bei Dritten dann zulässig, wenn eine Rechtsvorschrift dies vorsieht (§ 12 Abs. 4 Satz 1 Nr. 1 LDSG). Eine solche Rechtsvorschrift findet sich in § 9 Abs. 2 IHK-Gesetz.

Die Finanzverwaltung ihrerseits ist gem. § 31 AO zur Übermittlung an die IHK befugt. Diese Vorschrift geht den allgemeinen Übermittlungsregelungen des LDSG vor.

Ein Verstoß gegen das Steuergeheimnis oder gegen sonstiges Datenschutzrecht war also bei dem dargestellten Verfahren nicht festzustellen.

Es hat sich herausgestellt, daß auf den Beitragsbemessungsbescheiden der IHK zwar einige Rechtsgrundlagen angegeben waren, jene im Hinblick auf die Erhebung der sensiblen Steuerdaten indes nicht berücksichtigt wurden.

Aus der Sicht des LfD wäre es sinnvoll, bei der textlichen Gestaltung des Beitragsbescheids auf die Erhebungs- und Übermittlungsmöglichkeiten hinzuweisen, beispielsweise durch den Abdruck der einschlägigen Vorschriften. Er hat daher das Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau gebeten, die Industrie- und Handelskammern entsprechend zu informieren.

14. Wirtschaft und Verkehr

14.1 Überlassung von Zweitschriften der Gaststättenkonzessionen an die GEMA

Ein kommunaler Spitzenverband hat die Frage an den LfD herangetragen, ob hinsichtlich des Wunsches der GEMA, ihr von jeder neu zu erteilenden Gaststättenkonzession eine Kopie zu überlassen, aus der Sicht des Datenschutzes Bedenken bestehen.

Die Beantwortung der Frage erfolgte im Januar 1994, also zu einem Zeitpunkt, als das neue LDSG noch nicht in Kraft war. Mithin hatte die datenschutzrechtliche Beurteilung auf der Grundlage der Regelungen in § 7 LDatG zu erfolgen. Es wurde zwischen automatisierten und nichtautomatisierten Verfahren unterschieden. Nach Absatz 1 durften personenbezogene Daten, die in automatisierten Verfahren verarbeitet wurden, an Personen oder an andere Stellen außerhalb des öffentlichen Bereichs übermittelt werden, wenn und soweit dies gesetzlich zugelassen war oder wenn der Betroffene mit der Übermittlung einverstanden war. Personenbezogene Daten, die nicht in automatisierten Verfahren verarbeitet wurden, durften gemäß Absatz 2 an Personen oder andere Stellen außerhalb des öffentlichen Bereichs übermittelt werden, wenn dies zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich war oder soweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft machte und schutzwürdige Belange des Betroffenen nicht beeinträchtigt wurden. Im Falle eines automatisierten Verfahrens galt im Rahmen des § 7 Abs. 1 LDatG folgendes: Für das Anliegen der GEMA, von jeder neu zu erteilenden Gaststättenkonzession eine Kopie zu erhalten, ist im Gaststättengesetz eine besondere Rechtsgrundlage nicht vorhanden. Eine Datenübermittlung nach § 7 Abs. 1 LDatG war mithin ausgeschlossen, es sei denn, der Betroffene war mit der Übermittlung einverstanden. Aber auch die Regelung in § 7 Abs. 2 LDatG war im Ergebnis nicht geeignet, regelmäßig Zweitschriften an die GEMA zu übermitteln.

Zu demselben Ergebnis gelangt man auf der Grundlage des neuen LDSG. Gemäß der in § 16 Abs. 1 Nr. 1 getroffenen Regelung ist die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist. Nach Nummer 2 dürfen personenbezogene Daten an nichtöffentliche Stellen durch Behörden weitergegeben werden, wenn eine Rechtsvorschrift dies vorsieht, die Betroffenen eingewilligt haben oder dies zur Abwehr erheblicher Nachteile für die Allgemeinheit oder die Rechte der einzelnen erforderlich ist. Eine Übermittlung personenbezogener Daten an Private ist nach Nummer 3 dann zulässig, wenn ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht wird und überwiegende schutzwürdige Interessen der Betroffenen nicht entgegenstehen. Die Übermittlung personenbezogener Daten an nichtöffentliche Stellen kann im Einzelfall nach Nummer 4 zulässig sein, wenn dies im öffentlichen Interesse liegt oder der Empfänger ein berechtigtes Interesse an den Daten geltend macht und die Betroffenen nach Unterrichtung über die beabsichtigte Übermittlung nicht widersprochen haben.

Zwar ist bezüglich der Datenanforderungen wohl davon auszugehen, daß die GEMA grundsätzlich ein rechtliches Interesse an der Kenntnis der von ihr angeforderten Informationen besitzt. Denn nach den Bestimmungen des Urheberrechtswahrnehmungsgesetzes (UrhWahrnG) ist die GEMA als Verwertungsgesellschaft verpflichtet, die zu ihrem Tätigkeitsbereich gehörenden Rechte und Ansprüche wahrzunehmen (vgl. insbesondere §§ 6 und 13 b Abs. 1 UrhWahrnG). Zu den berechtigten Interessen rechnet jedes von der Rechtsordnung als schutzwürdig anerkannte oder ideelle Interesse oder Vermögenswerteinteresse des Empfängers der Daten. Dazu gehören auch wirtschaftliche Interessen. Fernerhin ist bei der Prüfung der schutzwürdigen Interessen der Betroffenen im Rahmen des § 16 Abs. 3 zu berücksichtigen, daß die Vereitelung von Ansprüchen der GEMA im Hinblick auf die Vorschriften des UrhWahrnG grundsätzlich nicht als schutzwürdig angesehen werden kann.

Allerdings kann damit die generelle Übermittlung einer jeden neu zu erteilenden Gaststättenkonzession unter dem Gesichtspunkt des informationellen Selbstbestimmungsrechts der Betroffenen nicht gerechtfertigt werden. Es sind nämlich häufig Sachverhalte vorhanden, die einer Wahrnehmung der urheberrechtlichen Nutzungsrechte an geschützten Werken der Musik nicht zugänglich sind. So fallen unter die Erlaubnisvorschriften des Gaststättengesetzes beispielsweise auch jeder Imbißstand oder der als selbständiger Gewerbetreibender im Reisegewerbe tätige mobile Getränkeverkäufer.

Nach allem könnte aus der Sicht des Datenschutzes die Übermittlung lediglich in denjenigen Fällen erfolgen, die eindeutig in den Bereich der von der GEMA treuhänderisch wahrgenommenen Nutzungsrechte an geschützten Werken der Musik fallen. In diesem Zusammenhang ist indes darauf zu achten, daß nur die erforderlichen personenbezogenen Daten übermittelt werden; denn nicht jede Angabe über die persönlichen und sachlichen Verhältnisse des Erlaubnispflichtigen (z. B. Geburtsdatum und -ort, Familienstand usw.) besitzt Relevanz für die Aufgabenstellung einer Wahrnehmungsgesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte.

Schließlich war darauf hinzuweisen, daß § 16 LDSG für die GEMA auch in den oben angesprochenen bedenkenfreien Fällen natürlich keinen Anspruch auf die Übermittlung personenbezogener Daten begründet.

14.2 Auskunftserteilung an Private aus dem Gewerberegister

Auch in diesem Berichtszeitraum war das Thema aktuell. Die Frage, ob und in welchem Umfang Privatpersonen von Stellen Auskünfte aus dem Gewerberegister erhalten dürfen, hat bereits die DSK viele Jahre beschäftigt. So wurde das Thema schon im 9. Tätigkeitsbericht im Jahre 1983 (Tz. 13.2) angesprochen, im 10. Tätigkeitsbericht 1985 ausführlich dargestellt (Tz. 8.1.2), im 11. Tätigkeitsbericht 1987 erneut aufgegriffen (Tz. 11.7), im 12. Tätigkeitsbericht 1989 aufgrund der inzwischen weitgehend erfolgten Automatisierung der Gewerberegister erneut behandelt (Tz. 11.3.1) und schließlich im 13. Tätigkeitsbericht 1991 wiederum erörtert (Tz. 14.2).

Für die Auskunft aus Gewerbedateien hat bis zur Novellierung der Gewerbeordnung keine besondere Rechtsgrundlage existiert. Zur praktischen Lösung der Schwierigkeiten war die DSK bereits damit einverstanden, daß die Behörden, die die Gewerbekarteien führen, in allgemeiner Form die betroffenen Gewerbetreibenden auf die Möglichkeit hinweisen, gegen die Auskunftserteilung an Private generell Widerspruch einzulegen. Bezüglich aller Gewerbetreibenden, die keinen Widerspruch eingelegt hatten, konnte dann davon ausgegangen werden, daß diese mit Auskunftserteilungen einverstanden waren. Bei der Neueintragung von Gewerbetreibenden war auf die Möglichkeit hinzuweisen, der Auskunftserteilung an Private zu widersprechen.

Inzwischen wurde das Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften vom 23. November 1994 verkündet. Darin werden die Datenübermittlungen aus den Gewerbeanzeigen geregelt, die jeder Gewerbetreibende nach § 14 Gewerbeordnung zu erstatten hat. Allerdings tritt der geänderte § 14 Gewerbeordnung erst am 1. Dezember 1995 in Kraft. Danach ist vorgesehen, daß die Übermittlung von Name, betrieblicher Anschrift und angezeigter Tätigkeit aus der Gewerbeanzeige an nichtöffentliche Stellen und an öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, nur dann zulässig ist, wenn der Auskunftsbegehrende ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht. Dazu gehören auch wirtschaftliche Interessen. Die Übermittlung weiterer Daten aus der Gewerbeanzeige ist nur zulässig, wenn der Auskunftsbegehrende ein rechtliches Interesse, insbesondere zur Geltendmachung von Rechtsansprüchen, an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Gewerbetreibenden überwiegt. Zu beachten ist in diesem Zusammenhang, daß hier nur geregelt wird, welche Auskünfte aus den Gewerbeanzeigen erteilt werden können. So ist kein Rechtsanspruch Dritter auf Mitteilung von Angaben aus den Gewerbeanzeigen vorgesehen.

14.3 Bereichsspezifische Übermittlungsregelung im Schornsteinfegergesetz

Im 14. Tätigkeitsbericht (Tz 14.4) hat der LfD darauf hingewiesen, daß bereichsspezifische Regelungen für die Übermittlung von Daten aus Kaminfegerdateien (Kehrbücher) an Dritte, die nicht zu Prüfzwecken erfolgten, fehlten.

Nunmehr hat der Bundesgesetzgeber durch das Gesetz zur Änderung des Schornsteinfegergesetzes vom 20. Juli 1994 bereichsspezifische Datenschutzregelungen in das Schornsteinfegergesetz aufgenommen. Neben Regelungen zum Umfang der Daten, die ein Schornsteinfegermeister zu einer Feuerungsanlage aufzuzeichnen und in das Kehrbuch einzutragen hat, handelt es sich um den oben erwähnten Bereich der Übermittlung von Daten aus den Kehrbüchern an Dritte. So dürfen nach § 19 Abs. 4 Schornsteinfegergesetz an nichtöffentliche Stellen personenbezogene Daten nur übermittelt werden, soweit der Empfänger ein rechtliches Interesse an der Kenntnis der Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat. Nicht ausreichend ist also ein lediglich berechtigtes Interesse des Empfängers. Mithin ist es nach der Gesetzeslage nicht möglich, daß aufgrund eines (berechtigten) wirtschaftlichen Interesses z. B. Daten aus den Kehrbüchern bezüglich privater Kleinfeuerungsanlagen für Werbezwecke an die Heizungsbranche übermittelt werden.

14.4 Datenübermittlungen im Rahmen der Fremdenverkehrswerbung

Eine Verbandsgemeinde hat angefragt, ob eine Datenübermittlung an private Beherbergungsbetriebe aus der bei ihr geführten Adreßdatei über Personen, die aufgrund einer Werbeaktion in der Presse an Informationsmaterial über die Gemeinde Interesse gezeigt haben, zulässig sei.

Der LfD hat zunächst grundsätzlich darauf hingewiesen, daß § 5 LDSG den vom Bundesverfassungsgericht in seiner Rechtsprechung zum Recht auf informationelle Selbstbestimmung entwickelten Grundsatz enthält, wonach der Betroffene grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen soll. In Absatz 1 Nr. 1 ist dementsprechend geregelt, daß die Verarbeitung personenbezogener Daten dann zulässig ist, wenn die Betroffenen in diese Verarbeitung eingewilligt haben. Weiterhin ist die Verarbeitung nach Absatz 1 Nr. 2 auch ohne Einwilligung möglich, wenn die Verarbeitung personenbezogener Daten aufgrund einer Regelung des LDSG oder einer sonstigen Rechtsvorschrift erlaubt ist.

Weiterhin war klarstellend zu bemerken, daß bei der EDV-mäßigen Nutzung der angesprochenen Adreßdatei § 13 Abs. 1 Nr. 2, zweite Alternative, LDSG zu beachten ist. Danach dürfen die personenbezogenen Daten nur für Zwecke genutzt werden, für die sie erstmals gespeichert worden sind.

Hinsichtlich der Datenübermittlung an nichtöffentliche Stellen ist nach § 16 LDSG zu verfahren. Gemäß der in Nummer 1 getroffenen Regelung ist die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und Regelungen über die Zweckbindung nicht entgegenstehen. Die beabsichtigte Datenübermittlung (Adreßdatei der an Informationsmaterial über die Verbandsgemeinde Interessierten) seitens der Verbandsgemeindeverwaltung (Touristinformation) an private Dritte (Beherbergungsbetriebe) stellt zweifellos eine Zweckänderung dar. Sodann steht zu fragen, ob die Voraussetzungen für die Zulässigkeit einer Zweckdurchbrechung nach § 12 Abs. 4 oder § 13 Abs. 2 Nr. 3 LDSG vorliegen. Das ist unter anderem dann der Fall, wenn eine Rechtsvorschrift dies vorsieht oder offensichtlich ist, daß dies im

Interesse der Betroffenen liegt und kein Grund zu der Annahme besteht, daß sie in Kenntnis des Zwecks ihre Einwilligung verweigern würden oder die Daten unmittelbar aus allgemein zugänglichen Quellen entnommen werden können oder beispielsweise für die wissenschaftliche Forschung erforderlich sind. Auf der Grundlage des vorgetragenen Sachverhalts war allerdings davon auszugehen, daß die in diesen Vorschriften genannten Fallgruppen, bei deren Vorliegen personenbezogene Daten auch für andere Zwecke genutzt werden dürfen, nicht einschlägig gewesen sind.

Insbesondere ist nicht davon auszugehen, daß jeder an Informationsmaterial über das touristische Angebot der Verbandsgemeinde Interessierte es wünscht, sozusagen in den Verteiler der ortsansässigen Beherbergungsbetriebe aufgenommen zu werden. Es läßt sich bereits aufgrund allgemeiner Lebenserfahrung sagen, daß einer Vielzahl lediglich an der Zusendung von Prospektmaterial (z. B. in bezug auf Sehenswürdigkeiten) gelegen sein wird.

Nach § 16 Abs. 1 Nr. 2 LDSG dürfen personenbezogene Daten an nichtöffentliche Stellen durch Behörden weitergegeben werden, wenn eine Rechtsvorschrift dies vorsieht, die Betroffenen eingewilligt haben, dies zur Abwehr erheblicher Nachteile für die Allgemeinheit oder die Rechte einzelner erforderlich ist oder die Daten unmittelbar aus allgemein zugänglichen Quellen entnommen werden können oder die datenverarbeitende Stelle sie veröffentlichen durfte. Eine Übermittlung personenbezogener Daten an Private ist nach Nummer 3 dann zulässig, wenn ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht wird und überwiegende schutzwürdige Interessen der Betroffenen nicht entgegenstehen. Die Übermittlung personenbezogener Daten an nichtöffentliche Stellen kann im Einzelfall nach Nummer 4 zulässig sein, wenn dies im öffentlichen Interesse liegt oder der Empfänger ein berechtigtes Interesse an den Daten geltend macht und die Betroffenen nach Unterrichtung über die beabsichtigte Übermittlung nicht widersprochen haben.

Auch danach war hier eine Rechtsgrundlage für die Datenübermittlung nicht vorhanden.

Nach allem hat der LfD die Verbandsgemeinde darauf hingewiesen, daß es durchaus möglich wäre, die Daten gem. § 16 Abs. 1 Nr. 4 LDSG zu übermitteln; nämlich dann, wenn seitens der Beherbergungsbetriebe ein berechtigtes Interesse geltend gemacht würde – hierzu zählt jedes ideelle und wirtschaftliche Interesse, das im Rahmen der Rechtsordnung verfolgt werden kann – und die Betroffenen nach Unterrichtung über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck der Datenübermittlung nicht widersprochen haben. Die Unterrichtung ist umfassend (schriftlich) auszugestalten, so daß ersichtlich ist, welche personenbezogene Daten für welchen Zweck übermittelt werden sollen. Auf dieser Grundlage können die Betroffenen dann ihre Entscheidung bezüglich eines etwaigen Widerspruchs treffen.

14.5 Musterentwurf zur Durchführung der §§ 14, 15 und 55 c der Gewerbeordnung (GewO)

Die datenschutzrechtliche Beurteilung des Entwurfs hat zu einer Überarbeitung der Regelungen geführt, in denen jene Gewerbezweige aufgeführt sind, bei denen die Landesregierung durch Rechtsverordnung nach § 38 GewO bestimmen kann, welche Auskünfte die Gewerbetreibenden den für die Überwachung zuständigen Behörden zu erteilen haben. Es handelt sich u. a. um die Bereiche An- und Verkauf von Gebrauchtwaren, An- und Verkauf von Edelmetallen und edelmetallhaltigen Legierungen, Auskunfteien, Detekteien, Vermittlung von Eheschließungen sowie den Betrieb von Reisebüros und die Vermittlung von Unterkünften.

Ursprünglich war vorgesehen, daß die Behörde in diesen Fällen vom Gewerbeanzeigenden ein Führungszeugnis von Amts wegen direkt beim Bundeszentralregister einholt. Gegen eine solche Vorgehensweise hat der LfD Bedenken angemeldet und darauf hingewiesen, daß die zuständige öffentliche Stelle gem. § 11 Abs. 1 Satz 1 GewO personenbezogene Daten des Gewerbetreibenden erheben darf, soweit die Daten zur Beurteilung der Zuverlässigkeit und der übrigen Berufsausübungskriterien bei der Durchführung gewerberechtlicher Vorschriften und Verfahren erforderlich sind. Nach Abs. 2 Satz 1 sind die Daten grundsätzlich beim Betroffenen zu erheben.

Die nunmehr vorgesehene Regelung, wonach nicht mehr von Amts wegen ein Führungszeugnis eingeholt wird, sondern bei einer Anmeldung der genannten Gewerbe den Anzeigenden aufzugeben ist, ein Führungszeugnis vorzulegen, entspricht den vorgenannten Erfordernissen. Auch die Vorgabe, daß die Einholung von Amts wegen dann möglich ist, wenn die Aufforderung zur Vorlage eines Führungszeugnisses erfolglos bleibt, hat eine gesetzliche Grundlage, die in der überarbeiteten Fassung mit dem Hinweis auf § 31 BZRG zum Ausdruck kommt. In diesem Zusammenhang wurde – was die Erhebung personenbezogener Daten bei Dritten anbelangt – angeregt, ergänzend die Regelung des § 11 Abs. 3 GewO in Bezug zu nehmen, wonach die Einholung von Auskünften nach § 31 BZRG (Erteilung des Führungszeugnisses an Behörden) unberührt bleibt.

Aus datenschutzrechtlicher Sicht ist damit das informationelle Selbstbestimmungsrecht der betroffenen Personen gewahrt; denn es wird für die Gewerbeanzeigenden die Möglichkeit eröffnet, selbst zu entscheiden, ob unter den konkreten Umständen das Führungszeugnis vorgelegt oder z. B. die Gewerbeanzeige zurückgenommen wird.

14.6 Automatische Gebührenerhebung auf Autobahnen

Nach den Vorstellungen des Bundesverkehrsministeriums sollen – langfristig gesehen – Autobahngebühren erhoben werden. Geplant ist die Errichtung elektronischer streckenbezogener Abrechnungssysteme (road-pricing). Überlegungen in diese

Richtung werden nicht nur in Deutschland angestellt. Die Verkehrsminister der Europäischen Union haben sich darüber verständigt, daß ab 1998 streckenbezogene Gebühren mit Mitteln elektronischer Techniken erhoben werden können.

Eine unverzichtbare Voraussetzung für die Einführung elektronisch bemessener Straßenbenutzungsgebühren ist eine Klärung sämtlicher Fragen des Datenschutzes. Auch nach Auffassung des Bundesverkehrsministeriums darf der Autofahrer künftig nicht von einem „elektronischen Überwachungsstaat" kontrolliert werden. Eine Inbetriebnahme derartiger Systeme, die sowohl räumliche als auch zeitliche Parameter verarbeiten, setzt grundsätzlich die Wahrung der Anonymität der Benutzer voraus. Es muß daher eine Trennung personenbezogener Daten von den zum Betreiben des Systems notwendigen Informationen vorgenommen werden. Die automatisierte Gebührenerhebung darf nicht die Möglichkeit schaffen, Bewegungsprofile einzelner Personen zu erstellen. Eine Fahrtroutenverfolgung muß ausgeschlossen werden. Die Abwicklung der Gebührenerhebung und der Kontrollvorgänge muß eindeutig und rechtssicher geregelt werden. In diesem Zusammenhang könnte man sich an bereits vorhandenen Regelungen – z. B. bei der Telefondatenerfassung – orientieren.

Aufgrund der von der Industrie angebotenen verschiedenartigen Systemarchitekturen sind unterschiedliche Szenarien innerhalb und zwischen den einzelnen Phasen der automatisierten Gebührenerfassung möglich. Diese berühren wiederum in unterschiedlicher Weise die Datenschutzproblematik. Beispielsweise werden gegenwärtig Systeme erprobt, die auf Mikrowellentechnik und solche, die auf Mobilfunktechnik basieren.

In mehreren Bundesländern werden Pilotversuche zur automatisierten Erfassung von Straßenbenutzungsgebühren durchgeführt. Für den Bereich der automatisierten Autobahngebührenerfassung war dies ein einjähriger Großversuch auf einem Autobahnteilstück der BAB 555 zwischen Bonn und Köln. Unter Beteiligung verschiedener Firmenkonsortien wurden dabei vom TÜV Rheinland im Auftrag des Bundesverkehrsministeriums insgesamt zehn unterschiedliche Systeme im Rahmen eines Feldversuches unter praktischen Bedingungen erprobt.

Wegen der mit einer flächendeckenden automatisierten Gebührenerfassung verbundenen Datenschutzrisiken (vgl. Tz. 14.7) haben die Datenschutzbeauftragten des Bundes und der Länder bereits frühzeitig auf die Notwendigkeit technischer Vorkehrungen hingewiesen.

Diese sind in hohem Maß von der konkreten Ausgestaltung des jeweiligen Erhebungsverfahrens abhängig. Die im Rahmen des Großversuchs eingesetzten Systeme weisen dabei zum Teil erhebliche Unterschiede auf. Neben Systemen, welche das vorhandene satellitengestützte Global Positioning System (GPS) zur Positionsbestimmung der einzelnen Fahrzeuge nutzen, sind Lösungen vorhanden, bei welchen über mobile oder festinstallierte Empfangseinrichtungen mit der on-board-unit des Fahrzeugs eine Standortbestimmung und gegebenenfalls Fahrzeugidentifikation vorgenommen wird.

Grundsätzlich stehen für die streckenabhängige elektronische Gebührenerfassung und -abrechnung zwei Verfahren zur Verfügung: Post-Paid und Pre-Paid.

Bei Post-Paid-Verfahren ist dabei zur nachträglichen Abrechnung über ein Gebührenkonto regelmäßig die Identifikation des Fahrzeugs bzw. des Verkehrsteilnehmers sowie die Feststellung der zurückgelegten Strecke und des Zeitpunkts der Gebührenerfassung erforderlich. Damit besteht bei den Abrechnungsstellen grundsätzlich die Möglichkeit, „Bewegungsbilder" zu erstellen.

Bei Pre-Paid-Verfahren erfolgt hingegen die Abrechnung über die Abbuchung vorausbezahlter „Streckeneinheiten" von einer, der (anonymen) Telefonkarte vergleichbaren, Chipkarte. Dieses Verfahren erlaubt damit weitgehend „datenfreie Fahrt".

Aber auch hier bestehen aufgrund der erforderlichen Überwachungs- und Kontrollmaßnahmen ähnliche Probleme wie bei der Erfassung. Um Mißbrauch möglichst auszuschließen oder zu verfolgen, wird eine Autobahnbenutzung ohne Chipkarte bzw. mit ungültiger oder defekter Chipkarte erfaßt und das Fahrzeug identifiziert (Videoaufnahme/Photo/Senderkennung). Um im Rahmen einer gerichtlichen Auseinandersetzung einen entsprechenden Nachweis führen zu können, kann auch die längerfristige Speicherung von Zeitpunkt, Mautstation, Senderkennung bzw. Kfz-Kennzeichen, Gebührenhöhe usw. erforderlich sein.

Die eingesetzte Technik bietet dabei grundsätzlich auch die Möglichkeit einer flächendeckenden Vollerfassung (z. B. in Fahndungsfällen); die Beschränkung auf die Erfassung lediglich der obengenannten Fälle ist von der Technik nicht vorgegeben. Aus Datenschutzsicht wäre daher technisch sicherzustellen, daß ein „Umschalten" auf eine flächendeckende Kontrolle verhindert oder wesentlich erschwert wird. Es muß gewährleistet sein, daß der Einsatz der Kontrollsysteme nachvollziehbar und kontrollierbar ist; dies setzt eine entsprechende Protokollierung voraus. Für die nicht mehr benötigten Fahrzeug-/Fahrerdaten ist die automatische Löschung vorzusehen.

Welche technische Lösung letztlich im Fall einer automatisierten Gebührenerfassung auf Autobahnen eingesetzt werden sollte, ist jedoch zur Zeit noch offen. Die Zielsetzung des Pilotversuches auf der BAB 555 bestand primär in der Erprobung unter-

schiedlicher Verfahrenskomponenten für Erfassung, Abrechnung und Überwachung; der Einsatz eines einheitlichen Systems ist danach nicht zwingend.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher auf ihrer 49. Konferenz die aus ihrer Sicht zu berücksichtigenden grundlegenden Anforderungen an Systeme zur automatischen Erhebung von Straßenbenutzungsgebühren formuliert (vgl. Anlage 19). Insbesondere deren Umsetzung bei der weiteren Entwicklung wird Gegenstand der künftigen Befassung der Datenschutzbeauftragten mit derartigen Systemen sein.

14.7 Die Grunderwerbsverzeichnisse im Planfeststellungsverfahren

Seitens einer Bezirksregierung wurde die Frage an den LfD herangetragen, ob es zulässig ist, daß die Grunderwerbsverzeichnisse als Bestandteil der Planunterlagen für jedermann zur Einsicht ausgelegt werden, wobei diese Verzeichnisse unter anderem neben der Lage, der Größe und der Nutzungsart des Grundstücks auch die Eigentümer mit Namen, Vornamen sowie Anschrift aufführen. Das Problem stellt sich sowohl im Planfeststellungsverfahren nach allgemeinem Verwaltungsverfahrensrecht als auch in den spezialgesetzlich erfaßten Planfeststellungen, wie z. B. im Bereich der straßenrechtlichen oder eisenbahnrechtlichen Planfeststellung.

Im Hinblick auf den Datenschutz in den Planfeststellungsverfahren wurde bislang hauptsächlich die Frage diskutiert, ob es zulässig ist, die Namen und Anschriften von Personen weiterzugeben, die Einwendungen gegen das planfeststellungsbedürftige Vorhaben erhoben haben. In diesem Zusammenhang hat die 3. Kammer des 1. Senats des Bundesverfassungsgerichts bereits eine Entscheidung getroffen, wonach personenbezogene Daten, die ein Einwendungsführer der Planfeststellungsbehörde preisgibt, einer besonderen Zweckbindung unterliegen (NVwZ 90, 1162). Diese Zweckbindung wird nach Auffassung des Gerichts durch eine öffentliche Bekanntmachung der nicht anonymisierten Daten im Planfeststellungsbeschluß unterlaufen und im Ergebnis aufgelöst. Bei diesem höchstrichterlich entschiedenen Problembereich ging es also – zeitlich gesehen – um die Schlußphase des Verfahrens, nämlich den Planfeststellungsbeschluß als einheitliche Entscheidung gegenüber allen Beteiligten.

Das Problemfeld, um das es hier geht, liegt – zeitlich gesehen – ganz am Anfang des Verfahrens. Ein Planfeststellungsverfahren wird mit dem Einreichen des Plans durch den Träger des Vorhabens bei der Anhörungsbehörde eingeleitet. Der nächste Verfahrensabschnitt besteht in der Planauslegung. Zu den Planunterlagen gehört auch das Grunderwerbsverzeichnis. Es enthält die von der Planung betroffenen Grundstücke. Dabei werden, offensichtlich seit jeher, jedenfalls in Rheinland-Pfalz, die Eigentümer mit Namen, Vornamen sowie Anschrift aufgeführt. Die Betroffenen haben weder selbst die Daten preisgegeben noch in die Übermittlung an jedermann im Rahmen der Planauslegung eingewilligt.

Fraglos liegt hier ein Eingriff in das informationelle Selbstbestimmungsrecht der Grundstückseigentümer vor, der einer gesetzlichen Grundlage bedarf, die dem Gebot der Normenklarheit entsprechen und den Verhältnismäßigkeitsgrundsatz beachten muß. Aus den nach § 73 Abs. 1 Satz 2 VwVfG einzureichenden Planunterlagen soll u. a. erkennbar sein, welche Grundstücke von dem Vorhaben betroffen sind. Die Planauslegung hat den Zweck der Information potentiell Betroffener, denen es dadurch ermöglicht wird zu prüfen, ob sie in ihren Rechten berührt sein können, und dient als Entscheidungshilfe dafür, ob im Anhörungsverfahren Einwendungen erhoben werden sollen. Es ist fraglich, ob die Angabe von Namen und Anschriften privater Grundstückseigentümer dazu erforderlich ist. Eine diesbezügliche normenklare Regelung im Hinblick auf die Preisgabe personenbezogener Daten in einer besonders intensiven Form, nämlich der öffentlichen Auslegung, ist in § 73 VwVfG jedenfalls nicht enthalten. Als Alternative käme hier die Zuordnung eines Grundstücks zu einem bestimmten Eigentümer, beispielsweise durch eine Referenzliste, in Betracht, die bei der Planfeststellungsbehörde geführt werden könnte.

Seitens des Landesamtes für Straßen- und Verkehrswesen wurde zwischenzeitlich vorgetragen, daß – auch in anderen Bundesländern – bislang keine Beanstandungen oder Beschwerden im Zusammenhang mit der Offenlegung der Grunderwerbsverzeichnisse bekannt geworden seien. Eine Forderung nach Verschlüsselung würde, bezogen auf die z. Z. in Rheinland-Pfalz laufenden Verfahren, einen Kostenmehraufwand von etwa zwei Millionen DM bedeuten. Fernerhin hat das Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau auf die Verknüpfung des Bundesfernstraßengesetzes und des Landesstraßengesetzes mit dem Landesenteignungsgesetz hingewiesen. § 19 Bundesfernstraßengesetz enthält Regelungen bezüglich der Zulässigkeit der Enteignung und verweist in Absatz 5 auf die im übrigen geltenden Enteignungsgesetze der Länder. Demgemäß gilt hinsichtlich der Enteignung nach § 9 Abs. 11 Landesstraßengesetz im übrigen das Landesenteignungsgesetz. Dies wiederum eröffnet mit seinen §§ 28 und 29 für die Enteignungsbehörde die Möglichkeit – soweit sie dies für sachdienlich hält – ein Planfeststellungsverfahren durchzuführen. Nach § 28 Abs. 2 sind dem Plan beglaubigte Grundbuchauszüge über die von den Vorhaben betroffenen Grundstücke und ein Verzeichnis aller Eigentümer und sonstigen Beteiligten beizufügen. Seitens des zuständigen Ministeriums wird nun argumentiert, daß dieses – enteignungsrechtliche – Planfeststellungsverfahren dem straßenrechtlichen Planfeststellungsverfahren funktional gleich sei, mit der Folge, daß speziell § 28 Abs. 2 in die rechtliche Würdigung des Problems einbezogen werden sollte.

Vorbehaltlich des Ergebnisses einer meinungsbildenden Umfrage bei den Datenschutzbeauftragten des Bundes und der Länder nach den dortigen Erfahrungen und Erkenntnissen zu dieser Thematik vertritt der LfD dazu folgende Auffassung:

Die in Bezug genommenen Vorschriften des Bundesfernstraßengesetzes und des Landesstraßengesetzes betreffen das Enteignungsrecht des Trägers der Straßenbaulast. Für diesen Tätigkeitsbereich sind folgerichtig jeweils Verweisungen auf das Landesenteignungsgesetz enthalten. Daraus folgt indessen, daß die Regelung, die der Gesetzgeber bereichsspezifisch (nur) für das enteignungsrechtliche Planfeststellungsverfahren getroffen hat, auf anderweitige Planfeststellungen gerade nicht anzuwenden ist. Wäre dies gewollt, so enthielten die seit nahezu zwanzig Jahren geltenden verwaltungsverfahrensrechtlichen Vorschriften zum Anhörungsverfahren in der Planfeststellung sicherlich entsprechende Bestimmungen. Letztlich wird der Gesetzgeber nicht umhinkommen, Klarheit bezüglich der Handhabung der Grunderwerbsverzeichnisse zu schaffen.

14.8 Neukonzeption des automatisierten Ordnungswidrigkeitenverfahrens

Das vom Landesrechenzentrum Mainz für eine Vielzahl von Bußgeldstellen des Landes Rheinland-Pfalz zur Verfügung gestellte automatisierte Ordnungswidrigkeitenverfahren wird gegenwärtig neu konzipiert. Es ist grundsätzlich vorgesehen, damit alle Ordnungswidrigkeitenverfahren, und nicht nur – wie bislang – Verkehrsordnungswidrigkeiten zu bearbeiten. Dennoch soll sich das automatisierte Ordnungswidrigkeitenverfahren zunächst auf diese Anwendung beschränken. Durch die frühzeitige Beteiligung des LfD war es möglich, datenschutzrechtliche Gesichtspunkte im Hinblick auf die Grundstruktur des Verfahrens einzubringen.

So wurde festgelegt, daß abgeschlossene Fälle bis zum Zeitpunkt der Verfolgungsverjährung (sechs Monate nach Erlaß des Bußgeldbescheides) automatisiert zur Verfügung stehen. Mit Ablauf dieser Frist werden lediglich die Grunddaten für weitere drei Jahre, nämlich bis zum Fristablauf der Vollstreckungsverjährung, zu Auskunftszwecken automatisiert zur Verfügung gestellt. Im Zusammenhang mit dem Verfahren zur Auskunftserteilung aus dem Ordnungswidrigkeitenverfahren an Dritte hat der LfD empfohlen, allgemein festzulegen, daß telefonische Auskünfte nur dann gegeben werden sollen, wenn der Anrufer zurückgerufen wird.

Die Protokollierung erfolgt derzeit über ein Log-Band, dessen Inhalt anläßlich datenschutzrechtlicher Kontrollen nur schwerlich ausgewertet werden kann. Künftig sollen alle durchgeführten Aktionen – auch fehlerhafte Zugriffe – mit Datum und Sachbearbeiter protokolliert werden, wobei die Modalitäten der Auswertungsmöglichkeiten in einer Dienstanweisung festzulegen sind.

Die Buchung der eingehenden Zahlungen durch die Regierungshauptkasse erfolgt gegenwärtig im Datenbestand des Ordnungswidrigkeitenverfahrens. Um sicherzustellen, daß künftig die Regierungshauptkasse nicht auf diesen Datenbestand zugreifen kann, sollen die eingehenden Zahlungen durch die Regierungshauptkasse getrennt erfaßt und über eine Schnittstelle an das Ordnungswidrigkeitenverfahren übergeben werden.

Noch nicht abschließend geklärt ist die Forderung nach einer zwingenden Speicherung aller Führerscheindaten eines Betroffenen auch dann, wenn offensichtlich kein Fahrverbot zu verhängen ist. Zunächst ist hier festzustellen, daß die begangene Ordnungswidrigkeit durch einen Bußgeldbescheid geahndet wird, dessen Inhalt abschließend in § 66 OWiG geregelt ist. Die Angaben zu der Fahrerlaubnis sind darin nicht enthalten. Fernerhin besteht eine Pflicht zur Angabe personenbezogener Daten für den Betroffenen gem. § 111 OWiG nur bezüglich Vorname, Familien- bzw. Geburtsname, Familienstand, Beruf, Wohnort, Wohnung und Staatsangehörigkeit. Der Betroffene ist demnach also nicht verpflichtet, Angaben zum Führerschein zu machen. Eine solche Pflicht besteht auch nicht etwa gem. § 4 Abs. 2 Satz 2 StVZO. Dies schließt natürlich nicht aus, daß der Betroffene freiwillig Angaben zum Führerschein machen kann, setzt jedoch voraus, daß er über die Freiwilligkeit seiner Angaben unterrichtet wird. Vor dem Hintergrund, daß eine fehlende Fahrerlaubnis einen Straftatbestand darstellt, der eine Strafanzeige und die Unzuständigkeit der Bußgeldstelle zur Folge hat, hält der LfD die Aufnahme eines Merkmals „erforderliche Fahrerlaubnis" mit der Angabe „ja/nein" für ausreichend.

Keine Übereinstimmung konnte bislang hinsichtlich der Ausgestaltung von Zeugenangaben bei Schreiben an den Betroffenen erzielt werden. Der LfD hat dabei die Auffassung vertreten, daß in dem auf die Ahndung von Ordnungswidrigkeiten gerichteten Verwarnungsverfahren die Angabe des Zeugen weder vorgeschrieben noch untersagt ist. Für die Nennung der Zeugen spricht zwar im Grundsatz das Rechtsstaatsprinzip, das es angezeigt erscheinen läßt, einem mit einer Sanktion (Verwarnungsgeld) belegten Betroffenen auch die Grundlage der gegen ihn gerichteten Anzeige zu nennen. In diesem frühen Verfahrensstadium kann aber, je nach Lage des Einzelfalls, häufig der Aspekt des Zeugenschutzes vor dem Interesse eines Betroffenen, den Namen eines Zeugen zu kennen, überwiegen. Um dem Rechnung zu tragen, sollte nach Auffassung des LfD auf die konkrete Zeugenbenennung im Anhörungsbogen verzichtet und der Zeuge statt dessen als „vorhanden" oder „bekannt" ausgewiesen werden.

Im Bußgeldbescheid hingegen ist nach § 66 Abs. 1 Ziffer 4 OWiG das Beweismittel anzugeben. In diesem Zusammenhang könnte es jedoch sinnvoll sein zu unterscheiden, ob es sich um einen „dienstlichen" oder einen „privaten" Zeugen handelt. Sofern neben einer Privatperson ein „dienstlicher" Zeuge (Polizeibeamter mit Angabe der Dienststelle) vorhanden ist, sollte auf die konkrete Angabe des „privaten" Zeugen verzichtet werden. Es erscheint hier als ausreichend, wenn neben der konkreten Angabe des „dienstlichen" Zeugen auf das Vorhandensein anderer Zeugen hingewiesen wird (z. B.: POM Mustermann, SPI

Musterhausen – „und andere Zeugen"). Für den Fall, daß ausschließlich eine Privatperson als Zeuge vorhanden ist, genügt es nach Ansicht des LfD, wenn im Bußgeldbescheid der Name des Zeugen – ohne weitere Angaben – aufgeführt ist.

Bereits mit Schreiben vom Februar 1995 hat der LfD das Ministerium des Innern und für Sport hierzu um eine Stellungnahme gebeten, die bislang allerdings nicht vorliegt. Es wurde lediglich mitgeteilt, daß man dieser Betrachtungsweise nicht folgen könne. Zwischenzeitlich hatte das Ministerium um schriftliche Ausführungen des Ministeriums der Justiz gebeten, die wiederum seit August 1995 dem Ministerium des Innern und für Sport (aber nicht dem LfD) vorliegen. Zunächst sollen, so das Ministerium, die Ausführungen des Ministeriums der Justiz „geprüft und bewertet" werden. Danach würde das Ergebnis (auch) dem LfD „unverzüglich" mitgeteilt. Soweit der Verfahrensstand zum 1. Oktober 1995, dem Zeitpunkt der Vorlage des Tätigkeitsberichts. Wenn auch eine schriftliche Stellungnahme des Ministeriums des Innern und für Sport noch nicht vorhanden ist, erscheint es doch angebracht, im Rahmen dieses Tätigkeitsberichts die Position des LfD hinsichtlich der Zeugenangabe im Bußgeldbescheid zu verdeutlichen.

Zunächst wird man tatsächlich davon ausgehen können, daß es bei der Bewertung des Beweismittels durch den Betroffenen regelmäßig nicht auf die Kenntnis der Wohnanschrift des Zeugen ankommt. Was die rechtliche Seite anbelangt, so wird hier nicht verkannt, daß nach § 222 StPO das Gericht bei der Namhaftmachung von Zeugen deren Wohn- oder Aufenthaltsort anzugeben hat und die Vorschriften der StPO nach § 46 Abs. 1 OWiG sinngemäß für das Bußgeldverfahren gelten; damit gilt auch die Regelung des § 68 StPO, wonach lediglich gefährdeten Zeugen gestattet werden kann, ihren Wohnort nicht anzugeben. Ebenso wird gesehen, daß der Betroffene nach der mit dem Justizmitteilungsgesetz geplanten Änderung des Ordnungswidrigkeitengesetzes die Möglichkeit haben wird, Einsicht in die Akte seines Bußgeldverfahrens zu nehmen.

Sollte die angekündigte schriftliche Stellungnahme des Ministeriums des Innern und für Sport keine darüber hinausgehenden Gesichtspunkte enthalten, wird der LfD bei seiner Position bleiben. Denn die regelmäßige Angabe des Wohnorts berücksichtigt nicht genügend den Grundsatz der Verhältnismäßigkeit, insbesondere im Hinblick auf die Bedeutung des Vorwurfs bei Verkehrsordnungswidrigkeiten, die überwiegend geringfügige Verfehlungen im Straßenverkehr betreffen. Das Gebot der Verhältnismäßigkeit verlangt in diesen Fällen eine Abstufung gegenüber den im Strafverfahren gebotenen Mitteln. Wenn nun der Betroffene die Rechtsfolgen des Bußgeldbescheides ablehnt, steht seinem Informationsinteresse (abgesehen von jenen in § 68 Abs. 2 StPO geregelten Fällen) nichts entgegen. Die Angabe der Wohnanschrift des Zeugen schon im Bußgeldbescheid führt jedoch dazu, daß oftmals personenbezogene Daten offenbart werden, deren Weitergabe nicht erforderlich ist. Was die Förderung von Nachforschungen zum Privatleben eines Zeugen anbelangt, bleibt im übrigen stets zu beachten, daß diesen Personen (wie jedem Staatsbürger) das Grundrecht auf informationelle Selbstbestimmung zusteht, in das nicht ohne wichtigen Grund eingegriffen werden darf.

Abschließend sei auch auf eine Entwicklung in der Rechtsprechung hingewiesen, die dem Informantenschutz Vorrang gegenüber dem Auskunftsinteresse des Betroffenen einräumt. Beispiele finden sich in den Entscheidungen des Bundesverwaltungsgerichts vom 3. September 1991 (Az.: 1 C 48/88; DuD 92, 490) und vom 17. September 1993 (Az.: 1 B 125.93; RDV 94, 28).

15. Landwirtschaft, Weinbau und Forsten

15.1 Müssen Öko-Landwirte gegenüber privaten Kontrollstellen die Betriebsdaten offenbaren?

Dem LfD ist bekanntgeworden, daß Kontrollverfahren nach der Verordnung (EWG) Nr. 2092/91 des Rates vom 24. Juni 1991 über den ökologischen Landbau und die entsprechende Kennzeichnung der landwirtschaftlichen Erzeugnisse und Lebensmittel (ABLEG Nr. L 198 S. 1) unter Einbeziehung privater Kontrollstellen (einer GmbH und einer Personengesellschaft) durchgeführt werden. Da diese Kontrollstellen in großem Umfang sensitive Informationen über die Landwirte erlangen, die sich diesem Kontrollverfahren unterziehen, ist insbesondere zu gewährleisten, daß die erhobenen und gespeicherten personenbezogenen Daten in gleicher Weise geschützt sind und ihre Verwendung auch in gleicher Weise überprüft werden kann, wie dies bei öffentlich-rechtlich organisierten Kontrollstellen der Fall ist. Die betroffenen Landwirte müssen die gleichen Rechte wie gegenüber öffentlichen Kontrollstellen haben.

Aus datenschutzrechtlicher Sicht hat der LfD deshalb in Anbetracht der Tatsache, daß die privaten Kontrollstellen wie Beliehene tätig werden, ohne aber förmlich durch einen Beleihungsakt in das öffentlich-rechtliche System von Aufsicht, Kontrolle und strafrechtlichen Sanktionen für amtspflichtwidriges Verhalten eingebunden zu sein, folgende ergänzende Maßnahmen gefordert:

Die Personen innerhalb der Kontrollstellen, die personenbezogene Daten der geprüften landwirtschaftlichen Betriebe zur Kenntnis erhalten, sind nach dem Verpflichtungsgesetz (BGBl. 1974 I, S. 547) zu verpflichten.

Die Kontrollstellen sind außerdem wie öffentliche Stellen der datenschutzrechtlichen Kontrolle durch den LfD zu unterwerfen. Dies könnte entweder durch Auflagen im Zulassungsbescheid oder auch durch eine vertragliche Verpflichtung erfolgen.

Auf dem gleichen Weg (Ergänzung der Zulassungsbescheide bzw. ergänzende vertragliche Vereinbarungen) ist zu gewährleisten, daß die betroffenen Landwirte gegenüber den Kontrollstellen die in § 6 LDSG genannten Rechte ausüben können.

Die Antwort des Ministeriums, ob und ggf. auf welche Weise diese Anforderungen wirksam erfüllt werden, steht derzeit noch aus.

15.2 Datenverarbeitung im Zusammenhang mit der Agrarförderung

Im Zusammenhang mit der Agrarförderung hat der LfD folgende Anregungen formuliert:

a) Bei der Agrarförderung für 1994 wurde eine „Einwilligungserklärung" verwendet, nach der die antragstellenden Landwirte ihre Zustimmung zur automatisierten Verarbeitung ihrer Antragsdaten und die Übermittlung dieser Daten an die beteiligten Behörden erklären. Diese Einwilligungserklärung ist aus datenschutzrechtlicher Sicht grundsätzlich abzulehnen: Es wurde bei den Antragstellern der Eindruck erweckt, ihre Einwilligung habe rechtlich eine Bedeutung. Dem ist nicht so. Die automatisierte Datenverarbeitung der für die Fördermaßnahmen erhobenen Daten war nicht aufgrund der Einwilligung, sondern aufgrund des § 5 LDSG zulässig. Die Formulierung „Einwilligung" begründet vielmehr das Mißverständnis, es bestünde eine Wahlmöglichkeit bzw. eine Freiwilligkeit im vorliegenden Zusammenhang. Der Staat sollte mißverständliche bzw. irreführende Erklärungen unterlassen. Angemessen wäre, auf die beabsichtigte automatisierte Datenverarbeitung und die Mitwirkungspflichten bei der Überprüfung hinzuweisen und eine Erklärung der Antragsteller vorzusehen, daß sie diese Hinweise zur Kenntnis genommen haben. Die Agrarverwaltung hat erklärt, dieser Anregung im Grundsatz folgen zu wollen.

b) Auch der Antrag 1994 auf soziostrukturellen Einkommenausgleich/Ausgleichszulage in den benachteiligten Gebieten enthielt eine Einwilligungserklärung. Aber auch hier war die Einwilligung als Rechtsgrundlage der automatisierten Datenverarbeitung aus datenschutzrechtlicher Sicht nicht angemessen: Eine Einwilligung kann nur dann rechtsbegründende Wirkung entfalten, wenn sie freiwillig erfolgt. Im Zusammenhang mit Maßnahmen der Agrarförderung kann von einer Freiwilligkeit der Teilnahme unter den Bedingungen des Agrarmarktes nicht ausgegangen werden: Die landwirtschaftlichen Betriebe sind überwiegend zu ihrer Existenzsicherung auf die Inanspruchnahme dieser Fördermaßnahmen angewiesen. Dementsprechend ist nicht die Einwilligungserklärung der Betroffenen, sondern der Erforderlichkeitsgrundsatz der Landesdatenschutzgesetze mit den entsprechenden Regelungen für die Erhebung und Speicherung von Daten Rechtsgrundlage für die Erhebung und automatisierte Speicherung der Förderdaten.

   Eine Einwilligungserklärung könnte allerdings eine Funktion auch in rechtsbegründender Hinsicht für die weitere Speicherung bzw. die Unterlassung der Löschung nach Abwicklung der Förderungsmaßnahme haben. Dann wäre die Einwilligung dafür einzuholen, daß die entsprechenden Daten nicht gem. § 13 LDatG (heute: § 19 Abs. 2 LDSG) nach Abschluß der Fördermaßnahme gelöscht werden, sondern daß diese Daten auch für die Bearbeitung von Folgeanträgen in Folgejahren in automatisierter Form vorgehalten werden dürfen. Auf diesen Aspekt sollte die Einwilligungserklärung allerdings auch beschränkt sein.

   Vergleichbare Überlegungen gelten für die Erklärung im Antrag „Allgemeine Regelung (mit Stillegungsverpflichtung) für 1994, Getreide, Öllein, Ölsaaten, Eiweißpflanzen und Stillegung" sowie für den Antrag „Vereinfachte Regelung (Kleinerzeugerregelung) für 1994, Getreide, Öllein, Eiweißpflanzen und Ölsaaten".

   Auch diesen Überlegungen will die Agrarverwaltung folgen.

c) Der LfD hatte außerdem problematisiert, ob zur Durchführung der o. g. Fördermaßnahmen die Vorlage von Nutzungsverträgen zwischen Eigentümern und Nutzungsberechtigten tatsächlich erforderlich sei. Die Erklärung des Ministeriums, in mehr als 12 000 Fällen sei es vorgekommen, daß ein Flurstück von mehreren Landwirten als bewirtschaftet angegeben worden sei, läßt dieses Verlangen als nachvollziehbar erscheinen. Da außerdem von dem Vorlageverlangen abgesehen werden soll, wenn sich die Fehlerzahl reduziert haben sollte, hat der LfD dieses Vorgehen nicht beanstandet.

16. Statistik

16.1 Mikrozensus 1995

Die amtliche Haushaltsbefragung „Mikrozensus und EU-Arbeitskräftestichprobe 1995" führte zu zahlreichen Anfragen, insbesondere hinsichtlich der Zufallsauswahl, der Geheimhaltung sowie der Freiwilligkeit der Beantwortung.

16.1.1 Zufallsauswahl und Geheimhaltung

Der Mikrozensus wird in jedem Jahr durchgeführt. Dabei wird jedoch nicht jedesmal eine gänzlich neue Zufallsauswahl vorgenommen. Vielmehr werden drei Viertel aller Haushalte, die schon im Vorjahr befragt wurden, wieder in die Erhebung einbezogen. Ein Viertel der Haushalte wird erstmals befragt. Das bedeutet, daß jeder Haushalt grundsätzlich über einen Zeitraum von vier Jahren hinweg für den Mikrozensus auskunftspflichtig ist. Grundlage der Zufallsauswahl ist das bewohnte Bundesgebiet, das in Flächen mit etwa gleich großer Bevölkerungszahl eingeteilt wird. Von diesen flächenbezogenen Auswahleinheiten werden dann ein Prozent mit Hilfe eines mathematisch-statistischen Zufallsverfahrens ermittelt. Das auf diese Art und Weise jeweils produzierte „statistische Gebilde" nennt man Auswahlbezirk, wobei alle in der ausgewählten Fläche wohnenden Haus-

halte in die Erhebung einbezogen werden. Ob eine Person dort gemeldet ist oder nicht, spielt also keine Rolle; ausschlaggebend sind allein die tatsächlich vorgefundenen Verhältnisse.

Vor diesem Hintergrund erklärt sich die häufig gestellte Frage, warum in der unmittelbaren Nachbarschaft weitere Haushalte in die Befragung einbezogen wurden.

Die Interviewer haben die in § 8 Mikrozensusgesetz geregelten organisatorischen Aufgaben zu erfüllen. Dazu gehört, daß sie für jeden von ihnen zu bearbeitenden Auswahlbezirk eine Verteilungsliste anlegen und für jeden dort wohnenden Haushalt einen Haushaltsmantelbogen, in den sie als Hilfsmerkmale Vor- und Familiennamen der Haushaltsmitglieder, Telefonnummer, Straße, Hausnummer, Lage der Wohnung im Gebäude sowie Vor- und Familienname des Wohnungsinhabers eintragen. Diese Hilfsmerkmale dienen lediglich der technischen Durchführung der Erhebung. Nachdem festgestellt wurde, daß die Unterlagen vollzählig sind, werden die Hilfsmerkmale von den eigentlichen Erhebungsmerkmalen getrennt. Das bedeutet, daß die bei der Befragung gemachten Angaben nicht mehr einzelnen Personen zugeordnet werden können. Aus datenschutzrechtlichen Gründen hat der Gesetzgeber diese Verfahrensweise vorgeschrieben.

16.1.2 Gestaltung der Erhebungsvordrucke

Ein Petent hat vorgetragen, daß seitens des Interviewers Angaben erfragt wurden, deren Beantwortung freiwillig ist. In diesem Zusammenhang hat der LfD das Statistische Landesamt auf das Problem der Vermengung von freiwilligen und Pflichtfragen in den Befragungsbogen des Mikrozensus 1995 hingewiesen. So wurden in den Mikrozensen der Vorjahre die auf freiwilliger Grundlage zu erhebenden Angaben auf einem gesonderten Bogen erhoben. Bei dieser Art und Weise der Gestaltung der Erhebungsvordrucke war sowohl für den Auskunftspflichtigen als auch für den Interviewer klar ersichtlich, für welche Angaben Auskunftspflicht besteht und welche Angaben Betroffene freiwillig der amtlichen Statistik zur Verfügung stellen konnten. Die Mikrozensuserhebung 1995 hat die freiwillig zu erhebenden Angaben inhaltlich unmittelbar dem jeweiligen Fragenkomplex zugeordnet und auf die Freiwilligkeit in recht unauffälliger Form durch eine leicht modifizierte Farbgebung, beim Selbstausfüllerbogen durch das Abkürzungssymbol „F" (für freiwillig) hingewiesen. Dieses Verfahren ist aus der Sicht des Datenschutzes problematisch.

Zwar sind laut Auskunft des Statistischen Landesamtes die Interviewer angehalten, vor oder während der Befragung noch einmal auf jene Fragen hinzuweisen, deren Beantwortung freiwillig ist. In der Praxis hat sich jedoch gezeigt, daß insbesondere dann, wenn der Auskunftspflichtige auf eine möglichst zügige Durchführung der Befragung Wert legt, die Gefahr besteht, daß der Interviewer die farblich hellere Unterlegung der Fragenspalten übersieht und damit den Hinweis auf die Freiwilligkeit vergißt. Das Statistische Landesamt sieht dann in solchen Fällen – sofern sie bekannt werden – von einer Verwertung der diesbezüglichen Angaben ab.

Auch die Art der Darstellung im Selbstausfüllerbogen – statt des Wortes „freiwillig" wird die Abkürzung „F" verwandt – ist schwerlich mit den Geboten der Normenklarheit und Transparenz in Einklang zu bringen. Denn es besteht die konkrete Möglichkeit, daß die Auskunftspflichtigen angesichts der Vielzahl der zu beantwortenden Fragen den Aspekt der Freiwilligkeit leicht übersehen. Dem Gebot der schriftlichen Unterrichtung über die Freiwilligkeit der Auskunftserteilung gem. § 12 Nr. 4 Mikrozensusgesetz wäre nach Auffassung des LfD nur dann entsprochen, wenn der Betroffene „auf den ersten Blick" erkennen kann, ob es sich um Fragen mit Auskunftspflicht oder um freiwillige Angaben handelt.

Künftig sollte bei dem Layout der Vordrucke auf eine entsprechende datenschutzgerechte Gestaltung besonderes Gewicht gelegt werden.

16.1.3 Inhalt des Ankündigungsschreibens

Ein weiteres Problem betrifft das vom Statistischen Landesamt entworfene Ankündigungsschreiben zur Haushaltsbefragung Mikrozensus 1995. Aus diesem Anschreiben geht nicht hervor, daß der zu Befragende den Fragebogen auch selbst ausfüllen und so den Interviewerbesuch verhindern kann. Aus datenschutzrechtlicher Sicht ist es erforderlich, die Betroffenen bereits in diesem Anschreiben darauf hinzuweisen, daß die Möglichkeit besteht, den Fragebogen auch selbst auszufüllen. Das Statistische Landesamt hat zwischenzeitlich die Bereitschaft angekündigt, den Text des Ankündigungsschreibens für die kommende Erhebung umzugestalten und einen expliziten Hinweis auf die verschiedenen Arten der Auskunftserteilung zu bringen.

16.2 EG-Statistikverordnung

Die Europäische Kommission hat einen Vorschlag für eine Verordnung des Rates der Europäischen Union über die Tätigkeit der Gemeinschaft im Bereich der Statistik (EG-Statistikverordnung) vorgelegt. So werden hinsichtlich der Harmonisierung von Statistiken der EU-Staaten gemeinschaftsrechtliche Regelungen angestrebt, die zum Teil erhebliche Auswirkungen auf das nationale Statistikrecht – insbesondere auf das Statistikgeheimnis – hätten. Die Datenschutzbeauftragten des Bundes und der Länder haben sich in einer Entschließung vom 25. August 1994 zu diesem Thema geäußert (s. Anlage 26) und betont, daß bislang eine selbständige und unabhängige Stellung des Statistischen Amtes der Europäischen Gemeinschaften nicht gewährleistet ist.

Außerdem widerspricht es dem Gebot der Abschottung, wenn die Möglichkeit eröffnet werden soll, vertrauliche statistische Daten an Stellen außerhalb des Statistischen Amtes der Europäischen Gemeinschaften zu übermitteln. Ein weiterer Kritikpunkt ist das Fehlen einer Regelung bezüglich der Trennung und Aufbewahrung von Erhebungs- und Hilfsmerkmalen.

Es bleibt zu hoffen, daß hier die erforderlichen Korrekturen alsbald in Angriff genommen werden.

Hinzu kommt ein Grundproblem, das darin zu sehen ist, daß bislang die Europäische Kommission weder verbindliche Rechtsvorschriften für den Datenschutz in ihrer Verwaltung erlassen noch eine Datenschutzkontrolle eingerichtet hat. Sie hat allerdings bereits am 13. September 1990 mit dem ersten Entwurf zur EG-Datenschutzrichtlinie eine Erklärung veröffentlicht (KOM 90, 314 endg. – SYN 287 – 288), in der sie den Wunsch zum Ausdruck brachte, daß die Grundsätze der Datenschutzrichtlinie auf die Organe und Einrichtungen der Europäischen Gemeinschaft Anwendung finden sollen, und sich selbst verpflichtet, in ihrem Zuständigkeitsbereich die wesentlichen Grundsätze der EG-Datenschutzrichtlinie ab dem Erklärungszeitpunkt anzuwenden. Indes ist bisher nicht bekannt, was zur Umsetzung der Erklärung seitens der Kommission geschehen ist. Solange keine konkreten Maßnahmen ersichtlich sind, die zu einer Verwirklichung des Datenschutzes innerhalb der EU-Verwaltung führen, können Regelungen wie beispielsweise in Artikel 16 des Verordnungsentwurfs, wonach eine Gemeinschaftsdienststelle unmittelbaren Zugang zu einzelstaatlichen Verwaltungsregistern haben soll, nicht akzeptiert werden.

16.3 Verdiensterhebungen in Industrie und Handel

Ein Petent rügte, sein Betrieb werde seit Jahren in erheblicher Weise durch statistische Arbeiten im Bereich Verdiensterhebung sonderbelastet. Er vertrat die Auffassung, daß eine Stichprobenauswahl überhaupt nicht stattgefunden haben könne. Eine derartige Trefferquote sei im Rahmen einer Zufallsauswahl nicht zu erklären. Der LfD wies den Petenten darauf hin, daß die Verdiensterhebungen in Industrie und Handel gemäß den Regelungen des Gesetzes über die Lohnstatistik, nämlich die vierteljährliche Verdiensterhebung und die Bruttojahresverdiensterhebung, als Repräsentativerhebungen konzipiert sind. Die Neuauswahl der Berichtsbetriebe findet nach dem Zufallsprinzip statt, wobei auf der Basis der Ergebnisse der Arbeitsstättenzählung zuletzt die in § 12 Abs. 2 des Lohnstatistikgesetzes vorgeschriebene Neuauswahl im August 1991 durchgeführt wurde. Grundlage dieser Stichprobenauswahl ist ein vom Statistischen Bundesamt erstellter bundeseinheitlicher Stichprobenplan. Die Auskunftspflicht der ausgewählten Berichtsbetriebe begann mit dem Berichtsmonat Oktober 1991 und gilt bis zur nächsten Neuauswahl der Betriebe, die gemäß § 12 Abs. 2 Satz 2 des Lohnstatistikgesetzes nach vorliegenden Ergebnissen der nächsten Arbeitsstättenzählung vorzunehmen ist.

Vor diesem gesetzlichen Hintergrund erklärt sich die von dem Petenten angesprochene Trefferquote. Die Vermutung, sein Betrieb sei für jeden Berichtsmonat neu ausgewählt worden, traf mithin nicht zu.

17. Personaldatenverarbeitung

17.1 Telefonanlagen und Mitbestimmung

Anfragen verschiedener Personalräte haben den LfD veranlaßt, zu folgenden Fragen im Zusammenhang mit der Speicherung von Telefondaten in Behörden Stellung zu nehmen.

17.1.1 Dürfen die Nummern aller Dienstgespräche vollständig gespeichert werden?

Aus datenschutzrechtlicher Sicht bestehen keine Bedenken dagegen, die Nummern aller Dienstgespräche vollständig zu speichern. Ausgenommen sind allerdings Bereiche, in denen besondere Vertraulichkeitsbestimmungen (Geheimhaltungsvorschriften) bestehen. Soweit etwa Gespräche betroffen sind, die dem Arztgeheimnis oder einem vergleichbaren Schutz (vgl. § 203 Abs. 1 StGB) unterliegen, ist die Frage der Zulässigkeit der Speicherung differenziert zu beurteilen.

17.1.2 In welchem Umfang dürfen Telefondaten über im Dienst geführte private Gespräche gespeichert werden?

Bezüglich dieser Frage vertritt der LfD in Fortsetzung einer entsprechenden Auffassung der DSK die Meinung, daß zum Schutz des informationellen Selbstbestimmungsrechts der angerufenen Personen die angerufenen Telefonnummern nur in verkürzter Form gespeichert werden dürfen. Dem berechtigten Bedürfnis der Bediensteten, Abrechnungen nachprüfen zu können, wird Rechnung getragen, wenn die letzten beiden Ziffern der angerufenen Telefonnummer bei der Speicherung unterdrückt werden. Auch dann können die Anrufer nachvollziehen, wer ihr Gesprächspartner gewesen ist, ohne daß Dritte entsprechende Erkenntnisse gewinnen könnten.

17.1.3 Wie lange dürfen Gesprächsdaten bei privaten Telefongesprächen gespeichert werden?

Die Speicherung von Telefondaten privater Telefonate ist wie jede Speicherung personenbezogener Daten nach ihrer Dauer zu begrenzen. Dies ergibt sich aus § 19 Abs. 2 LDSG. Danach sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die datenverarbeitende Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist. Die Er-

forderlichkeit richtet sich nach den für die datenverarbeitenden Stellen getroffenen allgemeinen Regelungen über die Dauer der Aufbewahrung von personenbezogenen Daten einschließlich der Erfordernisse einer ordnungsgemäßen Dokumentation.

Im Zusammenhang mit der Speicherung von Personaldaten kommt für die Konkretisierung der hier maßgeblichen Fristen der Mitbestimmung eine besondere Bedeutung zu. Bei der Aufbewahrungsdauer sind verschiedene Interessen und Bedürfnisse miteinander zu vereinbaren: Dem Anliegen, Gesprächsdaten über private Telefonate möglichst schnell zu löschen, steht das Erfordernis gegenüber, auch im nachhinein die Berechtigung von Abrechnungen überprüfen zu können. Dem LfD sind entsprechende Dienstvereinbarungen bekannt, die hier eine Jahresfrist für die Dauer der Speicherung vorsehen. Eine solche Frist scheint angemessen zu sein, hiervon abweichende Festlegungen wären aber ebenfalls durchaus möglich und zulässig.

17.1.4 Dürfen Gesprächsdaten der vom Personalrat geführten Telefonate aufgezeichnet werden?

Auch in diesem Zusammenhang ist darauf zu verweisen, daß in einer hierzu abzuschließenden Dienstvereinbarung Details geregelt werden sollten. Grundsätzlich ist es der Dienstbehörde nicht untersagt, entsprechende Gesprächsdaten zu speichern. Allerdings sind Vorkehrungen zu treffen, damit die hierbei gewinnbaren Erkenntnisse nicht zu einer Beeinträchtigung der Unabhängigkeit des Personalrats genutzt werden können. Denkbar wäre es, in der Dienstvereinbarung etwa vorzusehen, daß dem Dienststellenleiter nur jeweils monatlich die Summe der vom Personalrat verbrauchten Gebühreneinheiten mitgeteilt wird. Nur im Einzelfall und unter Beteiligung des Personalrats ist es dem Dienststellenleiter möglich, etwa stichprobenweise nachzuprüfen, ob nur dienstlich veranlaßte Gespräche geführt worden sind. Selbstverständlich könnte die Dienstvereinbarung auch andere oder weitergehende Konkretisierungen hierzu enthalten.

17.1.5 Gibt es technische Vorrichtungen, die dem Gesprächsteilnehmer deutlich machen, daß sein Partner die Konferenzschaltung oder das Freisprechen eingeschaltet hat?

Es gibt technische Vorrichtungen, die dem Gesprächsteilnehmer deutlich machen, daß sein Partner das Freisprechen oder die Konferenzschaltung eingeschaltet hat. Üblicherweise geschieht dies durch eine Anzeige im Display der Nebenstelle, soweit diese damit ausgestattet ist, beziehungsweise durch einen „Aufmerksamkeitston", der die Aktivierung der Leistungsmerkmale „Aufschalten" oder „Konferenzschaltung" anzeigt. Ob die genannten Leistungsmerkmale überhaupt genutzt werden können bzw. in welcher Form eine Anzeige hierüber bei den Gesprächsteilnehmern erfolgt, wird bei der Konfiguration der Nebenstellenanlage festgelegt.

Das Leistungsmerkmal „Freisprechen/Lauthören" wird zum Teil automatisch dann aktiviert, wenn der Wählvorgang bei aufgelegtem Hörer erfolgt, ansonsten durch Betätigen der Lautsprechertaste. Die Tatsache, daß das Leistungsmerkmal aktiviert wurde, wird nicht an allen Systemen optisch oder akustisch angezeigt. Soweit dies nicht der Fall ist, kommt neben einer Beschränkung bei der Ausstattung der Telefone mit Mikrofon/Lautsprecher als technische Vorbeugemaßnahme die grundsätzliche Sperre des Leistungsmerkmals, die Sperre der Lautsprechertaste oder deren Belegung mit einer anderen Funktion in Betracht.

Das Sperren von Leistungsmerkmalen kann an manchen Systemen nicht für die Vermittlungsplätze erfolgen, so daß hier lediglich eingeschränkte technische Möglichkeiten bestehen, um eine unbefugte Nutzung wirksam zu verhindern.

17.1.6 Gibt es Bereiche, z. B. bei Arbeitsplätzen mit Publikumsverkehr, in denen auf die Möglichkeit des Freisprechens und der Konferenzschaltung ganz verzichtet werden muß?

Aus datenschutzrechtlicher Sicht kann nicht davon ausgegangen werden, daß es Arbeitsbereiche gibt, in denen auf die Möglichkeit des Freisprechens oder der Konferenzschaltung ganz verzichtet werden muß. Selbst bei Arbeitsplätzen mit Publikumsverkehr kann es durchaus geboten sein, Dritte – etwa Antragsteller – unmittelbar über das zu informieren, was der Gesprächsteilnehmer am Telefon ausführt. Voraussetzung ist grundsätzlich, daß der Gesprächsteilnehmer darüber informiert ist.

17.1.7 Ist es zulässig, Störungen per Fernwartung beheben zu lassen?

Fernwartung von automatisierten Systemen ist grundsätzlich als Auftragsdatenverarbeitung anzusehen. Allerdings sind in diesem Zusammenhang besondere technische und organisatorische Maßnahmen zu treffen, um den angemessenen Schutz der betroffenen personenbezogenen Daten zu gewährleisten.

a) Hierzu zählt die Absicherung des Wählleitungsanschlusses durch die Einrichtung einer automatischen Rückruffunktion in Verbindung mit fest vorgegebenen Anschlußnummern der wartenden Stelle. Weiterhin kann das ISDN-Leistungsmerkmal „Überprüfung der Anschlußnummer (des rufenden Teilnehmers) in der Vermittlung der Telekom" genutzt werden.

b) Für die Durchführung der Fernwartung, insbesondere dann, wenn diese durch ein privates Unternehmen erfolgen soll, muß ein separater, paßwortgesicherter Wartungszugang bzw. -anschluß eingerichtet sein. Da dieser nur in Ausnahmefällen benötigt wird, sollte er für die übrige Zeit deaktiviert werden. Die Freischaltung des Anschlusses darf nur nach einer (telefoni-

schen) Abstimmung zwischen der Dienststelle und der die Wartung durchführenden Stelle erfolgen. Die Zugriffsrechte der Wartungskennung sind auf das für die Wartungsarbeiten erforderliche Maß zu beschränken.

c) Ein weiteres Merkmal ist die Protokollierung, um die Nachvollziehbarkeit und Beweissicherung (sowie ggf. die Exkulpation betroffener Mitarbeiter bei erhobenen Mißbrauchsvorwürfen) sicherzustellen. Hierbei sollten wartende Stelle, Zeitpunkt, Dauer, Ablauf und Inhalt einer Fernwartung anhand automatisch erstellter Protokolle überprüfbar sein. In diesem Zusammenhang kommt einer verläßlichen Dokumentation der Anlagenkonfiguration – ggf. in Verbindung mit einer Änderungshistorie – besondere Bedeutung zu.

d) Von Bedeutung ist schließlich noch die Vertragsgestaltung mit der fernwartenden Stelle im Rahmen des § 4 LDSG. Welche Gesichtspunkte dabei berücksichtigt werden sollten, ist den in der Anlage beigefügten Hinweisen zur Vertragsgestaltung bei der Datenverarbeitung im Auftrag zu entnehmen.

17.1.8 Darf die Änderung von Kurzwahlnummern und die Vergabe der Geheimnummern über die Fernwartung erfolgen?

Auch hier stellt sich die Frage nach der Zulässigkeit und den Anforderungen im einzelnen.

Wenn auch die Änderungen von Kurzwahlnummern und die Vergabe der Geheimnummern über die Fernwartung erfolgen sollen, bedeutet dies, daß die Systemverwaltung insgesamt im Wege der Fernwartung auf einen Auftragnehmer übertragen wurde. Auch dies ist nicht grundsätzlich ausgeschlossen. Hier sind die gleichen technischen und organisatorischen Datenschutzmaßnahmen wie allgemein bei der Fernwartung zu erfüllen.

17.1.9 Dürfen die Privatgespräche aus der Hausmeisterwohnung nummernmäßig erfaßt werden?

Die Speicherung der Privatgesprächsdaten aus der Hausmeisterwohnung unterliegt grundsätzlich den gleichen Restriktionen wie die Erfassung von Privatgesprächsdaten der anderen Bediensteten. Hier kommt allerdings noch hinzu, daß es zur Wahrung des Datenschutzes des Hausmeisters selbst seiner Einwilligung auch in diese begrenzte Speicherung bedarf. Ohne Einwilligung des Hausmeisters darf aus datenschutzrechtlicher Sicht keine Detailspeicherung erfolgen.

17.2 Zeiterfassung

Die Daten, die von automatisierten Zeiterfassungssystemen gespeichert werden, können sehr sensible Informationen enthalten. Die Gewohnheiten der Mitarbeiter können exakt nachvollzogen werden. Der LfD hat deshalb besonderen Wert darauf gelegt, daß für solche Verfahren die zulässigen Nutzungszwecke der Daten und die Personen, die diese Nutzungen vornehmen dürfen, sowie die organisatorischen und verfahrensmäßigen Voraussetzungen der Nutzung (etwa in besonderen Fällen Beteiligung des Betroffenen selbst oder des Personalrats) abschließend und möglichst exakt festgelegt werden. Hinzu kommen selbstverständlich besondere Anforderungen an den technischen Datenschutz. Beide Aspekte hat der LfD bei der Einführung des einheitlichen Zeiterfassungssystems für die obersten Landesbehörden (insbes. die Ministerien) betont, an der er umfassend beteiligt wurde.

17.3 Personalverwaltungssystem AUP beim Landesamt für Jugend und Soziales und beim Landesversorgungsamt

Im Zusammenhang mit der geplanten Zusammenlegung des Landesamtes für Jugend und Soziales und des Landesversorgungsamtes und der dabei beabsichtigten Einführung eines Personalverwaltungssystems wurde der LfD Rheinland-Pfalz um Stellungnahme u. a. hinsichtlich der erforderlichen technisch-organisatorischen Maßnahmen gebeten.

Grundlage des Verfahrens war die bei der OFD Koblenz betriebene Anwendung Computerunterstützte Personalverwaltung (CUP). Entsprechend der AUP-spezifischen Anforderungen sollte eine Anpassung erfolgen.

Aus technisch-organisatorischer Sicht waren dabei insbesondere der vorgesehene Umfang der Zugriffsberechtigungen, die Auswertungsmöglichkeiten, die Art und der Umfang der Protokollierung sowie die Anbindung und Absicherung der als Endgeräte vorgesehenen PC klärungsbedürftig.

Den Empfehlungen des LfD Rheinland-Pfalz wurde dabei weitgehend Rechnung getragen. Für das Verfahren AUP wurden die Mechanismen der Zugriffskontrolle aus CUP übernommen. Insbesondere wurden der Umfang der Zugriffsberechtigungen und die Auswertungsmöglichkeiten entsprechend der Zuständigkeit der jeweiligen Mitarbeiter beschränkt. Soweit PC als Endgeräte eingesetzt werden, verfügen diese nicht über Disketten- oder Festplattenlaufwerke. Die in der Terminalemulationssoftware vorhandene Funktion zur Dateiübertragung steht an den PC-Arbeitsplätzen nicht zur Verfügung.

17.4 Vernichtete Vorgänge im Inhaltsverzeichnis einer Personalakte – Bewerbungsunterlagen in Personalakten

Ein Bediensteter des Landes trug vor, im Inhaltsverzeichnis zu seiner Personalgrundakte seien folgende Vorgänge benannt:
- Bewerbung um die Leiterstelle seiner Behörde,
- Beschwerde über den derzeitigen Behördenchef.

Die Beschwerdevorgänge seien aus der Personalakte entfernt worden, weil sie dort inhaltlich nicht hingehört hätten; zwischenzeitlich würden sie in einer entsprechenden Sachakte aufbewahrt werden. Durch die Eintragung im Inhaltsverzeichnis jedoch werde ein bestimmter Eindruck suggeriert: Die aufgrund des Akteninhalts unüberprüfbare und deshalb besonders belastende Interpretation liege zumindest nahe, daß er sich nach einer erfolglosen Bewerbung um die Leiterstelle der Behörde über seinen neuen Chef aus wenig sachgerechten Gründen beschwert hätte.

In Übereinstimmung mit dem Ministerium des Innern und für Sport vertritt der LfD hierzu folgende Auffassung: Das Inhaltsverzeichnis darf nur Eintragungen zu solchen Vorgängen enthalten, die in der Personalakte auch vorhanden sind. Falls Vorgänge, die im Inhaltsverzeichnis genannt sind, entfernt werden, ist dann ein neues Inhaltsverzeichnis zu fertigen, wenn dies zur Wahrung der schutzwürdigen Belange des Betroffenen erforderlich ist. Im vorliegenden Fall war dies bezüglich der Beschwerdevorgänge über den neuen Behördenchef der Fall.

Aber auch die Eintragung im Inhaltsverzeichnis über die Bewerbung selbst und die Aufnahme dieser Vorgänge in die Personalgrundakte sind nicht bedenkenfrei: Bei Bewerbungsunterlagen handelt es sich üblicherweise um Vorgänge, die in eine Sachakte zu der jeweiligen Besetzung der in Betracht kommenden Stelle genommen werden. Diese Unterlagen haben keinen unmittelbaren Bezug zur Dienstausübung des sich bewerbenden Beamten und vermitteln – bei Ablehnung – eher ein negatives Bild.

Dem wird durch folgende Verfahrensweise Rechnung getragen:
Vorgänge über die Besetzung eines freien (Beförderungs-)Dienstpostens gehören zu den nicht notwendigen Bestandteilen einer Personalakte. Danach müssen Bewerbungsvorgänge nicht in Personalakten aufbewahrt werden; sie können jedoch dort aufbewahrt werden, zumindest solange dies von dem betroffenen Beamten nicht beanstandet wird. Es unterliegt also der Entscheidungsbefugnis des Betroffenen, wie hier weiter verfahren wird.

Aus der Sicht des LfD entspricht dies den datenschutzrechtlichen Anforderungen.

17.5 IT-Heimarbeitsplätze, Telearbeit

Im Zusammenhang mit den Entwicklungen der Kommunikationstechnik werden insbesondere im privatwirtschaftlichen Bereich verstärkt Telearbeitsplätze eingerichtet. Das Tätigkeitsspektrum reicht dabei von Erfassungsarbeiten über die Überwachung des Betriebszustandes von Datenverarbeitungsanlagen, der Fehleranalyse und -bereinigung außerhalb der üblichen Arbeitszeiten oder während eines bedienerlosen Betriebs, bis hin zu sachbearbeitender Tätigkeit.

Soweit die Einrichtung von Telearbeitsplätzen auch für den öffentlichen Bereich vorgesehen ist, ergeben sich aufgrund des privaten Umfeldes solcher Arbeitsplätze und der im Vergleich zur gewohnten Büroumgebung andersartigen und teilweise höheren Risiken Fragen nach der Gewährleistung eines ausreichenden technisch-organisatorischen Datenschutzes.

Der LfD Rheinland-Pfalz hat sich daher bereits im Jahre 1993 mit einer Umfrage an 13 Rechenzentren in Rheinland-Pfalz gewandt und um Mitteilung gebeten, in welchem Umfang dort Telearbeitsplätze vorgesehen bzw. eingerichtet sind. Im Ergebnis wurden zwar in verschiedenen Fällen entsprechende Überlegungen angestellt, eingerichtete Telearbeitsplätze waren in diesem Bereich jedoch nicht zu verzeichnen. Neben offenen Fragen in personalwirtschaftlicher, haftungs- und versicherungsrechtlicher Hinsicht waren nach Aussage einiger Rechenzentren auch Sicherheitsüberlegungen dafür ausschlaggebend, die Planungen zurückzustellen.

Angesichts der Entwicklungen im Bereich der Informations- und Kommunikationstechnik ist nach Ansicht des LfD Rheinland-Pfalz jedoch davon auszugehen, daß die Einrichtung von Telearbeitsplätzen über die bisherigen Ansätze hinaus künftig auch im öffentlichen Bereich Bedeutung erlangen wird. Soweit sichergestellt ist, daß dabei kein kontrollfreier Raum entsteht und wirksame technisch-organisatorische Sicherungsmaßnahmen ergriffen werden (vgl. Tz. 21.5 und Tz. 21.6), stehen datenschutzrechtliche Gesichtspunkte dem nicht entgegen.

17.6 Mitbestimmung bei Nebentätigkeitsgenehmigungen

Eine Dienststelle hatte aus datenschutzrechtlicher Sicht Bedenken gegen die Regelung des § 79 Abs. 2 LPersVG, wonach der Personalrat bei der Genehmigung von Nebentätigkeiten im Einzelfall mitzubestimmen hat. Dieses Mitbestimmungsrecht führe nämlich dazu, daß der Personalrat über alle Details der Nebentätigkeiten der Bediensteten informiert werde. Der LfD hat dazu folgendes ausgeführt:

Für die Bedenken gegen die Beteiligung des Personalrats in Fällen der Genehmigung einer Nebentätigkeit für einen öffentlich Bediensteten habe er aus datenschutzrechtlicher Sicht volles Verständnis. Die Mitbestimmung bei derartigen personellen Einzelmaßnahmen widerspreche wohl auch dem Prinzip, daß sie grundsätzlich ein Mittel der kollektiven Interessenwahrnehmung der Bediensteten sei.

Dieses Prinzip werde allerdings durch das Personalvertretungsgesetz in verschiedenen Zusammenhängen durchbrochen. Der Gesetzeswortlaut sei im vorliegenden Zusammenhang eindeutig: Bei Genehmigungen von Nebentätigkeiten ist der Personalrat einzubeziehen (§ 79 Abs. 2 Nr. 11 LPersVG). Damit enthalte das Personalvertretungsgesetz eine normenklare Regelung, die das informationelle Selbstbestimmungsrecht der betroffenen Bediensteten insoweit einschränke.

Dieses Gesetz gehe dem allgemeinen Datenschutzrecht vor. Es möge in Zweifel gezogen werden können, ob das Gesetz insgesamt verfassungsgemäß sei und insbesondere auch, ob die hier angesprochene Thematik verfassungskonform geregelt sei. Allein zuständig für die Feststellung der Verfassungswidrigkeit eines Gesetzes sei jedoch die Verfassungsgerichtsbarkeit. Bis zu einer entsprechenden Feststellung sei das Gesetz auch mit den im vorliegenden Fall eintretenden Konsequenzen bezüglich der Datenübermittlung an den Personalrat anzuwenden.

17.7 Stammdatenspeicherung bei Personalvertretungen; Weitergabe von Personalstammdaten aus der Personalverwaltung an die Personalvertretung

Ein Personalrat hat den umfassenden Zugriff auf Personalstammdaten seiner Dienststelle gefordert. Der LfD hat hierzu wie folgt Stellung genommen:

Zunächst ist die Frage zu beurteilen, ob und in welchem Umfang der Personalrat auf die dauernde Verfügbarkeit von Grundinformationen über alle Mitarbeiter angewiesen ist, um seine allgemeine Aufgabe der Vermeidung von Konflikten und der Erhaltung des Friedens in der Dienststelle erfüllen zu können. Wenn eine Dienststelle erheblich mehr als einhundert Mitarbeiter umfaßt, könnte es – in besonderen Fällen – durchaus erforderlich sein, zur Erfüllung dieser allgemeinen Aufgaben Informationen über alle Bediensteten ggf. in automatisierter Form zu speichern (insoweit folgt der LfD in vollem Umfang den Ausführungen des Bundesverwaltungsgerichts in seinem Beschluß vom 4. September 1990, NJW 91, 375, 376). Soweit sich die Informationen auf

- Namen,
- Vornamen,
- Abteilungs-/Referatszugehörigkeit sowie
- Besoldungs-/Vergütungs-/Lohngruppe

beschränken, dürften bei solch umfangreichen Personalkörpern diese Informationen beispielsweise erforderlich sein, um die Mitarbeiter durch den Personalrat konkret über bestimmte Aktivitäten informieren zu können. Auf freiwilliger Basis, mit Einwilligung der Beschäftigten, könnten ggf. noch weitere Informationen hinzukommen (etwa Dienstjubiläen, Geburtstage u. ä.).

Der LfD vertritt weiterhin die Auffassung, daß die allgemeinen Aufgaben des Personalrats es nicht rechtfertigen, eine Datei über alle Mitarbeiter mit weiteren Daten wie

- Geburtsjahr,
- Hinweis auf Ausbildung,
- Eintritt in den Vorbereitungsdienst,
- Ernennungsdaten,
- Beurlaubung von bis,
- Ermäßigung der Arbeitszeit,
- Zeitpunkt einer Eingruppierung,
- Zahlung von Zulagen

anzulegen und ständig verfügbar zu halten. Gerade vor dem Hintergrund, daß ein umfassendes Initiativrecht des Personalrats auch in personellen Angelegenheiten durch die Entscheidung des rheinland-pfälzischen Verfassungsgerichtshofs vom 18. April 1994, Az.: VGH N1/93; N2/93) für verfassungswidrig erklärt wurde, bestehen hiergegen Bedenken. Der Personalrat benötigt konkrete, personenbezogene Informationen grundsätzlich nur für die Mitwirkung in konkreten Einzelfällen und darf sie grundsätzlich auch nur insoweit erheben sowie – zeitlich begrenzt – aufbewahren.

In die gleiche Richtung zielt auch die Rechtsprechung des Bundesverwaltungsgerichts über die Information des Personalrats zum Zweck der Überprüfung der Einhaltung gesetzlicher Bestimmungen. In diesem Zusammenhang hat das Bundesverwaltungsgericht zutreffend entschieden, daß der Personalrat nicht von Amts wegen personenbezogene Daten von schwangeren Beschäftigten erhalten darf. Die allgemeine Aufgabe, die Einhaltung gesetzlicher Schutzvorschriften zu überwachen, rechtfertigt die Weitergabe entsprechender Daten durch die Personalverwaltung an den Personalrat nicht (NJW 91, 373).

Eine automatisierte Speicherung der anläßlich konkreter Mitwirkungsmaßnahmen übermittelten Daten durch den Personalrat oder ein entsprechender permanenter Zugriff auf Dateien der Dienststelle durch den Personalrat sind unzulässig. Dies ergibt sich deutlich aus § 72 Abs. 1 LPersVG, der keineswegs nur die doppelte Führung von Informationen durch den Personalrat untersagt, sondern der insoweit grundsätzlich die Erforderlichkeit des dauerhaften Zugriffs durch den Personalrat auf entsprechende Informationen verneint.

Das Ministerium des Innern und für Sport vertritt in diesem Zusammenhang eine teilweise abweichende Auffassung: Es hält auch die Speicherung der oben genannten zusätzlichen Stammdaten für zulässig (Geburtsjahr, Hinweis auf Ausbildung, Eintritt in den Vorbereitungsdienst, Ernennungsdaten, Beurlaubung von bis, Ermäßigung der Arbeitszeit, Zeitpunkt einer Eingruppierung, Zahlung von Zulagen), hat aber darüber hinausgehende Speicherungen ebenfalls für unzulässig erklärt.

17.8 Dienstordnungsverfahren: dienstliche Stellung und Befugnisse des Vorermittlungsführers

Ein Beschwerdeführer, ein Lehrer, ließ anwaltlich folgendes vortragen:

Im Rahmen von Vorermittlungen gem. §§ 26 ff. Dienstordnungsgesetz seien zwei Personalakten, eine Unfallakte sowie ein Vorgang der Bezirksregierung wegen Verhinderung des Schulbesuchs seiner schulpflichtigen Kinder durch den Ermittlungsführer, einen Beamten der Kreisverwaltung, in seinem Dienstordnungsverfahren angefordert und genutzt worden. Gegenstand der Unfallakte sei ein drei Jahre zurückliegender Verkehrsunfall gewesen. Er wandte sich dagegen, daß der Untersuchungsführer im Rahmen seines Dienstordnungsverfahrens Kenntnis von dieser Akte erhalten hatte.

Die Unfallakte war Teil der Personalakten des Beschwerdeführers. Es war zu klären, ob es sich bei der Übersendung der Personalakten an den Vorermittlungsführer um eine Übermittlung im Sinne des Datenschutzrechts gehandelt hat. Dies wäre nur dann der Fall, wenn der Ermittlungsführer „Dritter" i. S. d. § 3 Abs. 4 LDSG wäre, wenn er also eine Stelle „außerhalb der datenverarbeitenden Stelle" wäre. Dies wäre dann nicht der Fall, wenn der Ermittlungsführer als Teil der datenverarbeitenden Stelle anzusehen wäre. Dann wäre die Überlassung der Akten an den Ermittlungsführer keine Übermittlung, sondern eine bloße Nutzung der Personalakten zum Zweck der Personalverwaltung durch die personalverwaltende Stelle selbst.

Das Dienstordnungsverfahren ist Teil der Personalverwaltung; der Ermittlungsführer ist funktional Teil der personalaktenführenden Stelle. In seiner Eigenschaft als Ermittlungsführer ist er dem das DO-Verfahren betreibenden Dienstvorgesetzten – hier dem Regierungspräsidenten – unmittelbar zugeordnet. In dieser Eigenschaft dürfte er keiner Rechts- und Dienstaufsicht seiner eigenen Dienststellenleitung unterliegen. Damit ist er in dieser Funktion auch organisatorisch dem Dienstvorgesetzten des Beamten zugeordnet, gegen den das DO-Verfahren betrieben wird. Dann aber ist nicht zu prüfen, ob eine Übermittlung zulässig war, sondern es ist nur zu beurteilen, ob die hier erfolgte Nutzung der Personalakten, insbesondere auch der Unfallakte, zulässig war.

Verfassungsrechtlich ergab sich auch schon vor Erlaß des neuen LDSG, daß Datennutzungen ohne Zweckänderung durch die datenverarbeitende Stelle grundsätzlich keinen Grundrechtsbezug haben und zulässig sind. Aufsichtliche Zwecke – wozu letztlich disziplinarische Zwecke gehören – begründen keine Zweckänderung. Dies folgt nunmehr aus einer ausdrücklichen Regelung im novellierten LDSG (§ 13 Abs. 3 S. 1 LDSG).

Vor diesem Hintergrund kommt der strenge Erforderlichkeitsgrundsatz nicht zum Tragen. Die Nutzung der Personalteilakte „Unfallakte" wäre dennoch nur dann zulässig gewesen, wenn sie dem Zweck des DO-Verfahrens gedient haben konnte, wenn sie zweckdienlich war. Nur dann liegt eine Nutzung zum Zweck der Personalverwaltung und Personalwirtschaft vor (dies ist der Zweck, dem die Personalakten insgesamt dienen). Wenn die Unfallakte unter keinem denkbaren Gesichtspunkt für den Ermittlungsführer von sachlichem Interesse hätte sein können, wäre ihre Nutzung unzulässig gewesen. Davon kann jedoch nicht ausgegangen werden: Der Ermittlungsführer hat sich ein möglichst vollständiges Bild über die persönlichen und dienstlichen Verhältnisse des Beamten zu verschaffen; dabei sind nicht nur Umstände von Bedeutung, die den konkreten Vorwurf betreffen (vgl. Claussen/Benneke, RdNr. 94 in der Monographie „Das nichtförmliche Disziplinarverfahren", 2. Auflage Köln 1991). Auch aus dem Inhalt einer solchen Teilakte (etwa dem Schriftwechsel des Beamten mit seiner Behörde) lassen sich u. U. Persönlichkeitsmerkmale entnehmen, die für eine Beurteilung des konkreten Vorwurfs, der Gegenstand des Verfahrens ist, zumindest nützlich sein können. Dies gilt insbesondere dann, wenn – wie hier – ein außerdienstliches Verhalten des Beamten Gegenstand der dienstordnungsrechtlichen Prüfung ist.

Die Beweiserhebungsregelung des § 21 Dienstordnungsgesetz war nicht anzuwenden. Bei der Einsichtnahme in die Personalakten handelt es sich nicht um eine förmliche Beweiserhebungsmaßnahme, sondern um eine vorbereitende Handlung im Rahmen der Durchführung eines Ermittlungsverfahrens (vgl. Claussen/Benneke, a. a. O., wo die Beiziehung der Personalakte und deren Auswertung unter der Überschrift „d) Vorbereitung" abgehandelt werden).

Ein Anlaß, die hier erfolgte Aktenbeiziehung und ihre Auswertung durch den Ermittlungsführer aus datenschutzrechtlicher Sicht zu beanstanden, lag damit nicht vor.

17.9 Einsichtsrecht des Landesrechnungshofs in Personalakten der Landeszentrale für private Rundfunkveranstalter (LPR)

Der LfD wurde von der Staatskanzlei um Stellungnahme zu der Frage gebeten, ob und in welchem Umfang der Landesrechnungshof Einsicht in die Personalakten der LPR nehmen dürfe. Diesem Ersuchen war eine öffentliche Kontroverse zwischen LPR und Landesrechnungshof vorausgegangen.

Der LfD hatte zunächst darauf hinzuweisen, daß seine Zuständigkeit gegenüber dem Landesrechnungshof auf Kontrollen im Bereich der Verwaltung (und auf entsprechende inhaltliche Beurteilungen konkreter Einzelfälle) beschränkt ist (§ 24 Abs. 2 LDSG). Vorliegend handelte es sich um die Frage der Zulässigkeit einer Prüfungsmaßnahme, deren konkrete Bewertung die unabhängige Stellung des Rechnungshofes tangieren würde (vgl. Hockenbrink, DÖV 91, 50). Zu dem in Rede stehenden Problembereich konnte der LfD also nur in allgemeiner Form Stellung nehmen.

Die Frage, ob, in welchem Umfang und unter welchen besonderen Bedingungen die Rechnungshöfe Einsicht in Personalakten geprüfter Stellen nehmen können, ist seit langem Gegenstand der Erörterungen zwischen den Datenschutzbeauftragten, den Rechnungshöfen und den geprüften Stellen.

Bereits im Jahr 1980 hat der Bundesbeauftragte für den Datenschutz hierzu folgendes ausgeführt:

„Der verfassungsmäßige Auftrag des Bundesrechnungshofes ist in Artikel 114 Abs. 2 GG beschrieben und wird durch den V. Teil der BHO, insbesondere § 89 (Prüfung) und § 90 (Inhalt der Prüfung), konkretisiert. Zur Auskunftspflicht der Behörden gegenüber dem Bundesrechnungshof und seinen Beauftragten schreibt § 95 Abs. 1 BHO allgemein vor, daß auf Verlangen des Bundesrechnungshofes die zur Erfüllung seiner Aufgaben von ihm für erforderlich gehaltenen Unterlagen vorzulegen sind. Ob Unterlagen für die Erfüllung seiner Aufgaben erforderlich sind, kann allein der Bundesrechnungshof verbindlich feststellen. Dabei ist er allerdings an den Aufgabenbegriff des Artikels 114 GG und der §§ 88 ff. BHO sowie an den Verhältnismäßigkeitsgrundsatz gebunden. Der Bundesrechnungshof wird also zu berücksichtigen haben, daß es sich bei dem Personalaktengeheimnis um ein besonderes Amtsgeheimnis im Sinne der §§ 10 Abs. 1 Satz 2, 11 Satz 2, 24 Abs. 1, 45 Satz 2 Nr. 1 BDSG handelt. Sein Schutz geht noch über den durch die Vorschriften über das Amtsgeheimnis – § 61 BBG, § 39 BRRG – gezogenen Rahmen hinaus. Das Bundesverwaltungsgericht hat entschieden, daß Personalakten, was auch in der Verwaltungspraxis allgemein anerkannt sei und durch zahlreiche Regelungen bestätigt werde, ohne Einwilligung des Beamten grundsätzlich nur von einem eng begrenzten Personenkreis mit besonderer dienstlicher Verantwortung (Personalreferent, Behördenleiter) eingesehen werden dürften. Sie genössen sowohl im dienstlichen Interesse als auch im schutzwürdigen persönlich-privaten Interesse des Beamten einen besonderen Vertrauensschutz, der sich auch auf den Verkehr der Behörden untereinander erstrecke. Der Bundesrechnungshof wird daher bei der Prüfung der Erforderlichkeit seiner Akteneinsicht die in diesem Bereich gesteigerten Bedürfnisse zur Wahrung schutzwürdiger Belange des Betroffenen beachten und nur dann ein Einsichtsrecht fordern, wenn er seine Aufgabe sonst nicht erfüllen kann."

Zwischenzeitlich sind die seinerzeit vom Bundesbeauftragten für den Datenschutz genannten Gesichtspunkte, die die besondere Schutzbedürftigkeit von Personalakten begründen, durch die Gesetzgebung und durch die Rechtsprechung betont worden:

Das Beamtenrechtsrahmengesetz sowie das Landesbeamtengesetz sind um eine Reihe von Regelungen zum Personalaktendatenschutz ergänzt worden, die zum Ziel haben, Eingriffe in die Persönlichkeitsrechte der Beamten so gering wie möglich zu halten (§§ 56 bis 56 f BRRG; §§ 102 bis 102 g LBG).

Das Bundesverfassungsgericht hat das Grundrecht auf informationelle Selbstbestimmung definiert, das auch im Verhältnis des Beamten zu seiner Dienstbehörde jedenfalls dann Wirksamkeit entfaltet, wenn Personalaktendaten betroffen sind.

In diesem Zusammenhang wird neuerdings die Auffassung vertreten, da in den novellierten Vorschriften des Beamtenrechtsrahmengesetzes über die Führung der Personalakten keine Regelung über die Übermittlung von Personalakten an Rechnungshöfe vorhanden sei, fehle es derzeit an einer ausreichenden, den Grundsätzen der Normenklarheit, Zweckbindung und Verhältnismäßigkeit entsprechenden Rechtsgrundlage für die Übermittlung von Personalaktendaten an die Rechnungshöfe. Die Haushaltsordnungen würden mit ihren Regelungen (§ 95 BHO, § 95 LHO) keine ausreichende Rechtsgrundlage mehr bieten.

Diese Auffassung teilt der LfD nicht, auch wenn er für eine künftige gesetzliche Konkretisierung von § 95 LHO insbesondere in bezug auf Personalakten eintritt: Die Übermittlungsvorschriften der Beamtengesetze enthalten keine abschließende Regelung. Die Übermittlung an den Bundesrechnungshof wird in der Gesetzesbegründung ausdrücklich erwähnt. Demzufolge sind für den hier in Rede stehenden Sachverhalt § 95 der LHO sowie die allgemeine Regelung des LDSG über die Zweckeinheit von Aufsichtszweck und ursprünglichem Datenerhebungszweck (§ 13 Abs. 3) heranzuziehen.

Für Arbeiter und Angestellte verweist § 31 Abs. 1 LDSG ausdrücklich darauf, daß Personaldatenübermittlungen dann erfolgen dürfen, wenn eine andere Rechtsvorschrift dies erlaube.

Aus dem Grundsatz der Verhältnismäßigkeit resultieren jedoch allgemein folgende Beschränkungen für Personalakten:

- Der Wortlaut des § 95 Abs. 1 LHO stellt ausdrücklich die Übersendung mit der Vorlage gleich. Bei Personalakten folgt allerdings aus dem Grundsatz der Verhältnismäßigkeit nach Auffassung des LfD, daß hier die Einsichtnahme in den Räumlichkeiten der geprüften Stelle grundsätzlich Vorrang hat. Dies kann jedoch nicht ausnahmslos gelten. Unter besonderen Bedingungen ist ein Abweichen vom Grundsatz der Einsichtnahme in Personalakten bei der personalaktenführenden Stelle aus datenschutzrechtlicher Sicht gerechtfertigt.

- Der Grundsatz der Verhältnismäßigkeit gebietet es auch, bei einem größeren Personalaktenbestand eine angemessene Auswahl der zur Einsicht bzw. zur Übersendung zur Verfügung zu stellenden Personalakten zu treffen. Die Vorlage aller Personalakten wäre aus der Sicht des LfD jedenfalls dann, wenn keine Anhaltspunkte für konkrete Unregelmäßigkeiten vorliegen, unverhältnismäßig.

- Erforderlich kann nur die Vorlage von Vorgängen sein, bei denen ausgabenrelevante Auswirkungen bestehen können. Ausgabenrelevant in diesem Zusammenhang sind insbesondere Fragen der Einstufung der Mitarbeiter, der Zahlung von Zulagen (z. B. Leistungszulagen) sowie die Ausübung von Nebentätigkeiten.

  Soweit Vorgänge vorhanden sind, die unter keinem Aspekt ausgabenrelevant und überprüfungsfähig sind, besteht grundsätzlich kein Anspruch auf Übersendung und auch kein Einsichtsrecht des Landesrechnungshofs. Ihm obliegt allerdings die Beurteilung, ob es solche Vorgänge gibt und ggf. wie diese einzugrenzen sind.

- Die Fertigung von Kopien in diesem Zusammenhang stellt einen zusätzlichen Eingriff in die Rechte der betroffenen Bediensteten dar, da damit nicht nur Informationen an den Rechnungshof übermittelt, sondern weil damit Personalaktendaten beim Rechnungshof auch gespeichert werden. Damit entstehen – wenn auch möglicherweise in sehr unbedeutendem Umfang – jedenfalls ihrem Inhalt nach sogenannte „Nebenakten" zu den Personalakten beim Landesrechnungshof.

  Die Anlage solcher Nebenakten ist nach dem LBG dann zulässig, wenn sie zur Aufgabenerfüllung erforderlich (im Sinne von unabdingbar) ist (§ 102 Abs. 2 S. 2 LBG). Soweit sich die Fertigung von Kopien darauf bezieht, prüfungsrelevante Feststellungen im Einzelfall nachweisen zu können, ist dies auch in diesem Sinne erforderlich. Auch diese Beurteilung obliegt dem Rechnungshof selbst. Es ist aus datenschutzrechtlicher Sicht nicht unabdingbar, daß solche Kopien nur durch die personalaktenführende Stelle und nicht durch den Rechnungshof gefertigt werden dürften. Allerdings ergibt sich aus der Anforderung des – zumindest analog heranzuziehenden – § 102 Abs. 2 S. 3 LBG, wonach zum Schutz des Bediensteten und zur Wahrung seines Informationsanspruches in jeder Personalakte ein vollständiges Verzeichnis aller Teil- und Nebenakten vorhanden sein muß, daß in der Personalakte zu vermerken ist, wo mit welchem Inhalt Auszüge aus der Personalgrundakte aufbewahrt werden. Der geprüften Stelle ist also zum Zweck der Aufnahme in die Personalakte mitzuteilen, welche Seiten kopiert und beim Rechnungshof aufbewahrt werden. Von der Vernichtung dieser Kopien ist sie ebenfalls zu unterrichten.

- Aus datenschutzrechtlicher Sicht hat die Frage, ob bei der Einsichtnahme in Personalakten Bedienstete der geprüften Stelle anwesend sein sollen oder dürfen, nur sehr untergeordnete Bedeutung. Dem Rechnungshof wird jedenfalls aus datenschutzrechtlicher Sicht nicht abverlangt werden können, seine Prüfung von der Anwesenheit eines Bediensteten abhängig zu machen bzw. bei der Gestaltung seines Prüfungsablaufs darauf in irgendeiner Form Rücksicht zu nehmen.

Wenn die dargelegten Voraussetzungen vorliegen, besteht eine Pflicht der geprüften öffentlichen Stelle, die Personalakten dem Landesrechnungshof vorzulegen bzw. zu übersenden. Die geprüfte Stelle dürfte nur dann die Vorlage verweigern, wenn sie deutliche Anhaltspunkte dafür hat, daß die genannten Rechtmäßigkeitsvoraussetzungen des Handelns des Rechnungshofes nicht vorliegen. Die LPR war also nicht grundsätzlich aus datenschutzrechtlichen Gründen an einer Übermittlung von Personalakten an den Landesrechnungshof gehindert.

17.10 Nutzung von Personaldaten für Werbezwecke

Ein Personalrat hat den LfD auf folgenden Vorgang aufmerksam gemacht:

Die Verwaltung der betroffenen Hochschule habe einer gemeinnützigen Fördervereinigung Aufkleber mit Namen von Bediensteten (ab einer bestimmten Besoldungsgruppe) und deren dienstlicher Anschrift zur Verfügung gestellt.

Zur Begründung der Übermittlung hat die Verwaltung darauf verwiesen, daß die Namen und Adressen aller wissenschaftlichen Mitarbeiter und Mitarbeiterinnen im Personen- und Vorlesungsverzeichnis der Universität enthalten und somit jedermann zugänglich seien.

Der Personalrat hat demgegenüber darauf hingewiesen, es seien nicht nur Namen und Dienststellen von Personen übermittelt worden, die auch im Vorlesungsverzeichnis aufgeführt seien.

Datenschutzrechtlich ist die Angelegenheit unter der Geltung von §§ 102 ff. LBG, § 31 LDSG wie folgt zu beurteilen:

Bei einer Beschränkung der Übermittlungen auf diejenigen Personendaten, die dem Vorlesungsverzeichnis zu entnehmen waren, hätten aus der Sicht des LfD keine Bedenken gegen die erfolgte Übermittlung bestanden. Soweit allerdings andere Bedienstete von der Übermittlung betroffen waren, ist von der Unzulässigkeit der Übermittlung auszugehen: Hier wäre die Übermittlung nur aufgrund der informierten schriftlichen Einwilligung zulässig gewesen.

17.11 Nutzung von Bewerberdaten zu Werbezwecken durch einen Bediensteten

In einer Eingabe wurde folgender Vorgang geschildert:

Der Beschwerdeführer hatte sich als Beamter des mittleren Dienstes beworben. Wenige Tage nach seinem Vorstellungsgespräch habe sich ein Amtsinspektor bei ihm telefonisch gemeldet, um einen Termin für ein „wichtiges Gespräch" zu vereinbaren. Etwa eine Woche nach dem Eignungstest sei dieser Amtsinspektor dann bei dem Beschwerdeführer erschienen. Er habe sich als Ausbilder für den Beamtennachwuchs vorgestellt. Danach habe er ein Verkaufsgespräch für Versicherungen eingeleitet. Er habe auf die Notwendigkeit einer privaten Krankenversicherung hingewiesen und die Vorteile geschildert, die es habe, bei jemanden abzuschließen, mit dem man während der Ausbildung in engerem Kontakt stehe. Er habe auch auf die Möglichkeit verwiesen, daß der Beschwerdeführer selbst ihm als Auszubildender zugeteilt werden könnte. In diesem Zusammenhang habe er auch gesagt, daß er eine Einstellung zwar nicht zusagen könne, der Beschwerdeführer sich aber um eine Ablehnung keine Gedanken machen müsse. Dies habe in dem Betroffenen den Eindruck erweckt, daß eine etwaige Einstellung mit dem Abschluß einer Versicherung in Verbindung stehen könne, zumal der Amtsinspektor beim Einstellungsgespräch zugegen gewesen sei. Daraufhin habe er eine Kranken- sowie eine Lebensversicherung abgeschlossen.

Nach seiner Einstellung, während der Ausbildung habe der Beschwerdeführer erfahren, daß der Beamte mit der gleichen Vorgehensweise auch Versicherungsabschlüsse bei Kollegen vermittelt hätte. Er habe während der Ausbildung nicht gewagt, dieses Verhalten zu kritisieren.

Das zuständige Ministerium hat hierzu folgendes ausgeführt:

Bei der betroffenen Versicherung handele es sich um eine Selbsthilfeeinrichtung der Beamten. Die Tätigkeit hierfür unterliege keiner beamtenrechtlichen Nebentätigkeitsgenehmigung. Der Amtsinspektor habe sich die Daten der neu eingestellten Beamten nicht aus den Bewerberunterlagen verschafft, da den Sachbearbeitern der Personalabteilung eine entsprechende Weitergabe untersagt sei. Der Amtsinspektor habe zwischenzeitlich seine Tätigkeit als Vertrauensmann für die Versicherung eingestellt. Es habe sich nicht bestätigen lassen, daß er seine Vorgesetzten- bzw. Ausbilderfunktion bei den Versicherungsberatungen „ausgespielt" habe.

Dieser lapidaren Stellungnahme hat der LfD entnommen, daß der Sachverhalt dem Grunde nach nicht in Abrede gestellt wird. Der Amtsinspektor hatte seit ungefähr 20 Jahren eine solche Nebenbeschäftigung als Vertrauensmann ausgeübt. Die Namen der Bewerber hat er bei Gelegenheit des Bewerberauswahlverfahrens erfahren.

Aus datenschutzrechtlicher Sicht hat der LfD den Vorgang wie folgt bewertet:

In der Nutzung von Informationen, die ein öffentlich Bediensteter in Ausübung seiner dienstlichen Tätigkeit im Bewerbungsverfahren erfahren hat, zu außerdienstlichen Zwecken liegt grundsätzlich eine zweckwidrige Verwendung. Diese ist grundsätzlich unzulässig.

Die erfolgte Nutzung von Bewerberdaten zu Werbezwecken für eine im Wettbewerb stehende Versicherung war deshalb aus der Sicht des LfD datenschutzrechtlich unzulässig. Er hat das zuständige Ministerium hierauf hingewiesen.

17.12 Das Landesgleichstellungsgesetz

Der LfD hat intensiv an den Beratungen, die zum Erlaß des Landesgleichstellungsgesetzes geführt haben, teilgenommen. Aus datenschutzrechtlicher Sicht waren zwei unterschiedliche Problembereiche bedeutsam, die vom Gesetzgeber zu entscheiden waren:

Zum einen war zu klären, in welchem Umfang die nach dem Gesetz vorgesehene Gleichstellungsbeauftragte personenbezogene Informationen über die Bediensteten durch die Dienststelle erhalten und insbesondere, ob und in welchem Umfang sowie unter welchen Voraussetzungen der Gleichstellungsbeauftragten Einsicht in Personalakten sowie in sonstige personenbezogene Unterlagen gewährt werden sollte.

Zum anderen war zu prüfen, welche Regelungen für die weitere Aufbewahrung und Nutzung personenbezogener Informationen durch die Gleichstellungsbeauftragten gelten, ggf. ob diese Regelungen bereichsspezifisch ergänzt werden sollten.

In diesem Zusammenhang hat der LfD konkrete Formulierungsvorschläge vorgelegt. Er hat klarstellende Regelungen dahin gehend erreicht, daß eine Einsicht der Gleichstellungsbeauftragten in die Personalakten der Betroffenen grundsätzlich nicht zulässig ist. Sie ist vielmehr nur auf der Basis einer ausdrücklich erklärten Einwilligung der Betroffenen vorgesehen.

Soweit bei Personalentscheidungen nur männliche oder nur weibliche Bewerber zur Auswahl stehen, entfallen die Informationsrechte der Gleichstellungsbeauftragten.

Eine Vorlage von Unterlagen erfolgt nur bezüglich derjenigen Bewerberinnen und Bewerber, die von der Dienststellenleitung in die engere Auswahl gezogen wurden (§ 18 Abs. 3 Landesgleichstellungsgesetz).

Bezüglich der Aufbewahrung der personenbezogenen Unterlagen bei der Gleichstellungsbeauftragten regelt das Gesetz, daß diese Unterlagen nach Abschluß der Beteiligung grundsätzlich zurückzugeben sind. Ihre Sammlung, fortlaufende aktenmäßige Auswertung sowie Speicherungen in Dateien ist unzulässig. Unterlagen, die personenbezogene Daten enthalten, sind vor unbefugter Einsichtnahme zu schützen. Für die Einhaltung der Vorschriften über den Datenschutz durch die Gleichstellungsbeauftragte ist die Dienststelle zuständig (§ 18 Abs. 8 Landesgleichstellungsgesetz).

Mit diesen Regelungen ist den datenschutzrechtlichen Vorstellungen des LfD weitgehend entsprochen worden. Er geht davon aus, daß auf der Basis dieser klaren gesetzlichen Regelungen in der Praxis die auftretenden Fragen schnell und sicher gelöst werden können.

18. Datenschutz im kommunalen Bereich

18.1 Tonaufzeichnungen in Ratssitzungen

Die vom Ministerium des Innern und für Sport herausgegebene Mustergeschäftsordnung für kommunale Vertretungskörperschaften enthält in § 26 Regelungen über die Fertigung von Tonaufzeichnungen in Ratssitzungen. Es ist bestimmt, daß der Schriftführer als Hilfsmittel zur Vorbereitung der Niederschrift den Sitzungsverlauf mit Tonband aufzeichnen darf; bei nichtöffentlichen Sitzungen ist hierfür ein Ratsbeschluß erforderlich. Auch die Aufbewahrung von Tonaufzeichnungen für archivarische Zwecke ist nur mit ausdrücklicher Billigung des Rats zulässig. Die Aufbewahrung der Tonaufzeichnungen einer nichtöffentlichen Sitzung für Archivzwecke ist nur zulässig, wenn alle Ratsmitglieder, die das Wort ergriffen haben, zustimmen.

Ein Ratsmitglied hielt die Bestimmungen der Mustergeschäftsordnung, soweit die Ratsmehrheit gegen den Willen der Minderheit die Anfertigung oder Aufbewahrung von Tonaufzeichnungen beschließen kann, für unvereinbar mit dem Recht auf informationelle Selbstbestimmung und erbat eine Stellungnahme des LfD.

Tonträger fallen nach § 3 Abs. 6 LDSG unter den Aktenbegriff und damit unter die einschlägigen datenschutzrechtlichen Bestimmungen. Zu berücksichtigen ist indessen, daß die einschlägigen Bestimmungen der Mustergeschäftsordnung die Aufzeichnung der Äußerungen von Ratsmitgliedern in Ratssitzungen betreffen. Dies ist für die Beurteilung der Frage von Bedeutung, ob und inwieweit hierdurch das Recht auf informationelle Selbstbestimmung von Ratsmitgliedern beeinträchtigt sein könnte.

Das Bundesverwaltungsgericht hat in einer Entscheidung vom 3. August 1990 – 7 C 14/90 – (NJW 1991, 118), die die Untersagung des Mitschnitts der öffentlichen Gemeinderatssitzung durch Pressevertreter betrifft, festgestellt, daß das allgemeine Persönlichkeitsrecht der Ratsmitglieder im Rahmen der Entscheidung über die Zulassung des Mitschnitts durch den Ratsvorsitzenden nicht von tragender Bedeutung ist. Es hat damit deutlich gemacht, daß sich Mandatsträger in Ausübung ihres Amtes nur sehr eingeschränkt auf das Recht auf informationelle Selbstbestimmung berufen können. Die rechtliche Stellung des Ratsmitglieds bei der Mandatsausübung ist also nicht vergleichbar mit der des Bürgers, dem das informationelle Selbstbestimmungsrecht als Abwehrrecht gegen den Staat zusteht. Das Ratsmitglied ist bei der Mandatsausübung selbst „Staat"; Abwehrrechte stehen ihm nur insoweit zu, als es beispielsweise durch Äußerungen, die den privaten Bereich der Lebensführung betreffen oder durch Beleidigungen usw. in seinen schutzwürdigen Belangen beeinträchtigt wird.

Diese grundsätzlichen Überlegungen bilden den Hintergrund für die Beurteilung der Frage, ob eine Befugnis besteht, Daten durch Fertigung von Tonaufzeichnungen in Ratssitzungen zu erheben. Nach § 12 Abs. 1 LDSG ist die Datenerhebung zulässig, wenn ihre Kenntnis zur rechtmäßigen Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Diese Voraussetzungen dürften jedenfalls dann vorliegen, wenn Tonaufzeichnungen zum Zwecke der Protokollierung gefertigt werden, und zwar unabhängig davon, ob dies in öffentlichen oder nichtöffentlichen Sitzungen geschieht. Zu berücksichtigen ist, daß die erhobenen Daten einer grundsätzlichen Zweckbindung unterliegen.

Aber auch die Regelungen über die Aufbewahrung von Tonaufzeichnungen für archivarische Zwecke (§ 26 Abs. 7) und über die Vornahme von Tonaufzeichnungen durch andere Personen (§ 26 Abs. 8) begegnen im Blick auf die obigen Ausführungen zu den Persönlichkeitsrechten von Mandatsträgern keinen datenschutzrechtlichen Bedenken.

18.2 Zusammenarbeit der Handwerkskammern mit Mandatsträgern in den Gemeinderäten

Eine Handwerkskammer fragte an, ob die Gemeindeverwaltungen befugt sind, die folgenden Angaben über Mandatsträger in Gemeinderäten zur Verfügung zu stellen: Name und Anschrift, Parteizugehörigkeit, Berufsangabe, Angabe, ob selbständig oder nicht selbständig. Diese Angaben sollten dazu dienen, statistische Aussagen über die Repräsentanz des Handwerks in den Gemeinderäten zu gewinnen und – zu diesem Zweck waren Name und Anschrift erforderlich – die Mandatsträger an der Arbeit der Handwerkskammern zu beteiligen und sie über handwerkspolitische Themen zu unterrichten.

Der LfD beurteilte die Zulässigkeit der Datenübermittlung wie folgt:

Nach § 14 LDSG ist die Übermittlung personenbezogener Daten an öffentliche Stellen zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden oder der empfangenden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 12 Abs. 4 oder § 13 Abs. 2 Nr. 2 oder 3 zulassen würden. § 12 Abs. 4 Nr. 9 betrifft Daten, die unmittelbar aus allgemein zugänglichen Quellen entnommen werden können oder die von der datenverarbeitenden Stelle veröffentlicht werden dürfen.

Von der Erforderlichkeit der Daten zur rechtmäßigen Aufgabenerfüllung ist auszugehen. Veröffentlicht im Sinne des § 12 Abs. 4 Nr. 9 LDSG sind nach den Vorschriften des Kommunalwahlgesetzes in Verbindung mit der Kommunalwahlordnung Familiennamen, Vornamen, Geburtstag, Beruf oder Stand und Anschrift der Bewerber sowie deren Zugehörigkeit zu einer Partei und Wählergruppe und, nach Feststellung des Wahlergebnisses, Familiennamen und Vornamen der Gewählten, wiederum in Verbindung mit der Zugehörigkeit zu einer Partei oder Wählergruppe (§ 30 Abs. 1 i. V. m. § 25 Abs. 1 Satz 2 und § 65 Abs. 2 Kommunalwahlordnung).

Im Ergebnis war also gegen die Übermittlung der Daten nichts einzuwenden.

18.3 Weitergabe der Tagesordnung des Kreisrechtsausschusses an die örtliche Presse

Bei einer Kreisverwaltung war es üblich, daß die Tagesordnungen öffentlicher Sitzungen des Kreisrechtsausschusses der örtlichen Presse zur weiteren Verwendung mitgeteilt wurden. Die Vermutung, daß diese Praxis unter datenschutzrechtlichen Gesichtspunkten bedenklich sein könnte, führte zu einer Anfrage an den LfD.

Dieser äußerte sich wie folgt: Verwaltungsverfahren unterliegen grundsätzlich der Geheimhaltung nach § 30 VwVfG. Ausnahmen von diesem Grundsatz bedürfen einer normenklaren gesetzlichen Grundlage (BVerfGE 65,1). § 16 Abs. 1 AGVwGO statuiert eine Ausnahme für Vorverfahren vor den Rechtsausschüssen. Nach dieser Bestimmung sind die Verhandlungen öffentlich. Zugleich ist geregelt, daß die Öffentlichkeit aus wichtigem Grund ausgeschlossen werden kann. Als Ausnahmeregelung zu dem das gesamte Verwaltungsverfahrensrecht prägenden Grundsatz der Geheimhaltung ist die zitierte Vorschrift eng auszulegen. Eine Auslegung, die Vorbereitungshandlungen, wie Einladungen zu Sitzungen der Rechtsausschüsse, oder nachfolgende Informationsvorgänge, wie die Mitteilung des Ergebnisses an die Öffentlichkeit, als Teil der „Verhandlung" ansieht, kommt nicht in Betracht.

Derartige Offenbarungen können auch nicht damit gerechtfertigt werden, daß Informationen in einer öffentlichen Verhandlung erörtert werden sollen bzw. erörtert worden sind. Auch das Öffentlichkeitsprinzip ist im Lichte der o. a. Entscheidung des Bundesverfassungsgerichts zur Reichweite des informationellen Selbstbestimmungsrechts zu sehen. Danach ist grundsätzlich davon auszugehen, daß der Bürger selbst bestimmen darf, welche anderen Personen oder Stellen in die Lage versetzt werden, Informationen über ihn zur Kenntnis zu nehmen. Nur im überwiegenden Allgemeininteresse und aufgrund eines normenklaren Gesetzes sind Ausnahmen zulässig. Nur soweit die Durchführung einer öffentlichen Verhandlung Übermittlungen erfordert, dürfen diese also auch erfolgen. Eine vergleichbare Situation liegt im Bereich der Rechtsprechung vor, wo es unstreitig ist, daß der Akteninhalt, aber auch sonstige Informationen über das Verfahren nur im Rahmen von gesetzlichen Regelungen an Dritte übermittelt werden dürfen, auch wenn diese Informationen in einem öffentlichen Verfahren erörtert wurden oder künftig erörtert werden. Im Bereich von Widerspruchsverfahren kann keine andere Wertung Platz greifen.

Selbstverständlich sind gegen die Bekanntgabe des Verhandlungstermins und der zu erörternden Tagesordnungspunkte – ohne die Namen und Anschriften Betroffener – an die Presse keine Bedenken zu erheben.

Zum Ausschluß der Öffentlichkeit aus wichtigem Grund hat sich die Datenschutzkommission in ihrem 9. Tätigkeitsbericht (Tz. 10.1.4) wie folgt geäußert: „Das die Verhandlungen der Rechtsausschüsse bestimmende Öffentlichkeitsprinzip kollidiert mit dem Anspruch des Betroffenen auf Wahrung des Sozialgeheimnisses. Während das Sozialgeheimnis allerdings Ausfluß der grundgesetzlich geschützten Persönlichkeitssphäre ist, ist das Öffentlichkeitsprinzip des verwaltungsbehördlichen Vorverfahrens – anders als im Gerichtsverfahren – in § 16 AGVwGO lediglich durch einfaches Gesetz angeordnet. Der daraus abzuleitende Vorrang des Persönlichkeitsschutzes führt daher nach Auffassung der DSK notwendigerweise zum Ausschluß der Öffentlichkeit, wenn der Rechtsausschuß über Sozialleistungsangelegenheiten verhandelt."

Gleiche Überlegungen greifen auch dann Platz, wenn andere durch Berufsgeheimnisse oder besondere Amtsgeheimnisse – z. B. Steuergeheimnis, Statistikgeheimnis – geschützte Vorgänge in Rechtsausschüssen behandelt werden.

18.4 Aktenweitergabe an die nach dem Waffengesetz zuständige Erlaubnisbehörde

Das Ordnungsamt einer rheinland-pfälzischen Stadt hatte einen Antrag auf Erteilung einer Waffenbesitzkarte im Jahr 1991 wegen Unzuverlässigkeit des Antragstellers abgelehnt. Bei einer routinemäßigen Überprüfung von Anschriften brachte es 1993 in Erfahrung, daß der Betroffene 1992 in eine Stadt in Norddeutschland verzogen war. Es übersandte daraufhin unaufgefordert die vollständige Akte an das Ordnungsamt dieser Stadt. Dieses Verfahren – so das Ordnungsamt – entspreche einer allgemeinen Übung; Grundlage der Verfahrensweise sei Nummer 52.2 der Allgemeinen Verwaltungsvorschrift zum Waffengesetz – WaffVwV –.

Diese Aktenübersendung war unzulässig. Nummer 52.2 WaffVwV läßt zwar zu, daß die bisher zuständige Behörde die waffenrechtlichen Unterlagen über Erlaubnisinhaber an die zuständig gewordene Behörde übersendet, wenn sie von dieser angefordert werden oder wenn die bisher zuständige Behörde zuerst Kenntnis von dem Wohnsitzwechsel erhält. Die Versendung von Unterlagen über Personen, deren Antrag abgelehnt wurde, ist in der WaffVwV indessen nicht vorgesehen. Im Falle einer erneuten Beantragung erhält die zuständig gewordene Behörde Kenntnis von der vorangegangenen Ablehnung aufgrund von § 10 i. V. m. § 41 Bundeszentralregistergesetz. Sofern diese die früher zuständige Behörde in Wahrnehmung ihrer Amtsermittlungspflicht um Auskünfte ersucht, ist die Zulässigkeit der Datenübermittlung vor dem Hintergrund anderer Rechtsvorschriften (POG, LDSG) zu prüfen.

Die Übermittlung der aktuellen Anschriften in Ablehnungsfällen durch das Meldeamt an das Ordnungsamt war nach § 31 MG ebenfalls unzulässig, weil sie zur rechtmäßigen Aufgabenerfüllung nicht erforderlich war.

Die zuständigen Behörden erkannten die Rechtsauffassung des LfD an. Die ohne Rechtsgrundlage übermittelten Akten wurden zurückgefordert. Das Ministerium des Innern und für Sport entsprach der Empfehlung des LfD, alle Erlaubnisbehörden in Rheinland-Pfalz auf die genaue Beachtung der Übermittlungsbestimmungen hinzuweisen.

18.5 Datenschutz im Vollstreckungswesen

Eine Kreisverwaltung wollte wissen, ob es zulässig ist, an die Vollstreckungsbeamten der Städte und Verbandsgemeinden für Vollstreckungszwecke Fotokopien von Bußgeldbescheiden zu übermitteln. Der LfD beurteilte diese Rechtsfrage wie folgt:

Nach § 4 Abs. 3 Nr. 3 LVwVGDVO müssen aus dem Vollstreckungsauftrag die beizutreibenden Forderungen nach Grund und Höhe unter Angabe des Gläubigers und des Vollstreckungsschuldners ersichtlich sein. Es ist nicht ganz unumstritten, welche Informationen unter den vom Gesetzgeber verwendeten Begriff „Grund" der beizutreibenden Forderungen zu fassen sind. Mit der Angabe des Gesetzes, gegen das verstoßen wurde, ist der Grund einer Forderung nicht hinreichend deutlich beschrieben. Der Vollstreckungsbeamte muß in die Lage versetzt werden, den Zahlungspflichtigen exakt darüber zu informieren, welche Forderung vollstreckt wird. Es ist deshalb geboten, gegenüber der Vollstreckungsbehörde ergänzend die Rechtsvorschriften zu benennen, auf denen die Bußgeldfestsetzungen beruhen, ferner das Aktenzeichen des Bußgeldbescheids und das Datum des Verstoßes. Die Mitteilung des genauen Schuldvorwurfs kann nur in besonderen Ausnahmefällen in Betracht kommen, wenn beispielsweise in großen Unternehmen anders eine Klärung der Zuständigkeit nicht möglich ist.

Mit der Weitergabe unveränderter Kopien der Bußgeldbescheide würden Daten übermittelt, die zur Aufgabenerfüllung der Vollstreckungsstellen nicht erforderlich sind. Dieses Verfahren ist daher nicht zulässig.

18.6 Kommunale Datenerhebung zu Planungszwecken (§ 32 LDSG);
Umfrage zur Neuorganisation des Schulzweckverbandes

Eine Ortsgemeinde schrieb Einwohner an und fragte, welche Grund- bzw. Haupt- oder Regionalschule sie für ihr Kind bevorzugen würden, wenn eine entsprechende Entscheidung anstünde.

Die befragten Personen sollten ihr Votum unterschreiben und das gesamte Schreiben, auf dessen Vorderseite sich ihre Anschrift befand, an die Ortsgemeinde zurücksenden.

Eine Rechtsnorm, die die Betroffenen zur Angabe der Daten verpflichten würde, oder Rechtsvorteile, deren Gewährung von der Beantwortung der Fragen aufgrund einer gesetzlichen Regelung abhängig wäre, sind nicht ersichtlich. Die Erhebung wäre auch dann ohne ausdrückliche schriftliche Einwilligungserklärung der Betroffenen zulässig gewesen, wenn es sich um die Erhebung von Planungsdaten gehandelt hätte und wenn diese nicht in anonymisierter Form hätten erhoben werden können (§ 32 Abs. 1 LDSG). Es ist aber nicht ersichtlich, wieso die Antworten einzelnen Bürgern zugeordnet sein mußten, wieso es für die Meinungsbildung bzw. politische Willensbildung der Ortsgemeinde erforderlich gewesen wäre zu erfahren, welche namentlich bekannten Bürger für oder gegen einen bestimmten Schulstandort votieren. Eine anonyme Erhebung wäre also völlig aus-

reichend gewesen. Hingegen wäre eine Umfrage mit Angabe des Absenders allenfalls auf der Basis der freiwillig erteilten schriftlichen Einwilligung zulässig gewesen, wobei die Betroffenen ausdrücklich über die Freiwilligkeit sowie über die Rechtsfolgen einer nicht erteilten Einwilligung zu informieren gewesen wären (§ 5 Abs. 2 und 3 LDSG).

Dies ist nicht erfolgt. Die vorstehend dargestellte Erhebung personenbezogener Daten der Bürger der Ortsgemeinde wurde deshalb als datenschutzrechtlich unzulässig beanstandet. Der Ortsbürgermeister wurde aufgefordert, die ausgefüllten Fragebögen unverzüglich zu vernichten.

19. Medien

19.1 Multimedia am Start

Das digitale Medienzeitalter hat bereits begonnen; konzipiert und erprobt werden das digitale Fernsehen mit Video-on-demand und Pay-per-View. Die Zahl der verfügbaren Programmkanäle wird sich wohl auf 500 oder noch mehr vervielfachen. Jeder wird seine „special-interest"-Programme in digitaler Form gegen individuelle Bezahlung beziehen können. Telebanking und Teleshopping gibt es bereits; das Internet wird mehr und mehr genutzt. Fernsehbilder, Stereotöne, Fotos, Telefongespräche, Banküberweisungen oder Informationen aus Datenbanken werden auf dem „Datenhighway" mittels Richtfunkstrecken, Satellitennetzen, Kupfer- oder Glasfaserkabel übertragen.

Während in der Analogtechnik sorgfältig zwischen Rundfunk, Fermelde- und Datendiensten unterschieden wurde, wird diese Unterscheidung bei der Digitaltechnik schwierig. Allein im Internet erkunden weltweit über 30 Millionen Menschen die Multimedia-Angebote, indem sie digitale Texte, Fotos, Filme oder Radiosendungen abrufen. Häufig wird das Internet als Netzwerk von Netzwerken bezeichnet. So verbindet es derzeit weltweit etwa 45 000 eigenständige Teilnetze mit rund vier Millionen Computern, wobei die Zahl der Benutzer von heute 30 Millionen nach vorsichtigen Schätzungen sich bis zur Jahrtausendwende auf 300 Millionen verzehnfachen wird. In Größe und Struktur unterscheidet sich das Internet ganz erheblich von traditionellen Online-Diensten, die aus nur wenigen zentral verwalteten Großrechnern bestehen. Das Internet funktioniert indes ohne übergeordnete „Leitstelle", es hat keinen Betreiber im Sinne eines „Besitzers". Seit September 1995 bietet auch die Telekom AG ihrer Datex-J(BTX)-Gemeinde, wozu auch öffentliche Stellen gehören, per „Mausklick" die Datenreise ins Internet an. Damit wird das Problem der globalen Netzsicherheit dringend.

Auf Datenschutz ist das Internet in seiner jetzigen Form nicht ausgelegt. Die Spuren eines einzelnen Anwenders lassen sich blitzschnell aus dem Datenstrom filtern. Wenn erst einmal per Datenleitung eingekauft und recherchiert, ferngesehen und ärztlicher Rat eingeholt wird, läßt sich das Leben eines „Netzbewohners" fast lückenlos zusammensetzen. Eine wachsende Zahl von Internet-Anwendern bevorzugt die elektronische Post (E-Mail) gegenüber Brief, Fax und Telefon. E-Mail ermöglicht den schnellen Austausch und die papierlose Weiterverarbeitung von digitalen Informationen. Wenigen ist indessen bewußt, daß sie sich solche Vorteile mit hochgradiger Unsicherheit erkaufen. Verschlüsselung bietet den einzig wirksamen Schutz vor Lauschern und Fälschern. Elektronische Post ist also ohne weitere Vorkehrungen eine Art „elektronische Postkarte". Niemand kann sicher sein, daß die empfangene „Postkarte" authentisch ist, also tatsächlich vom vorgeblichen Absender stammt. Noch darf jeder alles im Internet. Das macht es zum Paradies der Meinungsvielfalt, aber auch zum Medium von Geschmacklosigkeit und Fanatismus. Nur am Rande sei erwähnt, daß kürzlich die US-Senatoren James Exon und Dan Coats diesbezüglich im Senat einen Gesetzentwurf zur „Sittlichkeit in der Kommunikation" eingebracht haben.

19.2 Der Rundfunkbegriff im Wandel

Das Recht der elektronischen Medien untersteht der Länderhoheit. Daran ändert sich auch nichts, nachdem die möglichen Betätigungsfelder der privatisierten Telekom AG weit in den Multimedia-Bereich hineinragen werden. Was die verfassungsrechtliche Einordnung angeht, so werden die neuen Dienste aufgrund ihrer Ausgestaltung entweder von Artikel 5 GG oder dem Auffanggrundrecht der allgemeinen Handlungsfreiheit nach Artikel 2 Abs. 1 GG erfaßt.

Im Rahmen des Landesgesetzes zum Zweiten Rundfunkänderungsstaatsvertrag – der die Förderung von Projekten für neuartige Rundfunkübertragungstechniken erlaubt – soll mit der Änderung des Landesrundfunkgesetzes (LRG) die Durchführung von Versuchen mit neuen Techniken, Programmen und Diensten in Rheinland-Pfalz ermöglicht werden. Aus der Begründung zum Gesetzentwurf hinsichtlich der diesbezüglich neu geschaffenen Vorschrift (§ 55 LRG-E) ergibt sich folgendes: Erfaßt werden insbesondere neuartige Rundfunkübertragungstechniken, wie z. B. die digitale Übertragung von Hörfunk und Fernsehen. Ferner können auch neue Programmformen und sonstige Dienste im Rahmen dieser Versuchsbestimmung erprobt werden. Der Versuch kann entweder organisatorisch im Land Rheinland-Pfalz stattfinden oder sich auf die Weiterverbreitung von Programmen und Diensten beschränken, die in anderen Ländern der Bundesrepublik Deutschland im Rahmen von Versuchen rundfunkrechtlich zulässigerweise veranstaltet werden. An den Versuchen können sich die für Rheinland-Pfalz zuständigen öffentlich-rechtlichen Rundfunkanstalten beteiligen. Dabei handelt es sich um den Südwestfunk, das Zweite Deutsche Fernsehen (ZDF) und um die von der Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland (ARD) sowie dem ZDF gemeinsam getragene Körperschaft Deutschlandradio. Schließlich können auch alle Ver-

anstalter an Versuchen teilnehmen, die in Rheinland-Pfalz über eine Erlaubnis zur Veranstaltung von Rundfunk verfügen. Ein Veranstalter, der über keine Erlaubnis in Rheinland-Pfalz verfügt, kann eine Versuchserlaubnis durch die Landeszentrale für private Rundfunkveranstalter (LPR) für die Dauer des Versuchs erhalten. Auch die LPR selbst kann sich an Versuchen beteiligen. Nach § 55 Abs. 4 LRG-E ist das Nähere über die Durchführung und Beteiligung privater Veranstalter am Versuch, das Erlaubnisverfahren sowie die Begleitung und Beobachtung durch die LPR mittels Satzung zu regeln. Aufgrund der unterschiedlichen Ausgestaltung der Versuche ist eine Regelung durch den Gesetzgeber selbst nicht vorgesehen. Die Durchführung von Versuchen ist bis zum 31. Dezember 1998 befristet. Bis zu diesem Zeitpunkt ist nach Auffassung der Landesregierung zu erwarten, daß die erforderlichen Erkenntnisse aus den Versuchen vorliegen, so daß die Programme und Dienste den allgemeinen Regelungen unterworfen werden können. Von dem Ergebnis der Versuche in Rheinland-Pfalz und in anderen Ländern der Bundesrepublik Deutschland wird es abhängen, inwieweit die allgemeinen Regelungen einer Ergänzung oder Änderung bedürfen.

Es wird zunächst abzuklären sein, welche Risiken für das informationelle Selbstbestimmungsrecht aufgrund der Datenflüsse entstehen. Wenn auch die genauen Formen der neuen Medien und ihre konkrete technische und rechtliche Ausgestaltung im einzelnen noch nicht bekannt sind, so kann doch bereits vom Ansatz her festgestellt werden, daß bei der datenschutzrechtlichen Einordnung Unterschiede bestehen, z. B. dahin gehend, ob Datenflüsse lediglich zwischen einzelnen Kommunikationspartnern fließen oder ob „offene" Kommunikation stattfindet. Je nach Art des Dienstes muß geprüft werden, ob das geltende Datenschutzrecht eine geeignete Grundlage bietet oder ob für die neuen Mediendienste spezifische Datenschutzregelungen zu treffen sind.

Hier wird das Bedürfnis nach einer – bislang nicht vorhandenen – „offiziellen" Definition von Multimedia-Dienstleistungen deutlich. Grundsätzlich sind Multimedia-Dienste dadurch gekennzeichnet, daß sie die Verwendung verschiedener Informationsmedien (Text, Bild, Ton) in einem Dienst zusammenfassen und den Benutzern über einen Rückkanal die interaktive Beeinflussung des Dienstes gestatten. Multimedia-Angebote werden dazu führen, daß viel mehr persönliche Daten gespeichert werden als bisher. Es muß darauf geachtet werden, daß der Datenschutz im neuen Multimedia-Datenstrom nicht „untergeht". Wer Multimedia-Dienste nutzt, muß damit rechnen, daß seine personenbezogenen Daten festgehalten werden. Das Verhalten eines Kunden dieser Dienste kann sehr viel stärker registriert werden als bisher üblich und möglich.

Die gegenwärtige Diskussion über Multimedia hat die damit verbundenen Datenschutzprobleme noch kaum zur Kenntnis genommen. Rechtliche und technische Anforderungen und harmonisierende Regelungen sind jedoch dringend geboten, wenn es um Daten des individuellen Medienkonsums geht. Der LfD wird sich diesbezüglich mit der LPR in Verbindung setzen.

Die skizzierte Entwicklung kann nicht ohne Einfluß auf den Rundfunkbegriff bleiben. Gegenwärtig wird unter dem Gesichtspunkt der Vereinheitlichung des Medienrechts von den Rundfunkreferenten der Bundesländer an einer „Negativliste" zum Rundfunkbegriff gearbeitet. Hier stehen eine Reihe von Fragen an, etwa zur Einordnung von Abruf- und Datendiensten im Audio- und Videobereich, Teleshopping oder Telebanking, Pay-per-view oder Video-on-demand. Wenn z. B. ein Medienunternehmer aus seinem Datenspeicher einen Spielfilm gegen Gebühr an einen Kunden per digitaler Telefonleitung überträgt, ist er dann überhaupt noch ein Rundfunkveranstalter oder ist der Vorgang nicht eher mit dem Verkauf einer Video-Kassette vergleichbar? Ein weiteres Problemfeld stellen die elektronischen Zeitungen und Zeitschriften dar, wobei auf elektronischem Weg dieselben Inhalte, wie sie in gedruckter Form vorliegen, verbreitet werden. Es zeigt sich, daß die Grenzen zwischen Fernsehen, Hörfunk und anderen Medien fließend werden.

19.3 Änderung des Rundfunkstaatsvertrages im Hinblick auf Reality-TV

Die Gefahren, die von der neuen Sendeform des Reality-TV für das informationelle Selbstbestimmungsrecht der Betroffenen ausgehen, hat der LfD im 14. Tätigkeitsbericht (Tz. 19.2) beschrieben. Er hat die Auffassung vertreten, daß die Medienfreiheit nicht die Mißachtung der Menschenwürde durch das Zurschaustellen menschlicher Notlagen rechtfertigt und insbesondere das Medienprivileg nicht dazu führen darf, daß die Fernsehveranstalter von der Achtung der Menschenwürde und des Persönlichkeitsrechts faktisch befreit sind. In diesem Zusammenhang hat er darauf hingewiesen, daß eine Einwilligung, die in einer konkreten Notsituation abgegeben wird, regelmäßig bereits wegen der Art und Weise ihres Zustandekommens treuwidrig und das Berufen auf die Einwilligung sittenwidrig ist.

Mit Genugtuung ist festzustellen, daß gerade dieser Aspekt in den Ersten Rundfunkänderungsstaatsvertrag mit Wirkung vom 1. August 1994 Eingang gefunden hat. Nunmehr wird in § 3 Abs. 1 Nr. 5 des geänderten Rundfunkstaatsvertrages bestimmt, daß Sendungen unzulässig sind, wenn sie Menschen, die sterben oder schweren körperlichen oder seelischen Leiden ausgesetzt sind oder waren, in einer die Menschenwürde verletzenden Weise darstellen und ein tatsächliches Geschehen wiedergeben, ohne daß ein überwiegendes berechtigtes Interesse gerade an dieser Form der Berichterstattung vorliegt. Das Ausstrahlungsverbot (Verbreitungsverbot) gilt auch dann, wenn die Betroffenen eingewilligt haben. In der amtlichen Begründung zu der Änderung heißt es: „Insoweit ist der Kernbereich der Menschenwürde ein objektiver, unverfügbarer und unverzichtbarer Wert, den der Staat nicht nur gegen Dritte, sondern sogar gegen den Betroffenen selbst schützen muß. Eine Einwilligung des Betroffenen in den Menschenwürdeverstoß ist daher unbeachtlich." Dem ist nichts hinzuzufügen.

19.4 Gerichtsfernsehen

Selbst mit Einwilligung aller Prozeßbeteiligten darf die unmittelbare Rundfunkberichterstattung aus dem Gerichtssaal nicht zugelassen werden. Diese dringende Mahnung erhoben die Datenschutzbeauftragten des Bundes und der Länder auf ihrer 49. Konferenz in Bremen im Rahmen einer einstimmig gefaßten Entschließung zu den Anforderungen an den Persönlichkeitsschutz im Medienbereich (vgl. Anlage 21). Sie treten damit den in jüngster Zeit zunehmend erhobenen Forderungen nach einer Aufhebung des Verbots der Fernsehberichterstattung aus Gerichtsverhandlungen entschieden entgegen. Vor laufenden Mikrofonen und Kameras würde es unweigerlich zu gravierenden Beeinträchtigungen des Persönlichkeitsrechts der Angeklagten, der Opfer, der Zeugen und ihrer Angehörigen insbesondere in Strafprozessen kommen. Die Datenschutzbeauftragten gehen dabei grundsätzlich von der gleichen Gefährdung in allen gerichtlichen Verfahren aus. Die Gerichtsverhandlung darf nicht zu einem massenmedial vermittelten „modernen Pranger" werden.

Die Rechtslage ist eindeutig: Fernsehaufnahmen aus der Gerichtssitzung sind nach § 176 GVG möglich, wenn der Vorsitzende es sitzungspolizeilich gestattet. Zur Sitzung gehören im Unterschied zur Verhandlung die Zeiten unmittelbar vor Beginn und nach Schluß der Verhandlung sowie die Verhandlungspausen. Fernsehaufnahmen aus der Verhandlung sind dagegen gem. § 169 GVG verboten. So hat das Bundesverfassungsgericht in seiner „Honecker-Entscheidung" (Beschluß vom 14. Juli 1994, Az.: 1 BvR 1595/92, NJW 1995, 184) ein Recht der Bildmedien bejaht, außerhalb der eigentlichen Gerichtsverhandlung Filmaufnahmen von Angeklagten im Gerichtssaal zu machen, falls es sich um Personen der Zeitgeschichte handelt. Danach reicht der Schutz der Rundfunkfreiheit wie der der Pressefreiheit von der Beschaffung der Information bis zur Verbreitung der Nachricht. Er erstreckt sich auch auf die medienspezifische Form der Berichterstattung und die Verwendung der dazu erforderlichen technischen Vorkehrungen. Wird die Berichterstattung durch den Rundfunk durch eine sitzungspolizeiliche Anordnung nach § 176 GVG beschränkt, so muß die Auslegung dieser Vorschrift der Bedeutung von Artikel 5 Abs. 1 Satz 2 GG Rechnung tragen und die Maßnahme dem Grundsatz der Verhältnismäßigkeit genügen. Was den konkreten Sachverhalt des vom Bundesverfassungsgericht zu entscheidenden Falles anbelangt, so hatte der Vorsitzende der Strafkammer in dem Strafverfahren gegen Erich Honecker, Erich Mielke, Willi Stoph, Heinz Keßler und andere das Fotografieren, Filmen und das Herstellen von Tonbandaufzeichnungen im Sitzungssaal nicht gestattet, ebenso Interviews mit Verfahrensbeteiligten im Sitzungssaal. Nach Auffassung des Bundesverfassungsgerichts greift der im vorliegenden Fall angeordnete Ausschluß von Fernsehaufnahmen in das Grundrecht der Rundfunkfreiheit ein. In den Entscheidungsgründen finden sich dazu folgende Ausführungen: „Die verbleibenden Gefahren für die äußere Ordnung des Strafverfahrens und das Persönlichkeitsrecht von Beteiligten und Dritten rechtfertigten ein vollständiges Verbot von Fernsehaufnahmen jedenfalls deshalb nicht, weil dieses die Rundfunkfreiheit unangemessen einschränkte. (. . .) Es bestand daher ein anerkennenswertes Interesse, mit den Mitteln der modernen Kommunikationstechnik auch einen optischen Eindruck von diesem Verfahren der Öffentlichkeit zu übermitteln und der Nachwelt zu erhalten."

19.5 Medienarchive

Ein weiteres Beispiel für die rasante Entwicklung der Medientechnik ist die verstärkte Nutzung von Medienarchiven. Die elektronischen Archive enthalten zumeist veröffentlichtes Material, wie Artikel aus Zeitungen, Zeitschriften und Meldungen von Nachrichtenagenturen. Es wurde bereits damit begonnen, ganze Jahrgänge von Zeitungen, Zeitschriften und Magazinen auf elektronische Datenträger, z. B. auf CD-ROM, zu pressen und zu vermarkten. Neue Techniken schleichen sich auf leisen Sohlen in unseren Alltag ein. Hier hat das Archiv nichts mehr mit Staub, sondern mit modernster Technik zu tun. Ein Verbund europäischer Verlage will noch in diesem Jahr aktuelle Zeitschriften parallel zum „normalen" Verkauf Online anbieten. Auch hier wird dann jedermann, in diesem Fall per Telefonleitung, gezielt auf personenbezogene Daten zugreifen können, und zwar auch dann, wenn sich die Datenträger etwa im außereuropäischen Ausland befinden.

Auf diese Weise öffnen also Medienarchive, die bislang ausschließlich für journalistische Zwecke genutzt wurden, riesige Datensammlungen für medienfremde Nutzer. Gerade hier liegt die besondere Brisanz dieser Entwicklung. Wenn nämlich auch lange zurückliegende Publikationen praktisch von jedermann recherchiert werden können, ist damit die Gefahr verbunden, daß in Persönlichkeitsrechte besonders tief eingegriffen wird. Damit droht das in verschiedenen Rechtsbereichen vorgesehene „Recht auf Vergessen" wirkungslos zu werden, das z. B. durch Löschungsvorschriften für das Bundeszentralregister gewährleistet werden soll. Als Beispiel könnte man an „Jugendsünden" von Politikern denken, die unter Umständen Jahrzehnte zurückliegen, und dennoch mittels einer Volltextrecherche von jedermann wieder sekundenschnell hervorgezaubert und entsprechend plaziert werden können. Aber nicht nur Politiker, sondern alle Personen können betroffen sein. So ist nach Ablauf von Jahrzehnten niemand mehr in der Lage, die Gegenargumente und die in den Medien (damals) möglicherweise nicht angemessen berücksichtigten Fakten zu nennen. Eine unter diesen Mängeln leidende Darstellung könnte dann irgendwann als „historische Wahrheit" im Raum stehen. Hier sollte eine ländereinheitliche Regelung gefunden werden, die datenschutzrechtliche Festlegungen enthält und klarstellt, daß ein wie auch immer geartetes Medienprivileg in diesem Zusammenhang keine Geltung beanspruchen kann, wobei auch der Abruf von im Ausland bereitgehaltenem Archivmaterial geregelt werden muß.

20. Telekommunikation

20.1 Europäische Richtlinie zum Datenschutz im ISDN

Im Bereich der Vermittlungstechnik und bei den Endgeräten verdrängt die digitale Welt der Informationsverarbeitung durch Computer die analoge Nachrichtenübertragung. Das diensteintegrierende digitale Fernmeldenetz (ISDN) ist ein Konzept, das

entwickelt wurde, um die Bereitstellung einer Vielzahl von Sprach- und Nichtsprachdiensten innerhalb desselben Netzes zu ermöglichen. Die Digitalisierung der Telekommunikationsnetze ermöglicht die effektive Kopplung von Datenverarbeitungssystemen mit digitalen Telefonanlagen. Weiterhin können mit diesen Netzen Verbindungen von Einzelplatzrechnern untereinander oder mit Großrechnern hergestellt werden, was wiederum die Voraussetzungen für eine Datenfernverarbeitung schafft. Im Bereich des Mobilfunktelefondienstes wirkt sich die digitale Übertragung besonders positiv auf die Qualität der Sprachübertragung aus. Bei allen Formen der digitalen Informationsübertragung werden in den Vermittlungsstellen notwendigerweise personenbezogene Daten gespeichert (vgl. hierzu 14. Tb., Tz. 20.1).

Aufgrund seiner universellen Eigenschaften und der vielfältigen Vorteile, über die das ISDN im Vergleich zum traditionellen Telefonnetz verfügt, ist es prädestiniert zum Ausbau als transeuropäisches Netz, wie es in Titel XII EGV vorgesehen ist. Angesichts dieser Bedeutung wurde auf EU-Ebene auch erkannt, daß hier ein rechtlicher Rahmen für den Schutz der Privatsphäre erforderlich ist.

Die Europäische Kommission hat am 13. Juni 1994 den geänderten Vorschlag für eine Richtlinie zum Datenschutz im ISDN vorgelegt (genaue Bezeichnung: Richtlinie des Europäischen Parlaments und des Rates zum Schutz personenbezogener Daten und der Privatsphäre in digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz und digitalen Mobilfunknetzen; Fundstelle: Amtsblatt der EG, C 200 vom 22. Juli 1994, S. 4).

Der Richtlinienvorschlag betrifft die Verarbeitung personenbezogener Daten durch Telekommunikationsorganisationen. Auf Deutschland bezogen sind dies die Telekom sowie lizensierte Betreiber von Mobilfunknetzen. Die Regelungen gelten für alle von diesen in digitalen Leitungs- oder Mobilfunknetzen angebotenen Telekommunikationsdienste. Einige Vorschriften gelten auch für Diensteanbieter in digitalen Netzen, die nicht Netzbetreiber sind. Teilnehmer am Telefonverkehr sollen danach künftig besser geschützt werden. Die Richtlinie wird in Europa die Nutzbarkeit der technischen Funktionen von ISDN und Mobilfunk einschränken. Sie behandelt die Verarbeitung von Rechnungs- und Verbindungsdaten, Einzelverbindungsnachweisen, die Anzeige der Rufnummer des Anrufenden, Telefonverzeichnisse und Überwachungsmaßnahmen. Da das Datenaufkommen in digitalen Telekommunikationsnetzen zu einer erhöhten Gefährdung der Persönlichkeitsrechte der Teilnehmer führt, sollen die Telekommunikationsunternehmen deshalb nur die erforderlichen Daten speichern dürfen. Darunter fallen Abrechnungsdaten, die aber gelöscht werden sollen, sobald der Kunde gegen die Rechnung keinen Einspruch mehr erheben kann. Die Liste der einzelnen geführten Gespräche soll nur auf Antrag gespeichert werden dürfen. Der Richtlinienvorschlag sieht fernerhin vor, daß die teilnehmende Person jeweils bei jedem Gespräch die Möglichkeit zur Unterdrückung der Identifikation erhalten muß. Der Angerufene kann dann die Nummer des Anrufenden nicht mehr auf dem Display seines Telefongeräts erkennen. Telefonkunden sollen auch die Möglichkeit erhalten, ihr Gerät für alle eintreffenden Anrufe zu sperren, bei denen die Identifikation des Anrufenden unterdrückt wird. Dadurch lassen sich anonyme Störanrufe verhindern. Auf Antrag ist die zeitweise Erfassung der Nummern aller Anrufer zulässig, wenn der Kunde anonyme Störanrufe zu beklagen hat. Weiterhin soll die Speicherung auf der Basis einer Gerichtsentscheidung möglich sein, wenn dies zur Verhinderung von erheblichen Straftaten notwendig ist.

Insgesamt hat das Niveau des Datenschutzes durch den geänderten Vorschlag gegenüber dem ursprünglichen Entwurf allerdings gelitten. Zu nennen sind folgende Punkte: Das ausdrückliche Verbot, personenbezogene Daten nicht zur Erstellung elektronischer Profile der Teilnehmer zu nutzen, ist entfallen; die Regelung über die Garantie der Vertraulichkeit der Kommunikationsbeziehungen und -inhalte wurde gestrichen; schließlich sind zum Einzelgebührennachweis und zur Anrufweiterschaltung konkrete Vorgaben im Richtlinienentwurf nicht mehr enthalten.

Begründet wurden diese Maßnahmen mit dem Hinweis auf das Subsidiaritätsprinzip, das in Artikel 3 b Satz 2 EGV vorgesehen ist. Diese Bestimmung lautet: „In den Bereichen, die nicht in ihre ausschließliche Zuständigkeit fallen, wird die Gemeinschaft nach dem Subsidiaritätsprinzip nur tätig, sofern und soweit die Ziele der in Betracht gezogenen Maßnahmen auf Ebene der Mitgliedstaaten nicht ausreichend erreicht werden können und daher wegen ihres Umfangs oder ihrer Wirkungen besser auf Gemeinschaftsebene erreicht werden können." In diesem Zusammenhang ist auf eine Kuriosität hinzuweisen. So steht in der Begründung der Kommission zu lesen, daß der geänderte Entwurf unter dem Gesichtspunkt der Subsidiarität zu einer tiefgreifenden Neubewertung geführt habe. Einige Zeilen später wird ausgeführt, daß die vorgesehene Maßnahme unter die ausschließliche Zuständigkeit der Gemeinschaft im Hinblick auf die Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten zur Verwirklichung des Binnenmarktes gem. Artikel 100 a EGV fällt. Ob dieser Widerspruch sehenden Auges hingenommen wurde, weil mit der Inbezugnahme des Subsidiaritätsprinzips der Kritik mancher nationaler Telekommunikationsorganisation besser begegnet werden kann, mag dahingestellt bleiben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat inhaltlich Verbesserungsvorschläge zum geänderten Richtlinienentwurf der Kommission vorgelegt (vgl. Anlage 16).

20.2 Postreform II – Rechtsgrundlagen in Bewegung

Schon die erste Postreform stand im Zeichen der Anpassung an EG-Recht – vor allem im Hinblick auf die Verwirklichung des Binnenmarktes –, beispielsweise an die Erfordernisse aus Artikel 59 EGV (freier Dienstleistungsverkehr) und Artikel 90 EGV,

wonach die Mitgliedstaaten in bezug auf öffentliche Unternehmen keine dem EG-Vertrag widersprechenden Maßnahmen treffen oder beibehalten. Zu nennen sind hier insbesondere das Verbot wettbewerbsbehindernder Vereinbarungen oder Beschlüsse (Artikel 85 EGV) und das Verbot des Mißbrauchs einer den Markt beherrschenden Stellung (Artikel 86 EGV). Der Einfluß des EG-Rechts wird allerdings dadurch begrenzt, daß die völlige Privatisierung der Telekommunikationsunternehmen eine autonome Entscheidung eines jeden Mitgliedstaates ist. So stellt Artikel 222 EGV klar, daß der EG-Vertrag die Eigentumsordnung in den Mitgliedstaaten unberührt läßt.

Allgemein ist festzustellen, daß zeitgleich mit der Digitalisierung im Bereich der Telekommunikation und der Entwicklung hin zu liberalisierten europäischen Telekommunikationsmärkten sich der Prozeß der Entstaatlichung der Telekommunikation durch Privatisierung der großen nationalen Telekommunikationsunternehmen fortgesetzt hat. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung vom 26. Oktober 1993 auf die Datenschutzprobleme bei der Privatisierung der Deutschen Bundespost Telekom und bei der europaweiten Liberalisierung des Telefonnetzes und anderer Telekommunikationsdienste hingewiesen (vgl. Anlage 6).

Als jüngstes Beispiel kann hier die Postreform II in Deutschland genannt werden, nach der aus dem bisherigen öffentlichen Staatsunternehmen Deutsche Bundespost Telekom zum 1. Januar 1995 die Deutsche Telekom AG wurde, eine juristische Person des Privatrechts. Zu diesem Zeitpunkt ist das (Artikel-)Gesetz zur Neuordnung des Postwesens und der Telekommunikation (PTNeuOG) in Kraft getreten. Zuvor wurde hinsichtlich der dafür erforderlichen Änderungen des Grundgesetzes ein Gesetzgebungsverfahren eingeleitet und sehr schnell zum Abschluß gebracht. Die Verfassungsänderung trat bereits am Tage ihrer Verkündung im Bundesgesetzblatt am 3. September 1994 in Kraft (Gesetz zur Änderung des Grundgesetzes vom 30. August 1994; BGBl. I, S. 2245). Das verfassungsändernde Gesetz verkürzt die Gegenstände bundeseigener Verwaltung nunmehr auch um die Bundespost. Hier ist von besonderer Bedeutung, daß durch die Überführung der deutschen Bundespost in privatrechtliche Unternehmensformen ein historisch gewachsener Adressat des grundrechtlich geschützten Post- und Fernmeldegeheimnisses entfällt; denn auf Private finden die Grundrechte keine unmittelbare Anwendung. Insbesondere auf dieses Problem haben die Datenschutzbeauftragten des Bundes und der Länder in einem Konferenzbeschluß vom 9. März 1994 aufmerksam gemacht (vgl. Anlage 9). Sie haben einen verfassungsrechtlichen Ausgleich gefordert, der allerdings nicht erreicht werden konnte. Nunmehr ist der Gesetzgeber in der Pflicht, den Schutz des Post- und Fernmeldegeheimnisses im einfachen Recht weiterhin zu gewährleisten. Eine zentrale Aussage hierzu trifft § 10 Fernmeldeanlagengesetz (FAG), wonach jeder, der eine für den öffentlichen Verkehr bestimmte Fernmeldeanlage betreibt, beaufsichtigt, bedient oder sonst bei ihrem Betrieb tätig ist, zur Wahrung des Fernmeldegeheimnisses verpflichtet ist. Beachtet werden sollte hier indessen, daß gem. § 28 FAG mit Ablauf des 31. Dezember 1997 (Ende des Netzmonopols) das FAG außer Kraft tritt.

Ferner haben die Datenschutzbeauftragten deutlich gemacht, daß im PTNeuOG ein der verfassungsgerichtlichen Rechtsprechung entsprechender Schutz von Individualrechten zu gewährleisten ist. Das Bundesverfassungsgericht hatte in seinem „Fangschaltungsbeschluß" entschieden, daß § 30 Abs. 2 Postverfassungsgesetz, die Ermächtigungsgrundlage der Datenschutzverordnung für die Deutsche Bundespost Telekom (TDSV), keine ausreichend verfassungskonforme Rechtsgrundlage für die Verarbeitung von Verbindungsdaten darstelle (vgl. 14. Tb., Tz. 20.3). Nunmehr wurde mit § 10 Postregulierungsgesetz – diese Vorschrift ist Bestandteil des Artikels 7 PTNeuOG – eine neue Verordnungsermächtigung geschaffen. In dieser Regelung sind datenschutzrechtliche Grundsätze wie die Verhältnismäßigkeit und insbesondere Beschränkungen bei der Erhebung, Verarbeitung und Nutzung von Daten sowie der Grundsatz der Zweckbindung vorgeschrieben. Das Bundesministerium für Post und Telekommunikation hat zwischenzeitlich den Entwurf einer Telekommunikations- und Informationsdienstunternehmen-Datenschutzverordnung (TIDSV) vorgelegt, auf dessen Mängel eine Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19. September 1995 näher eingeht (vgl. Anlage 27). Der Kernpunkt der Kritik besteht darin, daß der Verordnungsentwurf grundsätzlich die Identifikation der Nutzer von Telekommunikations- und Informationsdienstleistungen vorsieht und es den Betreibern von Netzen und Anbietern von Diensten gestattet, individualisierte Verbindungsdaten von den Teilnehmern zu erheben und zu verarbeiten. Eine solche Regelung wird der Bedeutung des Grundrechts auf unbeobachtete Kommunikation nicht gerecht. Denn im Zeitalter der elektronischen Information und Kommunikation ist es geboten, die Betreiber zur Bereitstellung anonymer Nutzungsmöglichkeiten zu verpflichten und den Bürger in die Lage zu versetzen, selbst zu entscheiden, ob er seine personenbezogenen Daten preiszugeben bereit ist.

20.3 Neuorganisation der Informationstechnik in Rheinland-Pfalz

In Rheinland-Pfalz ist eine Entwicklung im Gange, die staatliche und kommunale Informations- und Kommunikationstechnik (IuK) – erstmals auf der Basis einer gesetzlichen Regelung – neu zu organisieren. Bislang hat das Land – jeweils getrennt voneinander – die staatlichen Rechenzentren des Statistischen Landesamtes (ADV-Abteilung und Landesrechenzentrum Mainz) und der Zentralen Datenverarbeitung der Finanzverwaltung bei der Oberfinanzdirektion Koblenz (ZDFin) einschließlich der zentralen Datennetze des Landesrechenzentrums und der Finanzverwaltung betrieben. Aufgrund der tiefgreifenden Veränderung der Informations- und Kommunikationstechnik ist nach Auffassung der Landesregierung eine Umgestaltung der Organisation der Datenverarbeitung erforderlich. Nunmehr werden die Aufgaben der Rechenzentren einschließlich der Daten- und Kommunikationsnetze unter Berücksichtigung der Besonderheiten der Polizei und der Steuerverwaltung unter dem Dach einer

Anstalt des öffentlichen Rechts zusammengeführt. Ein Daten- und Informationszentrum (DIZ) soll seine Dienstleistung der Landesverwaltung sowie den kommunalen Gebietskörperschaften und anderen öffentlichen Stellen im Rahmen vertraglicher Absprachen gegen Erstattung der Kosten anbieten.

Es ist zu begrüßen, daß der LfD bereits in der Planungsphase beteiligt wurde. Er war insbesondere in der Arbeitsgruppe „Datenkommunikation" vertreten und hat in diesem Zusammenhang im April 1994 zu den Risiken des Projekts eine Stellungnahme abgegeben.

So macht die Vernetzung von Rechnern Informationsflüsse möglich, die bisher nicht realisiert werden konnten. Daraus ergeben sich Konsequenzen für die Informationstrennung und die Zweckbindung von Informationen. Der klassische Datenschutz als Instrument der Mißbrauchsverhinderung reicht im Hinblick auf die Einrichtung behördenübergreifender Netze nicht mehr aus. Wenn die vernetzten Rechner nicht nur in behördliche, sondern auch in öffentliche Netze (z. B. Datex-P, ISDN) integriert werden, ist dies im Hinblick auf die Gewährleistung des Datenschutzes und der Datensicherheit naturgemäß mit Problemen verbunden. Die technische Entwicklung hat dazu beigetragen, daß die Verantwortlichkeiten nicht mehr so klar strukturiert sind, wie sie es bei der Groß-DV waren. Heute liegt zwar grundsätzlich die Verantwortung bei der fachlich zuständigen Stelle, die jedoch auf vielfältige Weise mit anderen Beteiligten zusammenwirkt. Die fachlich zuständige Stelle betreibt z. B. selbst Rechner, die mit anderen Systemen kommunizieren. Die Rechner sind unter Umständen mittels lokaler, durch die Fachbehörde betriebener Netze (LAN) oder das Landesdatennetz mit anderen Rechnern verbunden.

Die Modernisierung des Landesdatennetzes führt dazu, daß von jedem beliebigen mit IuK-Technik ausgestatteten Arbeitsplatz mit jedem anderen angeschlossenen Arbeitsplatz Nachrichten ausgetauscht werden können und grundsätzlich auf jede IuK-Anwendung zugegriffen werden kann, unabhängig davon, auf welchem Rechner sie zur Verfügung gestellt wird. Durch die prinzipiell mögliche Kommunikation aller Anschlußnehmer können die Informationen so betrachtet werden, als seien sie in einem großen Datenpool vorgehalten. Probleme ergeben sich z. B., wenn Personen, die berechtigterweise Zugriff auf Informationen haben, diese gesetzwidrig übermitteln. Diese Probleme unterscheiden sich von den gegenwärtig schon bestehenden dadurch, daß die Technik gesetzwidrige Übermittlungen erleichtert und die Aufdeckung von Verstößen erschwert. Hier können die Grundrechte derjenigen Bürger berührt sein, deren Daten im Netz verarbeitet werden. Die rechtlichen, technischen und organisatorischen Steuerungs- und Kontrollmöglichkeiten für die IuK-Technik sollten im Zusammenhang mit der Vernetzung verbessert werden, um einen effektiven Grundrechtsschutz zu gewährleisten. Nach dem Volkszählungsurteil ist die Entscheidung über die Preisgabe und Verwendung von personenbezogenen Daten grundsätzlich Sache des Bürgers selbst; Abweichungen von diesem Grundsatz bedürfen einer gesetzlichen, normenklaren Regelung. Aus dem Grundsatz der Verhältnismäßigkeit ist abzuleiten, daß diese Regelungen eine Datenverarbeitung nur insoweit zulassen, als diese für die Erfüllung einer konkreten Verwaltungsaufgabe erforderlich ist. Aus dem Volkszählungsurteil ergibt sich ferner, daß die öffentliche Verwaltung keine informationelle Einheit darstellt. Daraus folgt für die Verwaltungstätigkeit der Grundsatz der Informationstrennung als technisch-organisatorische Konsequenz des Zweckbindungsgedankens.

Es sind Zweifel angebracht, ob die Regelung hinsichtlich des automatisierten Übermittlungsverfahrens in § 7 LDSG für behördenübergreifende Netze einschlägig ist, denn derartige Netze sind nicht an einzelne Verfahren gebunden. Es sollen vielmehr die technischen Voraussetzungen für einen Informationsaustausch beliebiger Partner geschaffen werden, wobei die im Netz verfügbare Kommunikationssoftware die Übertragung jedweder Information im Netz ermöglichen könnte. Der direkte Zugriff auf die Daten einer anderen Stelle birgt besondere Risiken für das Recht auf informationelle Selbstbestimmung.

Für alle Kontrollorgane der Verwaltung (z. B. LfD) ist das Ressortprinzip eine wesentliche Voraussetzung für die Wahrnehmung ihrer Aufgaben. Die durch Zuständigkeitsanordnungen zugewiesenen Verantwortlichkeiten sind Grundlage für die Beurteilung der Rechtmäßigkeit der Datenverarbeitung. Mit der Schaffung übergreifender Datenpools, in die verschiedene Stellen Daten einspeisen und auf die von verschiedenen Stellen zugegriffen werden kann, besteht die Gefahr, daß die Transparenz verlorengeht, wer für eine Entscheidung verantwortlich ist.

Beim Netzbetrieb sollte festgelegt sein, daß jede berechtigte Person von bestimmten, dem Netz bekannten Endgeräten bestimmte Anwendungen auf einem bestimmten Rechner nutzen und ggf. mit bestimmten anderen Personen an bestimmten Endgeräten im Rahmen bestimmter Aufgaben kommunizieren darf. Gemäß dem Gebot der Informationstrennung könnte auf diese Weise eine wirksame Abschottung gegenüber Verwaltungseinheiten mit unterschiedlichen Aufgabenstellungen gewährleistet werden.

In diesem Zusammenhang ist darauf hinzuweisen, daß die zunehmende Verwaltungsautomation auch das Recht auf informationelle Selbstbestimmung derjenigen Mitarbeiterinnen und Mitarbeiter berührt, die die IuK-Technik benutzen (Gefahr der Verhaltens- und Leistungskontrollen; Erstellen von Kommunikationsprofilen).

Aus Sicht des Datenschutzes ist es nicht nur wichtig, Kommunikationsinhalte gegen unberechtigte Zugriffe zu schützen. Ebenso wichtig ist es, das Bestehen von Kommunikationsbeziehungen vor unbefugter Kenntnis zu schützen. Die Vernetzung

heterogener Rechnersysteme schafft nicht nur die Infrastruktur zu einem übergreifenden Rechner- und Datenverbund, sondern führt auch zu gravierenden Datensicherungsrisiken, die nicht allein unter datenschutzrechtlichen Gesichtspunkten bedeutsam sind. Zusätzliche netzbedingte Risiken sind z. B. das Abhörrisiko und die unverschlüsselte Übertragung von Daten. Unter dem Aspekt des Schutzes der staatlichen Funktionsfähigkeit erhält neben dem Schutz personenbezogener Daten vor Mißbrauch die Datensicherheit zunehmend verfassungsrechtliche Relevanz.

Was die rechtliche Stellung des Netzbetreibers anbelangt, hat der LfD u. a. auf ein Gutachten des Justizministeriums Baden-Württemberg hingewiesen. Im Hinblick auf die Frage, ob eine Übertragung auf private Träger möglich ist, enthält das Gutachten folgende Kernaussagen:

- Das Landesverwaltungsnetz (LVN) „wird daher immer mehr vergleichbar mit einem ‚Nervensystem' der öffentlichen Verwaltung, ohne dessen ungestörtes Funktionieren in Kürze eine geordnete Verwaltung nicht mehr vorstellbar wäre. Der Betrieb des LVN ist somit untrennbar mit der Ausübung staatlicher Hoheitstätigkeit verbunden und muß als deren Bestandteil angesehen werden."
- Aus Artikel 108 GG „folgt, daß die Steuerverwaltung in der Form der unmittelbaren Staatsverwaltung durchgeführt werden muß. (. . .) Das Verwaltungsnetz der Finanzverwaltung darf demnach nicht auf einen privaten Träger übertragen werden, da es einen Bestandteil der Steuerverwaltung darstellt."

Für die Frage, ob beispielsweise auch privatrechtlich organisierte Firmen Netzteilnehmer sein können, hat der LfD auf die Neuregelung in § 2 Abs. 1 Satz 1 LDSG hingewiesen, wonach der Begriff der „öffentliche Stelle" nicht nur für die öffentlich-rechtlich organisierten Stellen des Landes einschließlich ihrer Vereinigungen gelten soll, sondern auch für deren in Privatrechtsform errichteten juristischen Personen oder Vereinigungen. Hierzu rechnen insbesondere auch in der Rechtsform einer Gesellschaft mit beschränkter Haftung (GmbH) geführte Einrichtungen der öffentlichen Hand. Gemäß § 2 Abs. 1 Satz 2 LDSG gelten als öffentliche Stellen auch diejenigen juristischen Personen und sonstigen Vereinigungen des privaten Rechts, an denen neben nichtöffentlichen Stellen die in Satz 1 genannten öffentlichen Stellen beteiligt sind, wenn ihnen allein oder gemeinsam mit den anderen in Satz 1 genannten Stellen die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht (Beispiel: Sonderabfall-Management-Gesellschaft Rheinland-Pfalz mbH; die Beteiligungsverhältnisse ergeben sich aus § 8 b Abs. 1 Nr. 2 Landesabfallwirtschafts- und Altlastengesetz i. V. m. § 1 der Landesverordnung über die Andienung von Sonderabfällen). Nach Auffassung des LfD bestehen keine Bedenken, diese Vorgaben für die Entscheidung über die jeweiligen Anschlußberechtigungen an das Netz heranzuziehen.

20.4 Entwurf eines Gesetzes über die Errichtung des Daten- und Informationszentrums Rheinland-Pfalz (DIZ)

Der LfD hat zu dem Gesetzentwurf in einem Erörterungstermin im Mai 1995 Stellung genommen, wobei er nochmals darauf hingewiesen hat, daß nach der vom Ministerium des Innern und für Sport im März 1993 versandten Ministerratsvorlage die staatliche und kommunale Informations- und Kommunikationstechnik in Rheinland-Pfalz erstmals auf der Basis einer gesetzlichen Regelung neu zu organisieren ist. Danach setzen „alle grundlegenden organisatorischen Veränderungen gesetzgeberische Initiativen voraus. (. . .) Hierfür ist ein Landes-IT-Organisationsgesetz erforderlich."

In dem Entwurf wird indessen im Begründungsteil unter dem Punkt „Allgemeines" ausgeführt, daß das Gesetz gerade „keine Festlegungen im Hinblick auf die Organisation der Informations- und Kommunikationstechnik innerhalb der Landesverwaltung" trifft. Der LfD geht mithin davon aus, daß die Absicht besteht, einen entsprechenden Gesetzentwurf, der den genannten Bereich betrifft, noch auszuarbeiten.

Im Gesetzestext findet der Schutz personenbezogener Daten in § 3 Abs. 1 Satz 2 letzter Halbsatz Erwähnung. Danach fördert das DIZ die Verwirklichung des Datenschutzes. Sonstige Regelungen zu diesem Thema sind nicht vorhanden. Sicherlich ist das „DIZ-Errichtungsgesetz" auch nicht der geeignete Ort, um datenschutzrechtliche Anforderungen, beispielsweise für die Kommunikation im Netz, zu formulieren. In diesem Zusammenhang hat der LfD jedoch zum Ausdruck gebracht, daß gerade dieser Bereich besonders datenschutzrelevant ist und seines Erachtens einer gesetzlichen Regelung bedarf. So gibt es zwar für den klassischen Dialog mit einem Host-Rechner Programme, die bei entsprechender Generierung den Datenschutz gewährleisten. Nun wird aber mit dem neuen Netz die Voraussetzung für die Kommunikation „jeder mit jedem" geschaffen. Damit sind Probleme aus Sicht des LfD vorprogrammiert, beispielsweise dann, wenn auf dem Zielrechner keine lückenlose Kontrolle ordnungsgemäßer Datenverarbeitung möglich ist.

Fernerhin hatte der ursprüngliche Entwurf im Begründungsteil Ausführungen enthalten, die aus Sicht des LfD mit der gesetzlichen Lage nicht in Einklang standen. So wurde die Auffassung vertreten, daß es „unter Beachtung des Datenschutzes und der Datensicherheit – mit wenigen Ausnahmen (z. B. bei berechtigten Bedenken von Sicherheitsbehörden) – keine Informationen geben darf, die das ‚Eigentum' nur einer Behörde oder einer Fachverwaltung sind. (. . .) Das Daten- und Informationszentrum soll Konzepte liefern, damit die Ressource Information im notwendigen Umfang und zum benötigten Zeitpunkt den beteiligten Stellen im Rahmen der Zugriffsberechtigung und der Erforderlichkeit zur Erfüllung ihrer Aufgabe zur Verfügung steht." Es wurde hier nicht berücksichtigt, daß gem. § 13 Abs. 1 LDSG personenbezogene Daten regelmäßig nur für die Zwecke ge-

speichert und genutzt werden dürfen, für die sie erhoben worden sind. Damit unterliegen grundsätzlich alle von der Verwaltung gespeicherten Daten der durch die Erhebung festgelegten Zweckbindung. Mithin hat der LfD vorgeschlagen, den entsprechenden Textteil unter dem Gesichtspunkt der Zweckbindung der personenbezogenen Daten zu überarbeiten. Dies ist zwischenzeitlich geschehen.

20.5 Gefahren beim täglichen Umgang mit Telefon und Anrufbeantworter

Stets aktuell sind Fragen hinsichtlich möglicher Gefahren für das Persönlichkeitsrecht im Bereich der Telefonie. Auch Presse und Hörfunk nehmen sich dieses Themas zunehmend an. Der LfD hat sich dazu u. a. im Mai 1995 in einem SWF-Hörfunkinterview geäußert.

Viele der heute eingesetzten Telefonanlagen verfügen über Leistungsmerkmale, die dem Nutzer die Arbeit wesentlich erleichtern können. Die moderne Technik birgt jedoch auch Gefahren in sich. Ein Beispiel ist das Mithören von Telefonaten Dritter oder von Gesprächen im Raum. So ist die Nutzung des häufig in die Telefone eingebauten Lautsprechers problematisch, wenn er ohne Wissen des Gesprächspartners eingeschaltet wird. Oft ist bei modernen Anlagen auch das Leistungsmerkmal „Aufschalten" vorhanden. Hier kann sich ein Dritter – z. B. die Arbeitskollegin in der Telefonvermittlung oder auch ein Vorgesetzter – bei bestehenden Verbindungen „aufschalten" und dann mithören. Dieser Vorgang wird bei den meisten Anlagen durch einen Hinweiston kenntlich gemacht, dessen Lautstärke allerdings auch oft verändert werden kann, so daß bei Leisestellung ein unbemerktes Aufschalten möglich ist. Ein weiteres Problem aus diesem Bereich besteht bei Telefonen mit Freisprechmöglichkeit. In ein solches Gerät ist ein Mikrofon eingebaut, so daß es ohne Abheben des Hörers möglich ist zu telefonieren. Wenn hier noch das Leistungsmerkmal „Direktansprechen" vorgesehen ist, wird das Mikrofon im Telefonapparat im Falle eines Anrufs automatisch eingeschaltet, also ohne Tätigwerden des Nutzers aktiviert. In diesem Zusammenhang ist durchaus der Fall denkbar, daß ein Anruf mit entsprechendem Signal erfolgt ist, bevor der Besitzer des Geräts den Raum betreten hat. Der Anrufer wird hier in die Lage versetzt, jedes im Raum gesprochene Wort unbemerkt mitzuhören.

Auch der Einsatz von Anrufbeantwortern mit Fernabfragemöglichkeit ist nicht unproblematisch. Diese Geräte sind technisch so ausgestaltet, daß eine Fernabfrage oder sogar die Fernbedienung aller Gerätefunktionen von einem anderen Telefonanschluß aus vorgenommen werden kann, wobei die Sicherheitsmechanismen sehr zu wünschen übriglassen. So wird von dem Abfragegerät meist ein nur aus zwei oder drei Tönen bestehendes Signal an den Anrufbeantworter gesendet, um die Identifizierung vorzunehmen und das Gerät für die gewünschten Funktionen zu aktivieren. Es ist in der Regel kaum ein Problem, den Schutzcode, also die Tonfolge (z. B. 2-1-3), etwa durch Ausprobieren zu ermitteln. Das Fernabfragegerät selbst kann für weniger als zehn DM im Fachhandel gekauft und im Anschluß ein Lauscheingriff gestartet werden. Denn durch die unzureichenden Sicherheitsmechanismen besteht die Möglichkeit des Abhörens der im Anrufbeantworter aufgezeichneten Mitteilungen. Darüber hinaus kann durch das Aktivieren der in die meisten Anrufbeantworter eingebauten Raumüberwachungsfunktion sogar das etwa im Wohnzimmer gesprochene Wort mitgehört werden.

Diese Beispiele zeigen, daß die schöne neue Telefonwelt auch mißbraucht werden kann und Gefahren für die Persönlichkeitsrechte der Telefonbenutzer mit sich bringt. Hier ist das kommunikative Selbstbestimmungsrecht als Ausprägung des Rechts auf informationelle Selbstbestimmung betroffen. Es geht insbesondere um den Schutz des vertraulich gesprochenen Wortes. Aufgabe des Datenschutzes ist es in diesem Zusammenhang, die Gefährdungen zu erkennen, zu beschreiben und mitzuhelfen, sie zu begrenzen, etwa durch die Herausgabe von Hinweisen zu der Gestaltung des Datenschutzes bei modernen Telekommunikationsanlagen (vgl. 14. Tb., Anlage 10).

21. Technischer und organisatorischer Datenschutz

21.1 Ergebnisse der Kontroll- und Beratungstätigkeit

Im Berichtszeitraum wurden unter technisch-organisatorischen Gesichtpunkten in ca. 60 Fällen örtliche Feststellungen nach § 24 Abs. 1 LDSG in unterschiedlichen Bereichen der staatlichen und kommunalen Verwaltung getroffen. Ergänzt wurden diese durch ca. 20 Beratungen nach § 24 Abs. 4 LDSG.

Neben anlaßbezogenen Kontrollen oder sich im Zusammenhang mit der Einführung neuer Verfahren ergebenden konkreten Fragen erfolgten wiederum systematische Prüfungen allgemeiner technisch-organisatorischer Maßnahmen beim Einsatz der Informationstechnik (vgl. 14. Tb. Tz. 21.4). So wurden Feststellungen u. a. bei

- Gesundheitsämtern,
- Kreisverwaltungen,
- Stadt- und Verbandsgemeindeverwaltungen,
- der Steuerberaterkammer Rheinland-Pfalz,
- Kassenärztlichen Vereinigungen,
- dem Landesrechenzentrum,

- der ZDFin Koblenz,
- dem Universitätsklinikum Mainz,
- Finanzämtern,
- Staatsanwaltschaften,
- verschiedenen Landesämtern,
- einer Körperschaft des öffentlichen Rechts,
- einer Sparkasse,
- einer öffentlichen Beratungsstelle,
- der Fachhochschule Rheinland-Pfalz

getroffen. Die 1993 begonnene Querschnittsprüfung im Bereich der Kreisverwaltungen wurde fortgeführt. Zwischenzeitlich sind bei elf von 36 Landkreisen und kreisfreien Städten örtliche Feststellungen erfolgt.

Die bereits im 14. Tätigkeitsbericht dargestellten Defizite waren auch im Berichtszeitraum zu beklagen. Angesichts des Wandels in der Informationstechnik und der zunehmenden Komplexität der eingesetzten Systeme haben sich die Probleme in den dort genannten Bereichen teilweise verschärft, wie die nachfolgenden Beispiele zeigen. So ergab sich im Rahmen der örtlichen Feststellungen unter anderem, daß

- alle Benutzer einer Anwendung (HKR) mit Systemverwalterberechtigung ausgestattet waren, obwohl dies nicht erforderlich war,
- in einem Verfahren (Kfz-Zulassung/Führerscheinwesen) bei sieben Beschäftigten an der eingesetzten AS400-Anlage insgesamt 49 Benutzerkennungen, davon mehrere mit Systemverwalterberechtigung, eingerichtet waren,
- in einer zentralen Anwendung (Umlageberechnung) keine für die Betreuung des Systems verantwortliche Person benannt war, das Paßwort der Systemkennung der öffentlichen Stelle nicht bekannt und die eingesetzte Software nicht dokumentiert war,
- im Bereich einer Personalabteilung die Konfiguration des eingesetzten Wählleitungsmodems zum Anschluß an das Telefonnetz der öffentlichen Stelle nicht bekannt war,
- in einer Beihilfestelle der für die Beihilfebearbeitung eingesetzte Arbeitsplatzrechner ohne Kenntnis der Verantwortlichen durch einen nicht vorgesehenen Mitarbeiter genutzt wurde sowie auf dem System nicht dokumentierte und nicht freigegebene Programme eingesetzt wurden,
- mangels Löschfunktionen bei selbsterstellten Anwendungen keine systematische Löschung abgeschlossener Fälle erfolgen konnte,
- Systemverwalterkennungen nicht mit Paßwortschutz versehen waren,
- Fernwartungszugänge mit Systemverwaltungsberechtigung ohne Grund aktiv und durchgeführte Fernwartungen nicht dokumentiert und nicht nachvollziehbar waren,
- elementare Empfehlungen zur Paßwortgestaltung (vgl. z. B. 14. Tb. Anlage 11) nicht berücksichtigt wurden; in einem Fall wurde im Sachgebiet „Beihilfe" für eine Anwendung mit der Bezeichnung „Beihilfe" das Paßwort „Beihilfe" gewählt.

Besondere Problembereiche waren wiederum die Zugriffs- und Speicherkontrolle, insbesondere bei Arbeitsplatzrechnern und an Netzwerkstationen, sowie – unter dem Gesichtspunkt der Protokollierung – die Eingabe- und Übermittlungskontrolle.

In einigen Fällen ergab sich dabei ein unzureichendes Sicherheitsniveau und eine Bestätigung der Vermutung, daß zu Lasten der Datensicherheit in vielen Fällen nach dem Grundsatz „never change a running system" verfahren wird.

21.2 Technisch-organisatorische Datenschutzfragen in einzelnen Verfahren

21.2.1 Automatisierte Vorgangsverwaltung der Polizei (Hamburger COMVOR-Verfahren)

Für die zur Zeit in Rheinland-Pfalz betriebenen polizeilichen Informationssysteme werden Überlegungen hinsichtlich einer Neugestaltung beziehungsweise der Anpassung an Entwicklungen in anderen Bereichen (INPOL-neu) angestellt. In diesem Zusammenhang wurde die Möglichkeit der Übernahme des Hamburger Verfahrens COMVOR zur automatisierten Vorgangsbearbeitung geprüft.

Zentraler Bestandteil des COMVOR-Konzeptes war die automatisierte Vorgangsbearbeitung der Polizei mit dem Ziel, hierbei erfaßte Daten für die Bereiche

- Vorgangsverwaltung einschließlich Führen einer elektronischen Kriminalakte,
- Ermittlungsunterstützung (Recherche) für Zwecke der Strafverfolgung, der Gefahrenabwehr sowie der vorbeugenden Straftatenbekämpfung,
- Erstellung von Lagebildern,
- Tagebuchauswertung,
- Erstellung der polizeilichen Kriminalstatistik (PKS) und
- Polizeiliche Meldedienste (KPMD)

nutzbar zu machen sowie Daten von vorgangsübergreifender Bedeutung den weiteren polizeilichen Verfahren (z. B. POLIS/INPOL) direkt zur Verfügung zu stellen. Die aufwendige Mehrfacherfassung von Daten sollte vermieden werden. Die unter Datenschutzgesichtspunkten bedeutsame Neuerung bestand dabei in der Zusammenführung zu einer einheitlichen Datenbasis.

Im Hinblick auf die datenschutzrechtliche Beurteilung des Hamburger Konzepts sowie die Frage, inwieweit sich die darin enthaltenen Vorgaben mit den in Rheinland-Pfalz bestehenden Anforderungen decken, wurde der LfD Rheinland-Pfalz um Stellungnahme gebeten.

Im Ergebnis hätten sich bei einer Übernahme des COMVOR-Konzepts im Vergleich zu den derzeitigen Verfahren Veränderungen bei

- der Art des Datenbestandes,
- der Art der Datenerfassung, -haltung und -pflege,
- den Auswertungsmöglichkeiten,
- Vernetzung der eingesetzten Systeme und Kommunikationsmöglichkeiten sowie
- der Art der eingesetzten Informationstechnik

ergeben. Datenschutzrechtlich bedeutsam war dabei insbesondere, daß das Konzept die Zusammenführung und teilweise Zentralisierung bislang getrennt geführter Datenbestände vorsah.

Zum Teil mögen die dadurch entstehenden Möglichkeiten einer solchen Lösung im Interesse eines effektiven Datenschutzes liegen (etwa bei der Durchführung von Löschvorgängen, bei der Erteilung von Auskünften). Ganz wesentlich waren aber auch die Gefahren einer solchen umfassenden technischen Zusammenführung im Blick zu behalten.

Punktuell waren im COMVOR-Konzept bereits Strukturen einer datenschutzgerechten Ausgestaltung vorgesehen; hierzu zählte die Unterscheidung zwischen einem Vorgangs-, Abgleich- und einem (anonymisierten) Statistikdatenbestand sowie die Unterteilung in bestimmte Personengruppen (Beschuldigter, Geschädigter, Zeuge, Verdächtigter, Anzeigeerstatter usw.), für die unterschiedliche Zugriffsmöglichkeiten eröffnet werden konnten. Weiterhin bot ein ausgefeiltes Funktionsmodell die (konzeptionelle) Grundlage einer effektiven Zugriffskontrolle; allerdings war eine Realisierung im Projektstadium noch nicht erfolgt. Als Besonderheit war für die Speicherung der Zugriffsberechtigung sowie der Benutzerprofile die Verwendung von Chipkarten vorgesehen.

Ein mit dem COMVOR-Daten- und Funktionsmodell korrespondierendes Datenschutzkonzept lag hingegen nicht vor, so daß für andere Bereiche Fragen offenblieben. Hierzu zählten insbesondere die nachvollziehbare Dokumentation der grundsätzlichen Datenschutzvorkehrungen, die Vorgaben hinsichtlich der Löschung und Archivierung der Vorgangsdaten, die Absicherung der Endgeräte sowie Protokollierungs- und Auswertungsfunktionen. Für diese Bereiche bestehen bei der derzeit in Rheinland-Pfalz noch eingesetzten Vorgangsverwaltung POLADIS bereits Regelungen, deren inhaltliche Übernahme aus Sicht des LfD erforderlich gewesen wäre.

Die Übernahme des Hamburger Verfahrens ist letztlich, insbesondere aufgrund der unterschiedlichen fachlichen Anforderungen, welche sich für die Polizei eines Flächenstaates im Vergleich zu der eines Stadtstaates ergeben, nicht erfolgt. Die vom LfD Rheinland-Pfalz problematisierten Datenschutzgesichtspunkte wurden insoweit im Rahmen der polizeifachlichen Prüfung bestätigt.

Die im Rahmen der COMVOR-Prüfung angesprochenen datenschutzrelevanten Punkte sind gleichwohl auch künftig von Bedeutung, soweit nämlich grundlegende Merkmale des Konzeptes wie die Einmalerfassung mit einheitlicher Benutzeroberfläche, die automatisierte Anbindung an andere Verfahren, ein einheitliches polizeiliches Daten- und Funktionsmodell und bestimmte technische Infrastrukturen für die absehbare Neugestaltung der polizeilichen Vorgangsbearbeitung in Rheinland-Pfalz sowie der Neukonzeption des INPOL-Verfahrens übernommen werden sollen. Der LfD geht davon aus, daß seine Empfehlungen dabei Berücksichtigung finden und wird dies weiter verfolgen.

21.2.2 Einsatz von Personalcomputern bei der Kommunalwahl 1994

Auch für die Kommunalwahl 1994 sollte, wie bereits 1989, die nach § 53 Abs. 10 Kommunalwahlordnung bestehende Möglichkeit genutzt werden können, die Stimmenauszählung automationsunterstützt vorzunehmen. Bei den in Betracht kommenden

Produkten handelte es sich – mit Ausnahme einer Großrechnerlösung – um Entwicklungen für den Einsatz auf Arbeitsplatzrechnern (PC) unter dem Betriebssystem MS-DOS.

Aufgrund der Erkenntnisse aus der zurückliegenden Kommunalwahl (vgl. 12. Tb., Tz. 16.3) wurde der LfD Rheinland-Pfalz im Rahmen der erforderlichen Freigabe der Programme durch den Landeswahlleiter um Stellungnahme gebeten.

Datenschutzrechtliche Gesichtspunkte betrafen, dem Charakter einer Wahl entsprechend, dabei nur wenige Bereiche; im wesentlichen galt dies für die Sicherstellung einer korrekten Verarbeitung der Daten sowie die Vermeidung unzulässiger Auswertungen (z. B. Reihungslisten gestrichener Kandidaten).

Eine besondere Bedeutung hatte jedoch der Einsatz von Arbeitsplatzrechnern für die Stimmenauszählung. Je nach Anzahl der Wahllokale einer Gemeinde war eine nennenswerte Zahl von Geräten erforderlich, 30 bis 50 Systeme stellten dabei eine übliche Größenordnung dar. Die benötigten Geräte wurden i. d. R. aus den einzelnen Verwaltungsbereichen (z. B. Sozialamt, Jugendamt, Ordnungsamt, Kasse usw.) abgezogen bzw. über entsprechende Aufrufe von dritter Seite zur Verfügung gestellt.

Aus Sicht des Datenschutzes war dabei sicherzustellen, daß während des vorübergehenden Einsatzes zu Wahlzwecken keine Preisgabe von personenbezogenen Daten aus den eigentlichen Verwendungsbereichen erfolgte. Weiterhin waren Beeinträchtigungen aufgrund der i. d. R. unbekannten Softwareausstattung bereitgestellter privater Geräte (im Endeffekt 57,5 % der eingesetzten Systeme) zu vermeiden (Stichwort: Computerviren).

Für den Einsatz von Arbeitsplatzrechnern bei der Kommunalwahl wurden daher vom LfD Rheinland-Pfalz in folgender Hinsicht Empfehlungen ausgesprochen:

- Löschen der auf den PC gespeicherten personenbezogenen Daten aus den eigentlichen Verwendungsbereichen,
- Überprüfung der eingesetzten Systeme vor der Wahl,
- Paßwortschutz der eingesetzten Programme,
- Bildung von Prüfsummen für die Programme und Stimmendaten (Versionskontrolle, Manipulationssicherheit),
- Protokollierung des Programmeinsatzes und der Ergebnisse,
- Möglichkeit einer Diskettenversion der Wahlprogramme, um bei Unterbrechungen die Wahldaten zu den Wahlunterlagen nehmen zu können,
- Hinweise zu organisatorischen Rahmenbedingungen bei der Vorbereitung und dem Einsatz der Geräte.

Die Empfehlungen des LfD Rheinland-Pfalz wurden im wesentlichen in die Hinweise des Landeswahlleiters zum Einsatz der automatisierten Datenverarbeitung bei Wahlen übernommen bzw. als Auflagen im Freigabeverfahren berücksichtigt.

In Zusammenarbeit mit den kommunalen Spitzenverbänden wurde eine Musterdienstanweisung für die lokalen Wahlleiter erstellt. Die Notwendigkeit insbesondere auch organisatorischer Vorgaben war daran erkennbar, daß ansonsten Manipulationsversuche (z. B. Stimmenumschichtung zwischen den Wahlvorschlägen) möglich waren, ohne daß dies anhand der bereitgestellten Protokolldaten erkennbar gewesen wäre. In einem Fall führte ein Eingabefehler bei der automatischen Erfassung zu einer Differenz von 500 Stimmen und damit zum Verlust eines Kreistagssitzes. Aufgrund der später erkannten Differenz zwischen dem maschinellen Protokoll und der Wahlniederschrift wurde letztere (!) ohne weitere Prüfung nachträglich abgeändert.

Nach dem Erfahrungsbericht des Gemeinde- und Städtebundes Rheinland-Pfalz zur Kommunalwahl 1994 (GStB Beilage 3/95 zu Heft 2/95) erfolgte die automatisierte Stimmenzählung in ca. 95 % der Stimmbezirke. Es ist davon auszugehen, daß auch die Stimmenzählung künftiger Wahlen in nennenswertem Umfang automationsunterstützt erfolgen wird. Im Hinblick auf die im Erfahrungsbericht des GStB angestellten Überlegungen zu künftigen Auszählungsverfahren sind dabei aus Sicht des LfD Rheinland-Pfalz rechtzeitig Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität der betroffenen Daten zu treffen.

21.2.3 Elektronische Post im Landesdatennetz (BKS-LRZ)

Im Rahmen einer zentralen Bürokommunikationsanwendung stellt das Landesrechenzentrum (LRZ) seit Mitte 1995 ein Verfahren für den Austausch elektronischer Post (e-mail) im Landesdatennetz zur Verfügung. Derzeit ist der Einsatz auf vier Pilotprojekte beim Gemeinde- und Städtebund, dem Landkreistag, dem Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau sowie dem Ministerium der Finanzen begrenzt; mit anderen Stellen der Landes- und Kommunalverwaltung werden Gespräche über einen Anschluß an das Verfahren geführt.

Der Rechner des LRZ dient dabei als zentraler Mail-Server, d. h. alle Teilnehmer besitzen dort ein elektronisches Postfach, in welchem eingehende Nachrichten abgelegt werden. Darüber hinaus soll es jedoch künftig ermöglicht werden, das Landesdatennetz lediglich als Übertragungsmedium zu nutzen und Nachrichten oder Dokumente direkt im DV-System des Empfängers abzulegen. Bislang werden dabei lediglich Systeme unterstützt, welche die Bürokommunikationsanwendung IBM Office Vision ermöglichen. Eine X.400-Schnittstelle ist für die Zukunft geplant.

Im Fall der Teilnahme wird jeder Benutzer in ein elektronisches Postverzeichnis mit den Angaben zur Organisation, Name, Benutzerkennung und Endgerätenummer eingetragen. Das Verzeichnis wird allen Teilnehmern zur Verfügung gestellt. Aus der Benutzerkennung ist die Behörde mit der jeweiligen Abteilung bzw. dem Sachgebiet ablesbar. Daher wird bei einem Personalwechsel lediglich der Name des neuen Bediensteten bei der Benutzerkennung ersetzt. Dies kann zur Folge haben, daß für den bisherigen Inhaber der Benutzerkennung bestimmte elektronische Post nunmehr an den neuen Inhaber gesandt wird, ohne daß dies dem Absender kenntlich gemacht wird. Der LfD hat daher angeregt, bei einem Personalwechsel die bisherige Benutzerkennung nicht direkt im Anschluß weiterzuverwenden und für den Zeitraum von drei Monaten zu sperren.

Im übrigen ist nach Auffassung des LfD Rheinland-Pfalz bei der Einrichtung und beim Betrieb elektronischer Postsysteme den Anforderungen Rechung zu tragen, welche in der Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Datenschutz bei elektronischen Mitteilungssystemen formuliert wurden (s. Anlage 24).

Danach sind insbesondere Maßnahmen vorzusehen, die

- die Authentizität von Benutzern, Nachrichten und Systemmeldungen,
- die Vertraulichkeit der übertragenen Daten,
- die Integrität von Nachrichten und Meldungen,
- fälschungssichere Kommunikationsnachweise sowie
- den Ausschluß der Bildung von Kommunikationsprofilen

gewährleisten. Die derzeitige Ausgestaltung des elektronischen Postsystems entspricht dem nur teilweise; so sind insbesondere die Fragen der Sicherstellung der Vertraulichkeit und Integrität von Nachrichten durch kryptografische Verfahren sowie des Umfangs der notwendigen Protokollierung noch offen. Die endgültige Antwort des Landesrechenzentrums hierzu steht noch aus.

21.2.4 Haushaltsaufstellungs- (HAVWin) und Haushaltsbewirtschaftungsverfahren (IRMA)

Auf der Grundlage eines Ministerratsbeschlusses vom 8. März 1994 wurde mit Beginn der Aufstellung des Haushalts 1996 für die Landesverwaltung ein automatisiertes Aufstellungsverfahren (HAVWin) auf der Basis ISDN-vernetzter Arbeitsplatzrechner (PC) eingeführt.

Aus Datenschutzsicht bedeutsam ist dabei weniger die Art der verarbeiteten Daten – ein Personenbezug ist dabei lediglich in Ausnahmefällen gegeben – sondern die Tatsache, daß das dem Verfahren zugrundeliegende technische Konzept zwischen den beteiligten Stellen zum Aufbau einer nach Art und Umfang bislang nicht vorhandenen technischen Infrastruktur führt, welche auch für weitere Anwendungen, insbesondere für das im Ministerratsbeschluß ebenfalls genannte Verfahren zur Haushaltsmittelbewirtschaftung (IRMA), genutzt wird.

Die Nutzung vorhandener technischer Möglichkeiten auch durch andere Verfahren ist grundsätzlich nicht zu beanstanden und wird, wie Erfahrungen aus der Praxis belegen, mittelfristig in aller Regel angestrebt. Neben praktischen Erwägungen sind dabei nicht zuletzt Wirtschaftlichkeitsüberlegungen von Bedeutung. Unter dem Gesichtspunkt des Datenschutzes und der Datensicherung ergibt sich damit jedoch die Notwendigkeit, beim Aufbau der IT-Struktur auch künftige Nutzungserweiterungen in Betracht zu ziehen.

Im Hinblick auf die geringe Sensibilität der im Verfahren HAVWin verarbeiteten Daten wurden die dort vorgesehen Maßnahmen der Zugriffskontrolle und Protokollierung vom LfD als ausreichend angesehen. Ähnliches gilt für die technischen Sicherungsmaßnahmen der ISDN-Anschlußkomponenten. Hier ist grundsätzlich die Bildung geschlossener Benutzergruppen, eine Rufnummernüberprüfung anhand fest vorgegebener Anschlußnummern sowie die protokollspezifische Konfiguration des ISDN-Routers vorgesehen. Die genannte Rufnummernüberprüfung in der ISDN-Anschlußeinheit ist nur bei geschlossenen Benutzergruppen, d. h. bei abgegrenztem Teilnehmerkreis möglich. Bei einigen Stellen bestehen jedoch Überlegungen, den HAVWin-Anschluß als allgemeinen Kommunikationsanschluß auszugestalten. In diesem Fall kann eine Rufnummernüberprüfung im Controller nicht mehr erfolgen. Der LfD hat insoweit empfohlen, die entsprechenden ISDN-Leistungsmerkmale der Telekom

- Rufnummernüberprüfung in der Vermittlungsstelle der Telekom,
- Übermittlung der Nummer des rufenden Teilnehmers,

zu realisieren, um innerhalb der Kommunikations- bzw. Anwendungssoftware eine Identifikationsprüfung zu ermöglichen.

Da die Leistungsmerkmale gezielt für bestimmte ISDN-Dienste eingerichtet werden können, besteht die Möglichkeit der Beschränkung auf den besonderen Bereich der Datenkommunikation; die übrigen Dienste (z. B. Telefonie) bleiben davon unberührt.

Im Rahmen der Protokollierung erfolgt die Aufzeichnung der eingehenden, insbesondere der ungültigen und erfolglosen Anrufe. Die geschilderte Konfiguration ist für den Bereich des Finanzministeriums verbindlich vorgegeben, den übrigen beteiligten Stellen wurde die Übernahme empfohlen. Der LfD beabsichtigt, dies zu überprüfen.

In seiner Stellungnahme hat der LfD darauf hingewiesen, daß mit der geschilderten Protokollierung keine Übermittlungskontrolle nach § 9 Absatz 2 Nr. 6 LDSG verbunden ist, da abgehende Rufe nicht erfaßt werden und sich die Aufzeichnung insgesamt auf die Verbindungsdaten der Kommunikation beschränkt. Um zumindest stichprobenweise eine Überprüfung im Sinne der o. g. Vorschrift zu ermöglichen, hat er empfohlen, in der Anwendung (IRMA) eine entsprechende Protokollierung vorzusehen.

Die Möglichkeiten der Anbindung der mittelbewirtschaftenden Stellen an die AS400-Systeme der Regierungshauptkassen wurden durch das Finanzministerium bereits untersucht. Wegen der geäußerten Sicherheitsbedenken ist kein direkter Zugriff auf das HKR-Verfahren, sondern die Bereitstellung der Bewirtschaftungsdaten in einer „Transferdatenbank" geplant.

Das Verfahren HAVWin läuft derzeit bei allen Ressorts, das Verfahren IRMA wird zur Zeit lediglich bei einigen Stellen im Probebetrieb eingesetzt. Die Beteiligung des LfD an der weiteren Verfahrensentwicklung wurde zugesichert.

21.2.5 Lohn- und Gehaltsabrechnung für die Zivilbeschäftigten der alliierten Streitkräfte Berlin

Auf der Grundlage einer Verwaltungsvereinbarung zwischen der Senatsverwaltung für Finanzen Berlin, dem Ministerium des Innern und für Sport Rheinland-Pfalz sowie dem Bundesminister der Finanzen wurde seit Anfang des Jahres 1994 die Lohn- und Gehaltsabrechnung für die Zivilbeschäftigten der Stationierungsstreitkräfte von Berlin nach Rheinland-Pfalz zum Amt für Verteidigungslasten (AfVL) Kaiserslautern verlagert. Für die Abrechnung kam das Verfahren LOGA der OFD Koblenz zum Einsatz. Die Verlagerung betraf dabei alle wesentlichen Aufgaben der Lohn- und Gehaltsabrechnung; in Berlin verblieben lediglich Erfassungsarbeiten.

Im Zusammenhang mit den sich dabei ergebenden datenschutzrechtlichen Fragen wurde der LfD vom Berliner Datenschutzbeauftragten um die Überprüfung der vorgesehenen technisch-organisatorischen Maßnahmen gebeten; diese erfolgte im November 1993. Dabei ergab sich, daß eine vergleichbare Verlagerung in der Vergangenheit bereits für die Lohn- und Gehaltsabrechnung für Zivilbeschäftigte amerikanischer Streitkräfte in Bayern und Baden-Württemberg erfolgt war; die hierfür getroffenen Sicherungsmaßnahmen wurden auch für das neue Verfahren zugrunde gelegt. Danach wurde für die erforderliche Übertragung der Erfassungsdaten zwischen der Verteidigungslastenverwaltung (VLV) Berlin und der OFD Koblenz eine ISDN-Verbindung mit geschlossener Benutzergruppe eingerichtet. Auf beiden Seiten kamen PC als Endgeräte zum Einsatz; eine direkte Verbindung zum Großrechner der OFD Koblenz wurde nicht eingerichtet, alle Datenübertragungen liefen über den als „Schleusen-PC" konfigurierten Arbeitsplatzrechner im Rechenzentrum der OFD.

Die in Berlin erfaßten Daten wurden zu bestimmten Zeiten durch die OFD Koblenz unter deren Kontrolle aus Berlin abgerufen. Nach der Übertragung auf den PC der OFD Koblenz und einer Überprüfung wurden die Daten zu einem späteren Zeitpunkt von dort auf den Zentralrechner übernommen.

Die (Großrechner-)Anwendung LOGA war über CICS- und RACF-Mechanismen ausreichend abgesichert. Ein Zugriff auf die Daten der Berliner Arbeitnehmer war nur für das AfVL Kaiserslautern möglich und innerhalb von diesem differenziert, entsprechend der Zuständigkeit der jeweiligen Sachbearbeiter.

Mit den getroffenen Maßnahmen wurde eine angemessene Datensicherheit erreicht; das Verfahren war aus datenschutzrechtlicher Sicht nicht zu beanstanden.

21.2.6 Verschlüsselung beim Datenaustausch zwischen den Allgemeinen Ortskrankenkassen und Arbeitgebern

Im Arbeitskreis der Spitzenverbände der Krankenkassen wurden seit geraumer Zeit Möglichkeiten erörtert, die bisherigen Formen der Datenübermittlung (Papier, Datenträgeraustausch) durch eine elektronische Kommunikation abzulösen. In diesem Zusammenhang wurde ein Verfahren zum elektronischen Datenaustausch zwischen den AOKs und den Arbeitgebern entwickelt, das in einem seit Januar 1995 in Hessen laufenden Pilotversuch erprobt wurde. Der Pilotversuch ist mittlerweile abgeschlossen; die Freigabe durch den AOK-Bundesverband ist erfolgt. Das Verfahren soll ab Oktober 1995 auch von der AOK Rheinland-Pfalz unter der Bezeichnung „AOK-Teleservice" eingesetzt werden.

Das Verfahren dient der Ablösung der bisherigen Form des Datenaustauschs auf Papier und damit der Verkürzung der Bearbeitungs- und Laufzeiten und dem Wegfall eines Teils der Schriftgutnachbearbeitung (Druck, Kuvertierung, Frankierung, Versand). Vorgesehen ist die elektronische Übermittlung von DÜVO-Daten, d.h. Verdienstbescheinigungen, Mitteilungen über Vorerkrankungen, Krankengeldbezug, evtl. Ersatzansprüche seitens des Arbeitgebers, Lohnfortzahlungen, laufende Arbeitsunfähigkeit und Mutterschaftsgeld. Vorerst soll zwischen Arbeitgebern und AOK der DFÜ-Austausch von Beitragsnachweisen und DÜVO-Meldungen erfolgen.

Die AOK steht derzeit in Verhandlungen mit mehreren Arbeitgebern, die in einer ersten Phase am DFÜ-Datenaustausch teilnehmen sollen; unter anderem sind das Amt für Verteidigungslasten (Zivilbeschäftige der Streitkräfte) bzw. die OFD Koblenz als lohn- und gehaltsabrechnende Stellen im Gespräch. Als Kommunikationspartner auf AOK-Seite ist dabei das AOK-Rechenzentrum Koblenz vorgesehen, da dort zwischenzeitlich zentral alle Versichertendaten geführt werden. Die langfristigen Planungen laufen darauf hinaus, neben den Arbeitgebern auch mit anderen Stellen einen DFÜ-Austausch durchzuführen und den AOK-Teleservice entsprechend auszudehnen.

Die eigentliche Übermittlung erfolgt über das ISDN-Netz der Telekom unter Einsatz eines von einem Fachunternehmen entwickelten Krankenkassenkommunikationssystems (KKS). Die übermittelten Daten werden dabei auf dem Übertragungsweg wahlweise nach dem RSA- bzw. DES-Verfahren verschlüsselt und mit einer elektronischen Unterschrift versehen. Der Datentransfer ist vom jeweiligen Verarbeitungsrechner bzw. den Anwendungen der AOK und des Arbeitgebers entkoppelt und wird über separate Kommunikationsrechner (PC) abgewickelt. Die zu übertragenden Daten werden auf dem Host gespeichert bzw. selektiert (Lieferdatei) sowie durch Steuerungs- und Verarbeitungsanweisungen ergänzt (Auftragsdatei). Im Anschluß werden die Daten im Kommunikationsrechner zur Verfügung gestellt und zeit- oder ereignisgesteuert übertragen.

Die Anwendung basiert hinsichtlich des Datenaustauschs auf dem OSI FTAM Protokoll. Für Verschlüsselung und digitale Unterschrift kommen der RSA- bzw. DES-Algorithmus zum Einsatz. Schlüsselerzeugung, Verwaltung und Management orientieren sich an den Vorgaben der CCITT-Normen X.500 bzw. X.509 (Directory-Service und Key-Management).

Die für eine asymmetrische Verschlüsselung erforderlichen geheimen und öffentlichen Schlüssel werden dabei dezentral, d. h. jeweils bei der Krankenkasse bzw. beim Arbeitgeber, erzeugt. Der geheime Schlüssel verbleibt (für die Entschlüsselung) bei der jeweiligen Stelle, der öffentliche Schlüssel (für die Verschlüsselung) wird zwecks Zertifizierung und Bereithaltung einer zentralen Instanz zur Verfügung gestellt.

Die Datenschutzbeauftragten haben nach Beratung in einer Arbeitsgruppe zu dem Verfahren Stellung genommen. Die dabei formulierten Empfehlungen wurden auch gegenüber der AOK Rheinland-Pfalz ausgesprochen.

Die Art der Verschlüsselung bzw. die gewählten Verfahren boten aus datenschutzrechtlicher Sicht keinen Grund zur Beanstandung. Einer Klärung bedürfen jedoch die Anforderungen, die an die schlüsselverwaltende Stelle (Clearing- oder Trust Center) als vertrauenswürdigen Dritten zu stellen sind. Bei der Beglaubigung der hinterlegten Schlüssel als Grundlage der Authentizität der übermittelten Daten sowie der beteiligten Stellen kommt dieser Instanz besondere Bedeutung zu (Notarfunktion). Im Rahmen des Pilotversuches wurde diese Funktion von der entwickelnden Firma übernommen. Im Hinblick auf einen späteren Wirkbetrieb ist jedoch zu prüfen, ob diese Funktion auch künftig durch eine private Stelle wahrgenommen werden kann bzw. welche Anforderungen an diese zu stellen sind. Dies gilt im vorliegenden Fall insbesondere im Hinblick auf die mögliche Ausweitung der Einsatzbereiche, ist jedoch insoweit von allgemeiner Bedeutung, als jedes Public-Key-Verfahren bei größerer Anzahl der beteiligten Stellen eines sog. Trust Centers bedarf.

Als verbesserungsbedürftig wurde die Absicherung und das organisatorische Umfeld des Kommunikationsrechners im Pilotversuch angesehen. Für den Einsatz in Rheinland-Pfalz ist in dieser Hinsicht die Installation des Kommunikationsrechners im Sicherheitsbereich des Rechenzentrums sowie die Absicherung über eine Sicherheitssoftware vorgesehen.

Es ist vorgesehen, nach Beginn des Wirkbetriebs örtliche Feststellungen beim Rechenzentrum der AOK zu treffen.

21.2.7 EWKOM

Die im Einwohnerinformationssystem Rheinland-Pfalz (EWOIS) gespeicherten Daten werden außer für melderechtliche auch für weitere einwohnerbezogene Zwecke genutzt (Einschulung, Wahlen, Lohnsteuerkarten, Jubiläen usw.). Für die hierzu erforderlichen Auswertungen der EWOIS-Daten wurden in der Vergangenheit jeweils Aufträge an das Landesrechenzentrum erteilt und von diesem entsprechende Listen erstellt.

Unter der Bezeichnung EWKOM wurde im Auftrag des Gemeinde- und Städtebundes Rheinland-Pfalz ein Verfahren entwickelt, das den Kommunalverwaltungen die Möglichkeit eröffnet, die erforderlichen Auswertungen vor Ort im Dialog selbst zu erstellen.

Zur Klärung der Frage, ob seitens des LfD im bereits angelaufenen Probebetrieb Bedenken erhoben werden müssen, wurden örtliche Feststellungen bei verschiedenen, am Probebetrieb beteiligten Kommunalverwaltungen getroffen.

Dabei ergab sich folgendes:

- EWKOM lief seit September 1994 im Probebetrieb mit Echtdaten bei insgesamt fünf Pilotanwendern. Eine Mitteilung hierüber bzw. die Anmeldung zum Datenschutzregister war nicht erfolgt.

- EWKOM verfügte über eine Möglichkeit der Verzweigung in die für die Erstellung der Anwendung genutzten Entwicklungsumgebung (Application System – AS). Diese ermöglichte die Programmierung eigener Anwendungen, die Angabe von Datenbeständen in der hinter EWKOM stehenden Datenbank (DB2) und die Formulierung von SQL-Datenbankabfragen ohne die durch EWKOM gesetzten Beschränkungen.

- Die Anwendung kann sowohl über die bisherige technische Ausstattung der Meldeämter (Terminals/Drucker) als auch über intelligente Endgeräte (z. B. PC) betrieben werden. In erstem Fall reichen die über das LRZ realisierten Maßnahmen der Zugriffskontrolle aus (TSO-Steuerung, RACF), im zweiten Fall sind, aufgrund der erweiterten technischen Möglichkeiten am Endgerät, zusätzliche Maßnahmen erforderlich (Sicherheitssoftware, Bootschutz, Festplattensperre o. ä.). Diese waren nicht erfolgt.

- Mit Hilfe des Verfahrens waren Auswertungen höchst sensibler Art möglich. So konnten Listen derjenigen Personen erstellt werden, denen das aktive oder passive Wahlrecht aberkannt wurde, oder die Religionszugehörigkeit und die Staatsangehörigkeit als Auswahlkriterien genutzt werden. Teilweise bestehende Verwendungsbeschränkungen von Listen waren dabei nicht ausreichend kenntlich gemacht. Weiterhin bestand die Möglichkeit einer freien Abfrage über die Eingabe mehrerer frei wählbarer personenbezogener Selektionskriterien. Der Umfang der Auswertungsmöglichkeiten bot dabei Anlaß für Zweifel, ob diese für die Aufgabenerfüllung erforderlich waren.

- Aufgrund der nur unzureichenden Protokollierung war die Nutzung von EWKOM nicht nachvollziehbar. Dies wog um so schwerer, als der Einsatz nicht auf den Bereich des Meldeamtes begrenzt war, sondern das Verfahren auch anderen Stellen der Verwaltung zur Verfügung steht.

- Nur durch zentrale Vorgaben (durch Empfehlungen oder eine Musterdienstanweisung) kann bei einem System, das wie das vorliegende zentral entwickelt wurde und zentral zur Verfügung gestellt wird, die Einhaltung weiterer organisatorischer Datenschutzmaßnahmen erreicht werden. Solche Vorgaben fehlten.

Der LfD hat die genannten Mängel gegenüber dem Gemeinde- und Städtebund als Auftraggeber beanstandet. Den dabei ausgesprochenen Empfehlungen wurde zwischenzeitlich weitgehend Rechnung getragen.

So ist künftig u. a. sichergestellt, daß bei freien Abfragen Benutzer, Datum/Uhrzeit, Abfrageparameter (Abfrageart, Menüpunkt, Merkmale) und Darstellungsparameter (Bildschirm-/Druckausgabe, Bildschirm-/Listenaufbau) protokolliert werden. Ähnliches gilt für fest vorgegebene Standardabfragen.

In der Anwendung EWKOM wird eine Auswertungsfunktion zur Verfügung gestellt, über welche auf die Protokolldaten der letzten sechs Monate zugegriffen werden kann. Diese werden in verständlicher Form präsentiert.

Der Umfang der EWKOM-Funktionen kann künftig entsprechend der Zuständigkeit der jeweiligen Verwaltungseinheit vorgegeben werden. Alle Funktionen stehen danach allein dem Meldeamt zur Verfügung. Andere Stellen der Verwaltung erhalten lediglich Zugriff auf

- Statistik- und Gliederungsdaten,
- Summenangaben personenbezogener Auswertungen oder
- personenbezogene (Standard-)Auswertungen nach sachlicher Zuständigkeit (Wahlamt, Kindergartenamt usw.).

Freie Auswertungen stehen außerhalb des Meldeamtes nicht zur Verfügung. Für die Umsetzung dieser Zugriffsbeschränkungen wird EWKOM die Bildung entsprechender Benutzerprofile erlauben, an welchen sich der Maskenaufbau und die Bildschirmmenüs orientieren.

Weiterhin stellt der Gemeinde- und Städtebund für die EWKOM nutzenden Kommunen „Hinweise für den Einsatz von EWKOM“ zusammen. Darin sollen die Verwaltungen auf die datenschutz- und melderechtliche Situation sowie auf die beim Einsatz intelligenter Endgeräte (PC) bzw. beim EWKOM-Zugang über eigene lokale Netze erforderlichen Datensicherungsmaßnahmen hingewiesen werden.

21.3 Landesdaten- und Kommunikationsnetz Rheinland-Pfalz (LDKN)

Mit dem Ziel, eine flächendeckende Kommunikationsinfrastruktur für die rheinland-pfälzische Verwaltung bereitzustellen, wurde mit dem Aufbau eines landesweiten Daten- und Kommunikationsnetzes begonnen. Beginnend mit der Zusammenführung der bislang getrennten Netze der Zentralen Datenverarbeitung der Finanzverwaltung (ZDFin Koblenz), des Landesrechenzentrums Mainz sowie der fachspezifischen Netze der Polizei und des Katastrophenschutzes ist die Bereitstellung eines vom Dateninformationszentrum (DIZ, vgl. Tz. 20.4) betriebenen landesweiten, einheitlichen Daten- und Kommunikationsnetzes beabsichtigt.

Im Hinblick auf das angestrebte umfangreiche Leistungsspektrum des künftigen LDKN (umfassende Sprach-, Bild-, Video- und Datenkommunikation aller angeschlossenen Stellen), die Unterstützung einer Vielzahl von Kommunikationsprotokollen sowie die Schaffung von Übergangsstellen in öffentliche Netze kommt einer ausreichenden Datensicherheit besondere Bedeutung zu. Mit erweiterten technischen Möglichkeiten beim Einsatz der Informations- und Kommunikationstechnik waren in der Vergangenheit regelmäßig neue, mehr oder größere Gefährdungen für das Recht auf informationelle Selbstbestimmung verbunden. Zwar wird in einem ersten Schritt lediglich der „Status quo" auf eine neue Infrastruktur übertragen, im weiteren Aufbau des Netzes werden sich jedoch neue Anwendungen, zusätzliche Kommunikationsmöglichkeiten sowie u. U. neue „Daten-Begehrlichkeiten" ergeben.

Technische Möglichkeiten, d. h. „Wollen" und „Können", dürfen aus der Sicht des LfD jedoch nicht Maßstab der Verarbeitung personenbezogener Daten sein; im Rahmen des Rechts auf informationelle Selbstbestimmung kommt hier nur ein „Dürfen" oder ggf. „Müssen" in Betracht. Diese Kategorien bedürfen beim Aufbau des LDKN jedoch der rechtlichen, technischen, organisatorischen und personellen Konkretisierung.

Der LfD hat daher bereits frühzeitig seine Vorstellungen konkretisiert und darauf gedrungen, bei der Realisierung zusätzliche technische und organisatorische Sicherungsmaßnahmen vorzusehen, um die Ausführung der datenschutzrechtlichen Vorschriften zu gewährleisten. Die Empfehlungen des LfD wurden weitgehend berücksichtigt und fanden ihren Niederschlag u. a. in den Ausschreibungsunterlagen des LDKN.

Weiterhin wurde in Zusammenarbeit mit dem Landesrechenzentrum ein für die Landesverwaltung verbindliches Zugangskontrollkonzept entwickelt, das es – anders als bisher – erlaubt, einen an der Person des Benutzers (d. h. dessen Zuständigkeiten und Befugnissen) orientierten, kontrollierten Netzzugang zu realisieren. Damit wurde der langjährigen Forderung des LfD nach Verbesserung der Zugangsschutzes im Landesdatennetz entsprochen (vgl. u. a. 14. Tb., Tz. 21.5). Die grundlegenden Regelungen hierzu wurden zwischenzeitlich in Form eines Rundschreibens als Benutzungsbedingungen für das landesweite Datenübertragungsnetz im Ministerialblatt veröffentlicht (MinBl. 1994, S. 131). Diese stellen die Grundlage für ein dezentrales Sicherheitsmanagement dar. Es ist jedoch absehbar, daß hier Erweiterungen erfolgen müssen.

Für einige Bereiche sind die Benutzungsbedingungen bereits umgesetzt, für andere muß dies noch erfolgen. Ein Zugang zum Netz darf danach nur für befugte, d. h. vorher bekannte, mit festgelegten Rechten ausgestattete Benutzer möglich sein. Für befugte Netzteilnehmer dürfen sich Zugriffsmöglichkeiten nur im Rahmen ihrer Zuständigkeit und Aufgabenstellung ergeben. Eventuelle Sicherheitslücken bei angeschlossenen Behördenrechnern (z. B. Stadtverwaltung) dürfen nicht dazu führen, daß über diese, quasi als Zwischenstation, ein unbefugter Netzzugang möglich ist.

In einer zweiten Stufe soll die Realisierung eines Zugangskontrollsystems erfolgen, das mit dem Netzwerk-Management-System über eine Schnittstelle verbunden ist. Wenn ein Eingangsknotenrechner erkennt, daß ein Teilnehmer auf das Netz zugreifen möchte, wird der Verbindungsaufbau nur zugelassen werden, wenn der Benutzer verifiziert werden konnte. Jede Anfrage zum Verbindungsaufbau soll protokolliert werden und nur zwischen vorgegebenen Schnittstellen möglich sein.

Vom Grundsatz her ist das künftige LDKN ein internes, d. h. behördenspezifisches Netz auf der Grundlage eigener, d. h. nicht der Öffentlichkeit zugänglicher Übertragungswege. Im Hinblick auf die daraus ebenfalls resultierende datenschutzrechtliche (günstige) Situation ist Überlegungen, gegebenenfalls behördenfremde, private Stellen einzubinden, aus Sicht des LfD mit Zurückhaltung zu begegnen.

Weitere Empfehlungen des LfD waren:

- die wirksame gegenseitige Abschottung der Datenbestände der angeschlossenen Netzteilnehmer u. a. durch den Einsatz moderner Sicherheitsmechanismen, wie z. B. kryptografischer Verfahren. Die Tatsache, daß alle Teilnehmer über ein gemeinsames Netz kommunizieren, darf nicht dazu führen, daß damit die Möglichkeit eines unzulässigen Zugriffs auf die Datenbestände anderer Verwaltungen (z. B. Polizei auf Steuerdaten) eröffnet wird;
- die Transparenz und Nachvollziehbarkeit der Verarbeitung personenbezogener Daten. So muß sich – unter Berücksichtigung personalvertretungsrechtlicher Aspekte – u. a. die Frage beantworten lassen, wer wann über das LDKN auf welche Daten zugegriffen hat, an wen ggf. Daten übermittelt wurden, welche Auswertungen erfolgt sind und ob diese zulässig waren. Die Nutzung des LDKN muß für die angeschlossenen Verwaltungen – und selbstverständlich auch für den LfD – kontrollierbar sein. Dies setzt eine effektive Protokollierung und Dokumentation sowie entsprechende Auswertungsmöglichkeiten im Rahmen der Netzadministration voraus;
- die wirksame Absicherung der Übergangsstellen zu öffentlichen Kommunikationsnetzen (vgl. Kap. 21.6).

Aus der Sicht des LfD ist es zu begrüßen, daß bereits frühzeitig die Möglichkeit bestand, die aus seiner Sicht erforderlichen Maßnahmen konzeptionell weitgehend zu berücksichtigen. Maßstab für die Beurteilung der datenschutzgerechten Ausgestaltung ist jedoch deren praktische Umsetzung im Rahmen des Netzaufbaus.

Beim schrittweisen Aufbau des Netzes muß dabei die Bereitstellung neuer Möglichkeiten der Informationsverarbeitung, der Kommunikation und der Auswertung von Kommunikationsbeziehungen von der Einrichtung entsprechender Datensicherungsmaßnahmen begleitet werden. Etwaige finanzielle oder personelle Engpässe dürfen dabei nicht zu Lasten des Datenschutzes gehen. Weiterhin sollten moderne Möglichkeiten der Datensicherung und deren Umsetzung in der Praxis (z. B. Verschlüsselung) unvoreingenommen beurteilt werden.

Soweit Daten mit besonderer Sensibilität im LDKN übertragen werden (z. B. polizeiliche Daten), sollte aus der Sicht des LfD grundsätzlich die Möglichkeit einer Ende-zu-Ende-Verschlüsselung bestehen. Entsprechende Anwendungen in anderen Bereichen (Informationsverbund Bonn-Berlin [IVBB], Verschlüsselung zwischen AOK und Arbeitgeber vgl. Kapitel 21.2.6, Pretty Good Priv [PGP] im Internet), zeigen, daß derartige Verfahren für die Praxis bereits zur Verfügung stehen.

Ähnliches gilt für die Verbindungsverschlüsselung zur Absicherung der (privaten) Festverbindungen der Telekom zwischen den Knotenrechnern des LDKN. Auch hier stehen marktgängige Lösungen zur Verfügung.

Beim Aufbau und Betrieb des Netzes ist weiterhin zu berücksichtigen, daß der Einsatz solcher Komponenten (HUBs, Router) erfolgt, die ein automatisches Überprüfen der Adressen angeschlossener Endgeräte und ein Filtern der Datenpakete entsprechend der jeweiligen Empfängeradressen ermöglichen. Die Konfiguration der Übertragungswege, d. h. die Festlegung der Netzadressen, an die Datenpakete automatisch weitergeleitet werden (Routing-Einträge), muß über entsprechende Zugangsbeschränkungen (z. B. Paßwort, Chipkarte) abgesichert sein. Der LfD hat dabei wiederholt die Notwendigkeit eines in sich geschlossenen Datenschutz- und Datensicherheitskonzeptes betont.

Der LfD wird den weiteren Aufbau des LDKN mit kritischer Aufmerksamkeit weiter verfolgen.

21.4 Arbeitsgruppe „Verfahrensübergreifende Sicherheitskonzepte" (IT-Grundschutz)

Die durch die Entwicklungen im Bereich der Informationstechnik entstandene heterogene IT-Landschaft besteht aus Systemen mit unterschiedlichen Sicherheitsniveaus. Die häufig praktizierte Aufteilung auf verschiedene Systeme, z. B. Datenhaltung auf einem Großrechner und Datenpräsentation oder Weiterverarbeitung auf einem PC, kann dazu führen, daß die gleichen Daten trotz unveränderter Sensibilität unterschiedlichen Sicherheitsstandards unterliegen.

Aus der Sicht des Datenschutzes wünschenswert sind verfahrensübergreifende Sicherheitskonzepte, die innerhalb einer Behörde oder Organisation einen einheitlichen Sicherheitsmindeststandard und damit die Verarbeitung gleicher Daten unter vergleichbaren Sicherheitsvorkehrungen gewährleisten (vgl. 14. Tb. Tz. 21.8).
Neben der Sicherstellung datenschutzrechtlicher Anforderungen ermöglichen derartige Konzepte auch die Berücksichtigung wesentlicher Interessen der Anwender z. B. hinsichtlich der Verfügbarkeit der Systeme und Integrität der Datenbestände.

Auf Initiative des LfD Rheinland-Pfalz im Interministeriellen Ausschuß für automatisierte Informationsverarbeitung (IMA) hat sich eine Arbeitsgruppe mit den Fragen möglicher Sicherheitsmaßnahmen eines IT-Grundschutzes befaßt. Der LfD Rheinland-Pfalz hat hierzu die aus seiner Sicht grundlegenden Maßnahmen für den Datenschutz und die Datensicherheit im Rahmen eines organisationsweit einheitlichen Mindeststandards formuliert. Dazu zählen im technischen Bereich die

- Vorgabe der Sicherstellung von Identifikations- und Autorisierungsmechanismen auf allen eingesetzten Systemen,
- Vorgabe der Einrichtung von Benutzerprofilen,
- Vorgabe der Berücksichtigung technischer Maßnahmen der Zugangskontrolle als Soll-Kriterien bereits bei der Ausschreibung für IT-Systeme,
- Vorgabe der Nutzung vorhandener Protokollierungs- und Revisionsmöglichkeiten,
- Festlegung eines Verfahrens für die Einrichtung und Nutzung von DFÜ- und Netzanbindungen,
- Festlegungen zum Aufbau und Betrieb lokaler Netze,
- einheitliche Regelungen (und Schaffung entsprechender Möglichkeiten) zur Vernichtung von Schriftgut und Datenträgern,
- Vorgabe der technischen und räumlichen Absicherung zentraler Komponenten,
- Vorgaben über eventuelle Verschlüsselungsmaßnahmen,
- Vorgabe eines behörden- bzw. organisationseinheitlichen Softwarestandards (z. B. für Textverarbeitung, Datenbankanwendungen, Sicherheitssoftware etc.),

im organisatorischen Bereich die

- Hervorhebung der Eigenverantwortung des Anwenders für die Nutzung der Systeme,
- Sicherstellung einer ordnungsgemäßen Datenträgerverwaltung (Kennzeichnung, Ausgabe, Aufbewahrung, Rücklauf, Aussonderung, Vernichtung),
- Festlegungen für den Datenträgereingang, -umlauf und -versand,

- Verbot bzw. Genehmigungspflicht der Nutzung privater Hard- und Software zu dienstlichen Zwecken,
- Verbot der Nutzung dienstlicher Systeme für private Zwecke,
- Festlegung zentraler Verantwortlichkeiten für das Einspielen von Software bzw. Etablierung von Freigabeverfahren,
- Festlegung klarer Verantwortlichkeiten für die Systembetreuung,
- Festlegung von Art und Umfang regelmäßiger Kontrollen,
- Regelungen hinsichtlich Besuchern, Wartungs- und Reinigungspersonal,
- Vorgaben zur Datensicherung

sowie im personellen Bereich die Schärfung des Bewußtseins der Mitarbeiter für bestehende Abhängigkeiten vom IT-Einsatz und der Tatsache einer gestiegenen Sicherheitsproblematik und die Information und Schulung der Systemverantwortlichen und der Anwender.

Zwischenzeitlich wurde vom Bundesamt für die Sicherheit in der Informationstechnik (BSI) das IT-Grundschutzhandbuch mit Maßnahmenempfehlungen für den niedrigen bis mittleren Schutzbedarf veröffentlicht. Aus der Sicht des LfD steht damit für verschiedene Einsatzbereiche ein Maßnahmenkatalog zur Verfügung, der für die Auswahl geeigneter Datensicherungsmaßnahmen im Rahmen eines behördeninternen verfahrensübergreifenden Sicherheitsstandards genutzt werden sollte.

21.5 Absicherung der Zugänge zu öffentlichen Kommunikationsnetzen

Im Berichtszeitraum wurden wiederholt Fragen an den LfD herangetragen, die die Ausgestaltung der Zugänge zu öffentlichen Kommunikationsnetzen betrafen. Hintergrund derartiger Anfragen war neben der beabsichtigten Einrichtung von Fernwartungsanschlüssen dabei zunehmend die Vernetzung von IT-Systemen über den lokalen Bereich hinaus sowie die Inanspruchnahme von IT-Dienstleistungen (z. B. Programmkorrekturen aus Hersteller-Mailboxen, Electronic Mail-Anwendungen).

Soweit Wählleitungsanschlüsse vorhanden waren, handelte es sich überwiegend um Modemanbindungen an das öffentliche (analoge) Telefonnetz; Datex-P-Anschlüsse bestanden nur im Einzelfall. Im Rahmen der Ausstattung mit ISDN-fähigen Telefonnebenstellenanlagen werden jedoch zunehmend auch (digitale) ISDN-Verbindungen zwischen IT-Systemen aufgebaut (vgl. Tz. 21.4.4). Häufig war festzustellen, daß die Kommunikationsanschlüsse nicht durch die öffentlichen Stellen, sondern durch den Lieferanten der Systeme eingerichtet wurden; die Konfigurationseinstellungen wurden dabei nur in Ausnahmefällen dokumentiert und waren den öffentlichen Stellen in der Regel nicht bekannt, damit auch nicht das Ausmaß der Zugriffsmöglichkeiten von außerhalb.

Je nach den Erfordernissen des Kommunikationsanschlusses erlauben bereits Standardlösungen Maßnahmen gegen unbefugte Zugriffe. Die nachfolgenden Empfehlungen zur Absicherung der Netzzugänge bleiben dabei, insbesondere für die Nutzung von Informationsdienstleistungen in öffentlichen Netzen, unabhängig vom Aufbau des Landesdaten- und Kommunikationsnetzes bedeutsam:

Die Vernetzung im Wide Area Bereich (WAN) erfolgt in der Regel über von Dritten bereitgestellte Verbindungen. Soweit die Verbindungen dabei nicht lediglich auf einen bestimmten Teilnehmerkreis beschränkt sind, sondern einer Vielzahl von Teilnehmern prinzipiell offenstehen (z. B. ISDN, Datex-P/J, Internet, Telefonnetze), ergibt sich verstärkt die Notwendigkeit einer ausreichenden Zugangs- und Zugriffskontrolle. Besonderes Augenmerk ist dabei auf die Absicherung der jeweiligen Netzzugänge zu richten; die hier in Betracht kommenden Maßnahmen sind jedoch in hohem Maße abhängig von der Art des Netzzugangs und dessen Nutzung.

Allgemein sollten seitens der öffentlichen Stelle die folgenden Maßnahmen geprüft und ggf. berücksichtigt werden (vgl. § 7 Abs. 2 Nr.4 LDSG):

- Beschränkung lediglich auf abgehende Verbindungen (Dial-Out) bzw. Aufteilung in ein- und abgehende Netzanschlüsse,
- Einrichten eines automatischen Rückrufs (Call-back) unter Verwendung fest vorgegebener Adressen,
- bei nur gelegentlich erforderlicher Kommunikation (z. B. Fernwartung) Aktivierung nur für die Nutzungszeit,
- Einsatz filternder Komponenten zur Ablehnung unberechtigter Adressen und Anmeldungen (Firewalls),
- Trennung von Gateway-Rechner und internem Netz bzw. Host, d. h. keine Nutzdatenspeicherung auf dem Anschlußrechner,
- grundsätzliche Identitäts- und Authentizitätsprüfung externer Anmeldungen (Paßwörter, Challenge-response-Mechanismen usw.),
- Sperren von „Gast"-Kennungen (gast, guest, anonymous, anybody usw.),
- restriktive Ausgestaltung der Zugriffsrechte externer Anmeldungen,

- Verwendung von Anschlußkomponenten, die die Einstellung von Sicherheitsparametern bzw. eine sichere Konfiguration ermöglichen,
- Protokollierung ankommender/abgehender Verbindungen.

Darüber hinaus stellt ein Teil der vorhandenen Kommunikationsdienste Sicherheitsfunktionen bereit. Im Datex-P-Netz sind dies vor allem die Leistungsmerkmale

- „Teilnehmerbetriebsklasse" bzw. „Geschlossene Benutzergruppe" für die Beschränkung der Kommunikation auf eine vorgegebene Gruppe von Anschlüssen/Rufnummern,
- Beschränkung auf abgehende/ankommende Verbindungen,
- Teilnehmerkennung NUI (Network User Identification).

Über weitere Leistungsmerkmale (Anschlußkennung, Benutzerangaben beim Verbindungsaufbau) können beim Verbindungsaufbau Angaben zur Verfügung gestellt werden, die eine Identifikation des rufenden Teilnehmers erlauben, und insoweit für die o. g. Identitätsprüfung genutzt werden können. Ohne zusätzliche Sicherheitsmaßnahmen sollte das Leistungsmerkmal „Gebührenübernahme" bei gespeicherten personenbezogenen bzw. sensiblen Daten nicht in Anspruch genommen werden.

Für weitergehende Sicherheitsanforderungen werden für Datex-P-Anschlüsse sogenannte „Black-Box"-Lösungen angeboten, die unter Verwendung des X.25-Protokolls und kryptografischer Verfahren benutzertransparent eine verläßliche Identifikation/Authentifikation und vertrauliche Kommunikation gewährleisten.

Für ISDN-Anbindungen stehen ähnliche Leistungsmerkmale wie in Datex-P zur Verfügung. Neben einer direkten Begrenzung der zu einem Anschluß zugangsberechtigten Teilnehmer im Rahmen einer geschlossenen Benutzergruppe besteht auch hier die Möglichkeit, beim Verbindungsaufbau zwischen den Teilnehmern vereinbarte Angaben für eine Identifikations- und Authentifikationsprüfung bereitzustellen.

- Geschlossene Benutzergruppe.
- Übermittlung der Nummer des rufenden Teilnehmers, um innerhalb der Kommunikations- bzw. Anwendungssoftware eine Identifikationsprüfung zu ermöglichen.

Soweit die Einrichtung von Euro-ISDN-Anschlüssen erfolgt, weiterhin die Merkmale

- Überprüfung der vom rufenden Teilnehmer übermittelten Rufnummer in der Vermittlungsstelle der Telekom,
- Subadressierung bzw. Teilnehmer-zu-Teilnehmer-Zeichengabe während des Verbindungsaufbaus, für die Durchführung von Identifikations- und Authentisierungsprüfungen innerhalb der Anwendungssoftware.

Aufgrund der besonderen Bedeutung von Kommunikationsverbindungen für die Datensicherheit ist zu gewährleisten, daß diese für die öffentliche Stelle nachvollziehbar dokumentiert sind. Die Nutzung der Anschlüsse, insbesondere die Zugriffe von außerhalb auf die jeweiligen IT-Systeme, sind auf der Grundlage einer entsprechenden Protokollierung stichprobenweise zu überprüfen.

21.6 Wartung/Fernwartung und Datenverarbeitung im Auftrag

21.6.1 Allgemeine Einordnung

Wie ist die mögliche Kenntnisnahme personenbezogener Daten im Rahmen der Wartung und Fernwartung rechtlich einzuordnen? Welche einheitlichen Kriterien können für die Auftragsdatenverarbeitung benannt werden? Welche LfD sind zuständig, wenn Auftragsdatenverarbeitung über Ländergrenzen hinweg stattfindet?

Mit der Klärung bzw. Vertiefung dieser Fragen beauftragte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 1993 einen Gesprächskreis unter Vorsitz des LfD Rheinland-Pfalz.

Das in einer eintägigen Gesprächsrunde Ende Januar 1994 in Mainz erarbeitete Tendenzpapier wurde von der DSB-Konferenz am 10. März 1994 in Potsdam zustimmend zur Kenntnis genommen. In der Gesprächsrunde wurde mehrheitlich die Auffassung vertreten, daß die rechtliche Einordnung von Fernwartung, Wartung und Systembetreuung als Auftragsdatenverarbeitung die größten Möglichkeiten bietet, umfassende technische und organisatorische Sicherungsmaßnahmen durchzusetzen.

Soweit Datenverarbeitungsaufträge an nichtöffentliche Stellen vergeben werden, können sich in bestimmten Bereichen Einschränkungen der Zulässigkeit ergeben. Hier sind mögliche verfassungsrechtliche Hindernisse zu nennen, wenn es u. a. um die gänzliche Übertragung eines Landesverwaltungsnetzes geht. Es können aber auch spezialgesetzliche Vorgaben wie beim Krankenhausgesetz entgegenstehen. Einschränkungen können sich ebenso aus besonderen Berufs- und Amtsgeheimnissen ergeben. Im Einzelfall ist es nicht ausgeschlossen, daß diese Überlegungen auch dann zum Zuge kommen, wenn es um die Auftragsdatenverarbeitung durch öffentliche Stellen geht.

Um bei der Vertragsgestaltung flexibel zu sein, sollte im Sinne des Datenschutzes unterschieden werden zwischen gesetzlichen Vorgaben, zwingenden Geboten und sachspezifischen Empfehlungen. Hierzu wurde eine Liste „Elemente einer Vertragsgestaltung" erarbeitet.

Die länderübergreifende Kontrolle öffentlicher Auftragnehmer sollte von den örtlich zuständigen LfD in Amtshilfe durchgeführt werden.

21.6.2 Anforderungen bei der Durchführung der Wartung/Fernwartung

Die Anforderungen des § 9 Absatz 1 LDSG hinsichtlich der technisch-organisatorischen Maßnahmen des Datenschutzes sind auch bei einer Fernwartung zugrunde zulegen, insbesondere sind dabei folgende Punkte zu berücksichtigen:

- Die speichernde Stelle hat sicherzustellen, daß eine Fernwartung nur im Einzelfall, mit ihrem Einverständnis und unter ihrer Aufsicht erfolgen kann. Hierzu ist ein Verfahren zur Einleitung einer Fernwartung (Benachrichtigung, Freischaltung) zu vereinbaren. Der Wartungsvorgang muß durch die speichernde Stelle jederzeit abgebrochen werden können.
- Es muß kontrollierbar sein, welche Arbeiten im Rahmen der Fernwartung durchgeführt werden, insbesondere welche Zugriffe auf personenbezogene Daten erfolgen.
- Die Fernwartungsarbeiten sind unter einer separaten, über Identifikations- und Authentisierungsmechanismen (Paßwort) geschützten Benutzerkennung durchzuführen; hierbei ist auch der Kreis des autorisierten Wartungspersonals festzulegen. Solange Fernwartungszugriffe nicht erforderlich sind, sollte die Benutzerkennung deaktiviert sein. Die Zugriffsmöglichkeiten sind auf das für die Durchführung der Wartungsarbeiten erforderliche Maß zu beschränken, insbesondere gilt dies für Systemverwalterprivilegien und den Zugriff auf personenbezogene Daten.
- Soweit die Fernwartung über Wählleitungsanschlüsse erfolgt, muß der endgültige Verbindungsaufbau stets durch die speichernde Stelle erfolgen; in Betracht kommt hier beispielsweise der automatische Rückruf über eine fest vorgegebene Nummer der Fernwartungsstelle. Diese Konfigurationsdaten sind vor unzulässigen Veränderungen zu schützen, beispielsweise durch den Einsatz paßwortgesicherter Anschlußmodems. Da die Wählleitungsanschlüsse im Rahmen der Fernwartung nur in bestimmten Fällen benötigt werden, sollte in der übrigen Zeit der Anschluß physikalisch von der Datenverarbeitungsanlage getrennt sein, um unzulässige Zugriffsversuche auszuschließen (vgl. auch Tz. 21.6).
- Um in Zweifelsfällen eine Revision zu ermöglichen, sind die Aktivitäten im Rahmen der Fernwartung (Zeitpunkt, Dauer, Art der Fernwartungszugriffe) in entsprechenden Protokolldateien festzuhalten und diese für die Dauer eines Jahres aufzubewahren.
- Die Übernahme neuer Programmversionen sollte grundsätzlich nicht im Rahmen der Fernwartung erfolgen. Soweit im Einzelfall unvermeidlich, ist die Übernahme zu dokumentieren und die Integrität der übernommenen Software durch geeignete Maßnahmen sicherzustellen.
- Der zugrundeliegende Wartungsvertrag (vgl. Datenverarbeitung im Auftrag) sollte Regelungen hinsichtlich Art und Umfang zulässiger Wartungsarbeiten, über die Weitergabe von im Rahmen der Wartung offenbarten personenbezogenen Daten sowie die Verpflichtung zur Beachtung der für den Auftraggeber geltenden datenschutzrechtlichen Bestimmungen enthalten.

21.7 Computerviren auf Versanddisketten

Unabhängig von der zum Teil spektakulären Presseberichterstattung zu entsprechenden Vorfällen boten auch im zurückliegenden Berichtszeitraum Vorkommnisse in der rheinland-pfälzischen Landes- und Kommunalverwaltung Anlaß, darauf hinzuweisen, daß es sich bei der Gefährdung durch Computerviren nicht lediglich um ein theoretisches Phänomen handelt, das die Besorgnis von Datenschützern auslöst, sondern um eine Beeinträchtigung der Datensicherheit, der in der täglichen Praxis begegnet werden muß.

In einem Fall wurden von einer obersten Landesbehörde für den Versand erstellte Disketten mangels ausreichender Vorsorge mit einem Computervirus infiziert und in diesem Zustand an andere öffentliche Stellen weitergegeben. Aufgrund einer sofort nach der Aufdeckung der Infektion erfolgten Rückrufaktion war der Schaden jedoch auf ein Mindestmaß zu begrenzen. Durch entsprechende Vorsorgemaßnahmen beim Umgang mit Computerdisketten wäre eine derartige „Infektion von Amts wegen" jedoch vermeidbar gewesen.

Im konkreten Fall handelte es sich um einen Virus aus der Familie der Boot-Viren („Parity-Boot-Virus"), der nach Ablauf einiger Zeit zum Stillstand des Systems führt. Aufgrund der Infektion zentraler Systembereiche kann eine Bereinigung im Einzelfall aufwendig und unter Umständen mit Datenverlusten verbunden sein. Da abhängig vom Virentyp das Ausmaß eines möglichen Schadens – von Beeinträchtigungen der Funktion von Datenverarbeitungssystemen bis hin zu einem totalen Datenverlust – auch von der Sorgfalt der Diskettenverarbeitung beim Empfänger abhängt, hat der LfD den Ministerien und den kommunalen Spitzenverbänden Vorsorgemaßnahmen empfohlen.

Danach sind bei der Verarbeitung von Datenträgern, insbesondere beim Einsatz von Arbeitsplatzrechnern, verfahrensmäßige Schritte vorzusehen, die eine Beeinträchtigung durch Computerviren verhindern, zumindest aber wesentlich erschweren. Im Rahmen des § 9 Absatz 1 LDSG zählen dazu insbesondere folgende Vorkehrungen:

- Einrichtung eines organisatorischen Verfahrens für die Erstellung und Behandlung von Versanddisketten,
- Einsatz fabrikneuer bzw. formatierter Disketten als Versanddatenträger,
- Ausstattung des für die Diskettenerstellung eingesetzten DV-Systems mit einer Sicherheitssoftware zur Gewährleistung einer ausreichenden Zugriffskontrolle,
- Ausstattung des DV-Systems mit einem Virensuch- bzw. einem residenten Virenschutzprogramm,
- eindeutige Kennzeichnung der verwendeten Datenträger,
- Virenprüfung der erstellten Disketten vor dem Versand,
- Nutzung eines ggf. vorhandenen Schreibschutzes der Datenträger,
- Dokumentation der Erstellung und des Versandes.

Außer bei der Erstellung von Versanddatenträgern sollten vergleichbare Maßnahmen auch für eingehende Datenträger vorgesehen werden. Unabhängig von der insbesondere bei größeren Organisationseinheiten bestehenden Schwierigkeit, die an den verschiedenen Stellen eines Hauses eingehenden Datenträger einem geordneten Verfahren zuzuführen, sollte deren organisatorische Behandlung geregelt werden. Hierbei ist insbesondere für empfangene Disketten vor einer weiteren Verarbeitung die Möglichkeit einer – gegebenenfalls dezentralen – Virenprüfung vorzusehen.

21.8 Protokollierung und Dokumentation

Bei örtlichen Prüfungen waren wiederholt im Bereich der Protokollierung und der Dokumentation von IT-Systemen Defizite festzustellen. Die Komplexität heutiger IT-Lösungen erschwert es zunehmend, die Nutzung der Systeme nachzuvollziehen. Beide, Protokollierung und Dokumentation, sind unverzichtbare Elemente einer wirksamen Kontrolle; sie dienen jedoch nicht allein der Überwachung datenschutzrechtlicher Vorschriften, sondern ebenso der öffentlichen Stelle im Hinblick auf einen ordnungsgemäßen Betrieb der IT-Systeme und – als nicht zu unterschätzender Gesichtspunkt – der möglichen Entlastung befugter Mitarbeiter bei Manipulations- oder Offenbarungsvorwürfen.

Im Berichtszeitraum hat sich der LfD auf entsprechende Anfragen hin wiederholt zu dem aus seiner Sicht erforderlichen Umfang einer Protokollierung und der Dokumentation von IT-Systemen geäußert.

Unter Protokollierung ist danach im datenschutzrechtlichen Sinn die Erstellung manueller oder automatisierter Aufzeichnungen bei der Verarbeitung personenbezogener Daten (s. § 3 LDSG) und der Verwaltung und Betreuung von IT-Systemen zu verstehen. Sie dient damit insbesondere der Nachvollziehbarkeit und Beweissicherung.

In einigen Fällen wird sie gesetzlich ausdrücklich gefordert (z. B. § 9 Abs. 2 Nr. 6 und 7, § 7 [4] LDSG), in anderen Fällen ergibt sie sich aus der Art der zu schützenden Daten und dem Erfordernis, geeignete technisch-organisatorische Schutzmaßnahmen zu realisieren.

Aufgrund der Aufzeichnungen in Protokollen sollten sich Fragen („Wer hat wann was veranlaßt bzw. worauf zugegriffen?") beantworten oder Systemzustände („Wer hatte von wann bis wann welche Zugriffsrechte?") ableiten lassen.

Die Dokumentation umfaßt die (nachvollziehbare) Beschreibung festgelegter Verfahrensweisen, Systemkonfigurationen u. a., um im Wege eines Soll-/Ist-Vergleichs etwaige Abweichungen erkennen zu können (z. B. Benutzerliste, Dokumentation der Zugriffsprofile, Übersicht der Kommunikationsanschlüsse an öffentliche Netze, Dokumentation der Systemkonfiguration und -parameter).

Vor diesem Hintergrund empfiehlt es sich, folgende Vorgänge in Abhängigkeit von der Sensibilität der Verfahren und Daten bei der Verwaltung und Betreuung von IT-Systemen vollständig oder selektiv zu protokollieren:

- Einstellung und Veränderung von Systemparametern,
- Änderungen der Systemkonfiguration,
- Einrichten, Löschen und Sperren der Zugriffsrechte,
- Verwaltung von Zugriffsrechten,
- Einspielen und Änderung von Software,
- Änderungen der Dateiorganisation,
- Durchführung von Datensicherungen (Back-up/Restore).

Geht man von wirksamen Verfahren der Authentifizierung (Paßwörter o. ä.) und sachgerechten Zugriffsbefugnissen aus, kommt der Protokollierung aller „auffälligen Vorgänge", insbesondere bei der Benutzung von IT-Systemen eine zentrale Bedeutung zu. Benutzer ist dabei auch der Systemverwalter. Auffällig sind alle jene Vorgänge, die bei ordnungsgemäßer Nutzung nicht oder nur in Ausnahmefällen auftreten. Beispiele sind:

- Anmeldeversuche mit ungültigen Benutzerkennungen,
- wiederholte Anmeldeversuche mit ungültigen Paßworten,
- Anmeldungen zu „unüblichen" Zeiten,
- Anmeldungen unter Systemverwalterkennungen,
- Verstöße gegen Zugriffsregelungen,
- zurückgewiesene Programm- und Funktionsaufrufe.

In den meisten Fällen werden die Ursachen hierfür in irrtümlich fehlerhaften Eingaben o. ä. zu suchen und somit leicht erklärbar sein; wichtigster Gesichtspunkt ist jedoch, daß derartige Vorfälle überhaupt erkennbar werden und damit den Fällen, die auf anderen Ursachen beruhen, begegnet werden kann.

Bei der Verarbeitung personenbezogener Daten, insbesondere bei der Eingabe und Übermittlung, ist ebenfalls eine Protokollierung vorzusehen. Zu protokollieren sind dabei vor allem die

- Eingabe von Daten (§ 9 Abs. 2 Nr. 7 LDSG),
- Datenübermittlungen (§ 9 Abs. 2 Nr. 6 und § 7 Abs. 4 LDSG),
- Benutzung automatisierter Abrufverfahren (§ 7 Abs. 4 LDSG),
- Löschung von Daten,
- Programm- oder Funktionsaufrufe sowie grundsätzlich
- Benutzerkennung und Datum/Uhrzeit.

Protokolldaten sind personenbezogene Daten. In erster Linie besteht ein Personenbezug zu den Nutzern der automatisierten Datenverarbeitung. In vielen Fällen lassen Protokolle außerdem Rückschlüsse auf Daten von Betroffenen zu; damit gelten die datenschutzrechtlichen Anforderungen auch für Protokolldaten. Die Notwendigkeit eines ausreichenden Manipulationsschutzes ergibt sich schon aus dem Nachweiszweck von Protokolldateien (Beweissicherung).

Hinsichtlich ihrer Nutzung unterliegen Protokolldaten einer engen Zweckbindung. Sie dürfen grundsätzlich nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden. Eine anderweitige Nutzung ist lediglich zur Abwehr erheblicher Gefährdungen der öffentlichen Sicherheit zulässig (§ 13 Abs. 5 LDSG).

Ausdrücklich untersagt ist die Nutzung zu Zwecken der Verhaltens- oder Leistungskontrolle (§ 31 Abs. 5 LDSG).

Die Aufbewahrungsdauer der Protokolle richtet sich, da es sich um personenbezogene Daten handelt, nach den allgemeinen Löschungsregeln der Datenschutzgesetze, d. h. nach der Erforderlichkeit und den Erfordernissen einer ordnungsgemäßen Dokumentation (§ 19 Abs. 2 LDSG).

Eine exakte Bestimmung des Zeitraums der Erforderlichkeit für Protokolle, deren Auswertung zeitlich nicht konkretisiert ist, ist nicht möglich. Als Anhaltspunkte können dienen:

- die Wahrscheinlichkeit, daß Unregelmäßigkeiten (noch) offenbar werden können und
- die Möglichkeit, die Gründe von Unregelmäßigkeiten anhand der Protokolle und anderer Unterlagen aufdecken zu können.

Erfahrungsgemäß sollte eine Aufbewahrungsdauer von einem Jahr nicht überschritten werden. Soweit Protokolle zum Zwecke gezielter Kontrollen angefertigt werden, ist eine kürzere Speicherungsfrist vorzusehen; in der Regel reicht dabei eine Aufbewahrung bis zur tatsächlichen Kontrolle aus.

Protokollierung sollte nicht verwechselt werden mit einem „Monitoring", bei welchem eine permanente und umfassende Überwachung aller (System-)Aktivitäten erfolgt. Dies kann beim Betrieb von Rechenzentren oder besonderen IT-Verfahren erforderlich sein.

Protokollierung sollte auch keine „Datenfriedhöfe" erzeugen, sondern sie muß ergänzt werden durch eine regelmäßige, stichprobenartige oder anlaßbezogene Auswertung. Einer Begrenzung des Protokollierungsumfangs auf das für eine Auswertung notwendige und sinnvolle Maß ist damit ebenfalls Beachtung zu schenken.

21.9 Dienstanweisungen

Nach § 9 Abs. 5 LDSG muß jede öffentliche Stelle die technischen und organisatorischen Maßnahmen in einer Dienstanweisung festlegen. Diese Verpflichtung gilt nicht nur für die automatisierten Verfahren, sondern auch für die herkömmliche Datenverarbeitung, also z. B. für die Aktenführung oder für die Verarbeitung personenbezogener Daten in nichtautomatisierten Dateien (z. B. Karteien).

Die technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes können nicht generell festgelegt werden, denn der Aufwand für solche Maßnahmen muß unter Berücksichtigung der Art der zu schützenden personenbezogenen Daten und ihrer Verwendung in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen. Es kommt also ganz entscheidend auf die Situation vor Ort, insbesondere Art und Umfang der automatisierten Datenverarbeitung, die zu verarbeitenden Daten, die eingesetzte Hard- und Software, die äußere und innere Gebäudesicherheit usw. an.

Aus der Praxis wurde der Wunsch an den LfD herangetragen, eine Musterdienstanweisung auszuarbeiten und zur Verfügung zu stellen. Diesem Wunsch konnte aus den vorgenannten Gründen nur insoweit entsprochen werden, als Regelungsbeispiele für eine Dienstanweisung zusammengefaßt wurden. Der Verwaltung muß es überlassen bleiben, diese Regelungsbeispiele in geeigneten Fällen in eine Dienstanweisung nach § 9 Abs. 5 LDSG zu übernehmen und sie unter Berücksichtigung der örtlichen Gegebenheiten zu ergänzen.

Die Regelungsbeispiele werden in der Schriftenreihe des LfD „Informationen zum Datenschutz", Heft 2, veröffentlicht.

22. Öffentlich-rechtliche Wettbewerbsunternehmen, Sparkassen

22.1 Wahlfreiheit für Sparkassenkunden, welche Filiale auf ihre Kontendaten zugreifen kann

Auch in großen Sparkassenorganisationen können – unabhängig vom konkret geäußerten Willen der Kunden – die Schalterbediensteten jeder Filiale auf bestimmte Informationen über die Girokonten und die Sparkonten nahezu aller Kunden per Bildschirm zugreifen. Technisch jedenfalls gibt es hier keine wirksame Zugriffsbeschränkung. Auf dieses Problem ist der LfD durch die Eingaben verschiedener Bürger aufmerksam geworden.

Das hier bestehende Problem wird auch nicht dadurch geringer oder ist auch nicht deshalb zu vernachlässigen, weil die Sparkassen regional beschränkte Zuständigkeitsbereiche hätten. Nicht nur aufgrund von Sparkassenfusionen, sondern auch aufgrund langer Traditionen bedienen einige Sparkassen räumlich weit ausgedehnte Bereiche. Gerade aber auch im Bereich kleiner überschaubarer ländlicher Gemeinden ist es häufig das Problem der persönlichen Bekanntschaft mit den Bediensteten der örtlichen Sparkassenfiliale, das das Bedürfnis hervorruft, dem Sparkassenmitarbeiter, der in der Nachbarschaft wohnt, nicht unbedingt alle Informationen über die finanziellen Verhältnisse zur Verfügung zu stellen, sondern die Zugriffsmöglichkeiten etwa auf die Hauptstelle in der nächsten Stadt zu beschränken.

Das hier bestehende Problem wird in seiner grundsätzlichen Bedeutung durch einen Vergleich mit dem öffentlichen Bereich deutlich:

Jeder Steuerpflichtige des Landes Rheinland-Pfalz wäre sicherlich empört, wenn nicht nur das für ihn zuständige Finanzamt, sondern auch die umliegenden Finanzämter aus Gründen der „Bürgerfreundlichkeit" Zugriff auf seine Steuerdaten hätten, damit er – bei Bedarf – auch die Nachbarfinanzämter um Rat und Auskunft bitten könnte. Die technisch abgesicherte räumliche Beschränkung der Zugriffsbefugnisse innerhalb des öffentlichen Bereichs auf die Stelle, die für die Belange des Bürgers zuständig ist, ist selbstverständlich.

Grundsätzlich anderes kann auch nicht für private Unternehmen oder öffentliche Stellen, die am Wettbewerb teilnehmen, gelten, wenn sie ihre Tätigkeit an verschiedenen Orten ausüben. Auch hier ist jeweils der Grundsatz der Erforderlichkeit das maßgebliche Kriterium, unabhängig davon, in welcher gesetzlichen Regelung im einzelnen der rechtliche Geltungsgrund dieses Verfassungsgrundsatzes gesehen wird.

Zu betonen ist, daß das datenschutzrechtliche Anliegen keineswegs darauf gerichtet ist, Servicemöglichkeiten, die die Sparkasse im Interesse ihrer Kunden anbietet, zu beschränken oder zu behindern. Das Gegenteil ist der Fall: Die Anregung des LfD zielt darauf, dem Kunden eine Wahlmöglichkeit einzuräumen, durch welche Zweigstellen er bedient werden will. Dies könnte praktisch etwa in folgender Weise geschehen:

- Bei der Kontoeröffnung wird der Kunde darüber befragt, ob er einem Zugriff aller Filialen auf seine Daten zustimmt. Wenn er dies ablehnt, wäre die ihn betreuende Filiale im Datensatz festzulegen. Dazu könnte die bereits jetzt im Datensatz enthaltene Rubrik „Betriebsstellennummer" genutzt werden. An diese Betriebsstellennummer könnte grundsätzlich der örtliche Zugriff geknüpft werden.

– Denkbar wäre auch, dem Kunden anzubieten, daß in allen Filialen ad hoc ein Zugriff auf seine Daten bei Anfragen eröffnet wird, wenn er seine Scheckkarte bei sich trägt. Dann könnte der Kundenberater unter Nutzung der Scheckkarte eine Freigabe bewirken. Ein Modell für den überregionalen Zugriff unter Verwendung der Krankenversichertenkarte wird derzeit im Bereich der allgemeinen Ortskrankenkassen diskutiert.

Zur Vermeidung von Mißverständnissen ist darauf hinzuweisen, daß mit dieser Forderung keinesfalls beabsichtigt ist, den Zugriff zentraler Funktionsbereiche auf Kundendaten einzuschränken: Soweit zentrale Funktionsbereiche den umfassenden Zugriff auf Datenbestände aller Kunden benötigen, ist dies streng von der hier in Rede stehenden Frage der örtlichen Zugriffsbeschränkung verschiedener Betriebsstellen zu unterscheiden.

Außerdem ist darauf hinzuweisen, daß für die Sparkassenmitarbeiter bezüglich der Informationen über die sie selbst betreffenden Konten spezielle technische Zugriffsbeschränkungen selbstverständlich sind.

Die Sparkassen haben darauf verwiesen, daß durch folgende Maßnahmen sichergestellt sei, daß ihre Mitarbeiter keine unberechtigten Abrufe aus bloßer Neugier oder sonst unzulässigen Motiven vornehmen:

- ein bestimmter Prozentsatz aller Abrufe werde dadurch kontrolliert, daß der Datenzugriff nur möglich sei, wenn ein Kollege mitwirke und den Abruf freigebe;
- die Abrufe würden umfassend protokolliert, so daß bei einem Mißbrauchsverdacht völlige Aufklärung möglich sei;
- ein Verstoß gegen die Anordnungen habe grundsätzlich erhebliche dienstrechtliche Folgen (im Regelfall Kündigung).

Angesichts dieser Umstände hat der LfD von einer Beanstandung des derzeitigen Verfahrens abgesehen. Er hält dennoch vor dem Hintergrund der sich ständig weiterentwickelnden Technik (besonders im Zusammenhang mit der elektronischen Geldbörse) und der dadurch bedingten Neuausstattung der Sparkassen mit Informationstechnik seine Forderung aufrecht, bei deren Erfüllung die Datenzugriffe jedenfalls erheblich weniger mißbrauchsanfällig wären.

22.2 Geldwäschegesetz

22.2.1 Speicherung in staatsanwaltschaftlichen Dateien

Der Vollzug des Geldwäschegesetzes hat aus datenschutzrechtlicher Sicht gewisse Probleme verursacht. Die Fragen der Rechte des Betroffenen in diesem Zusammenhang hat der LfD im 14. Tätigkeitsbericht ausführlich geschildert. Vor dem Hintergrund der jetzt vorliegenden praktischen Erfahrungen hat sich bestätigt, daß von diesem Gesetz in großer Zahl Personen betroffen sind, denen kein strafrechtlicher Vorwurf zu machen ist: Im Jahr 1994 hat es 3 282 Verdachtsanzeigen gegeben. Daraufhin sind 2 738 Ermittlungsverfahren eingeleitet worden, aber nur in 4 % aller Verfahren hat ein konkreter Verdacht der Geldwäsche vorgelegen (so jedenfalls die in der Presse bekanntgewordenen Statistiken, vgl. Handelsblatt vom 28. August 1995).

Grundsätzlich werden die Verdachtsanzeigen nach dem Geldwäschegesetz von den Strafverfolgungsbehörden als Strafanzeigen angesehen und dementsprechend in das Js-Register eingetragen. Künftig bedeutet dies, daß diese Information bundesweit für alle Staatsanwaltschaften abrufbar ist (im staatsanwaltschaftlichen Informationssystem SISY, s. dazu oben Tz. 7.3). Die Datenschutzbeauftragten der Länder sind deshalb der Auffassung, daß eine entsprechende Eintragung in ein gesondertes Register erfolgen sollte, das keine überregionale Abrufbarkeit zur Folge hat.

22.2.2 Wann darf der Personalausweis fotokopiert werden?

Das Geldwäschegesetz hat noch andere für den Bürger zum Teil nicht verständliche Folgen: Die Banken und Sparkassen sind aufgrund einer Empfehlung des Bundesaufsichtsamtes für das Kreditwesen (zuletzt vom 26. Oktober 1994 – V 94) dazu übergegangen, bei allen Kontoeröffnungen, aber auch bei der Einräumung von Vollmachten die Personalausweise der Beteiligten zu fotokopieren. Dies geschieht unter Berufung auf das Geldwäschegesetz. Dies ist rechtlich unzutreffend: Zwar sieht das Geldwäschegesetz vor, daß in den Fällen, in denen die Kunden zu identifizieren sind, die Identifizierung im Regelfall durch eine Fotokopie des Personalausweises zu erfolgen hat (§ 9 Abs. 1 Satz 2 GWG). Nur bestimmte Transaktionen jedoch lösen die Pflicht zur Identifikation aus (Bartransaktionen ab 20 000 DM und vergleichbare Handlungen). Die genannte Verfahrensweise der Banken und Sparkassen ist weder durch das Geldwäschegesetz noch durch das allgemeine Datenschutzrecht (§ 28 Abs. 1 BDSG) gedeckt (vgl. auch Urteil des BGH vom 18. Oktober 1994, Az.:XI ZR 237/93, veröffentlicht in der Zeitschrift DuD 95, 363).

Der LfD hat den Sparkassen- und Giroverband hierauf aufmerksam gemacht.

22.3 Installation von Videokameras im Außenbereich

Eine Sparkasse hatte geplant, den Bereich vor ihrem Eingang ständig mit einem Videogerät in der Form zu überwachen, daß von der gegenüberliegenden Straßenseite aus laufend Aufnahmen des Trottoirs gefertigt werden sollten, die erst nach einer gewissen Zeit (etwa 24 Stunden) wieder gelöscht werden sollten, wenn keine Straftat mit Hilfe dieser Bilder aufzuklären war.

Dieses Verfahren hat der LfD als unvereinbar mit datenschutzrechtlichen Vorschriften abgelehnt.

Rechtsgrundlage der Prüfung ist zunächst das BDSG (gem. § 2 Abs. 3 LDSG). Für den hier zu beurteilenden Vorgang greift es jedoch nicht ein: Bild und Tonträger sind zwar als Akten im Sinne des Bundesdatenschutzgesetzes anzusehen (§ 3 Abs. 3 BDSG). Die Vorschriften des BDSG für die Datenverarbeitung privater Stellen gelten aber nicht für Daten in Akten (§ 27 Abs. 2 BDSG) und damit auch nicht für die Erstellung von Videoaufzeichnungen durch Sparkassen.

Die ohne Einwilligung erfolgende Fertigung von Videoaufnahmen greift aber in das allgemeine Persönlichkeitsrecht der Betroffenen ein. Jeder darf grundsätzlich selbst und allein darüber befinden, ob und wie er durch eine Abbildung erfaßt wird. Für den Tatbestand der Verletzung des Persönlichkeitsrechts durch die Fertigung von Abbildungen ist es allerdings grundsätzlich bedeutsam, zu welchem Zweck die Abbildung gemacht worden ist; erst die Widerrechtlichkeit der Fertigung einer Abbildung führt dazu, daß von einem Eingriff in das Persönlichkeitsrecht gesprochen werden kann (so jedenfalls das OLG Hamm, Urteil vom 2. April 1987, NJW-RR 1988, 425; vgl. auch BGH vom 25. April 1995, NJW 95, 1955). Das Recht am eigenen Bild gem. § 22 KunsturhebG greift nicht ein, weil dieses nur vor der unzulässigen Verbreitung, nicht aber vor der ungenehmigten Erstellung von Abbildungen schützt. Die generelle Aufzeichnung aller Passanten jedenfalls ohne konkreten Anlaß ist durch Strafverfolgungszwecke nicht gerechtfertigt, ein Überwiegen der Interessen am Fertigen solcher Aufzeichnungen ist nicht feststellbar.

Aufgrund dieser Überlegungen hat die Sparkasse vorgeschlagen, erst mit dem Auslösen von Alarm gleichzeitig eine Videokamera im Außenbereich der Sparkasse zu aktivieren.

Der Zweck, den Täter einer Straftat zu identifizieren, rechtfertigt es selbstverständlich, Aufnahmen von diesem Täter zu fertigen (so das Kammergericht, NJW 1980, 894; ablehnend allerdings Schwerdtner, in Münchner Kommentar, 2. Auflage, § 12 RdNr. 173; offengelassen durch OLG Hamm, Urteil vom 2. April 1987, NJW-RR 1988, 425; für die Zulässigkeit der Fertigung von Fotografien zu Beweiszwecken insbesondere auch Helle, Jürgen, Besondere Persönlichkeitsrechte im Privatrecht, Tübingen 1991, S. 78 ff., 204 f.).

In einer Situation, in der der Täter nur zusammen mit anderen Personen aufgenommen werden kann, rechtfertigt der Zweck der Straftatenverfolgung auch – im Rahmen der Verhältnismäßigkeit – das Fertigen von Aufnahmen anderer, unbeteiligter Personen.

Vor diesem Hintergrund wäre also das Verfahren, Videoaufnahmen von dem Bürgersteig vor der Sparkasse nach dem Auslösen des Alarms zu fertigen, dann mit dem allgemeinen Persönlichkeitsrecht vereinbar, wenn die Dauer der Aufnahmen auf das in diesem Zusammenhang Erforderliche beschränkt würde und wenn die Aufnahmen dann gelöscht würden, wenn diese für Strafverfolgungszwecke nicht mehr erforderlich wären.

Der LfD hat dementsprechend gegen dieses Verfahren keine Einwendungen erhoben.

22.4 Telefonische Datenübermittlungen über den Kontostand durch eine Sparkasse

Aus einem konkreten Anlaß wollte ein Sparkassenkunde Antwort auf folgende Fragen:

a) Darf ein Geldinstitut die Angabe telefonisch bestätigen, daß ein bestimmter Betrag zu einem bestimmten Datum eingegangen ist, wenn vom Anrufer der Betrag und das Datum genannt werden?

b) Besteht grundsätzlich ein Schadensersatzanspruch, wenn einem Unbefugten telefonisch Auskunft erteilt wurde?

c) Kann dann mit Aussicht auf Erfolg ein Strafverfahren eingeleitet werden?

Der LfD hat diese Fragen wie folgt beantwortet:

Wenn tatsächlich derjenige, der eine Überweisung veranlaßt hat, anruft und nach der Ausführung der Überweisung fragt, läge in der Antwort an den Auftraggeber der Überweisung keine Offenbarung von Daten und auch keine Übermittlung. Voraussetzung ist also, daß die telefonische Anfrage tatsächlich von dem Urheber der Überweisung ausgeht. Dies ist bei telefonischen Kontakten grundsätzlich zweifelhaft. In solchen Fällen ist im Regelfall das Rückrufverfahren, und zwar über die jeweilige Zentrale der Institution, der anzugehören der Anrufer vorgegeben hat, zu wählen.

Auch in der Bestätigung eines Zahlungsvorganges gegenüber einem Dritten liegt nämlich eine Datenübermittlung, selbst wenn dieser über den Zahlungsvorgang grundsätzlich bereits informiert war: Die Bestätigung hat dann als solche einen eigenen Informationswert. Wenn dies nicht der Fall wäre, würde eine entsprechende Anfrage nicht erfolgen.

Die Vorwerfbarkeit des Fehlverhaltens des Sparkassenmitarbeiters im vorliegenden Fall war jedoch gering, da weder die Brisanz der Information für den auskunftgebenden Bediensteten noch auch ein Anlaß für ein besonderes Mißtrauen aus sonstigen Gründen erkennbar war.

Grundsätzlich ist auf öffentlich-rechtliche Kreditinstitute das BDSG anzuwenden (§ 2 Abs. 4 LDSG). Für den Schadensersatz gilt danach § 8 BDSG. Diese Regelung enthält nur eine Umkehr der Beweislast hinsichtlich der Kausalität der Schadensfolge. Ein Schadensersatzanspruch selbst kann sich also nicht aus dem BDSG, sondern nur aus anderen – etwa deliktischen oder vertraglichen – Regelungen ergeben.

Auch bezüglich der Strafvorschriften gilt gegenüber öffentlich-rechtlichen Kreditinstituten das BDSG. Insofern gibt es hier eine Verschärfung gegenüber den Regelungen, die für öffentliche Stellen nach dem LDSG gelten. Die Tat ist allerdings ein Antragsdelikt (§ 43 Abs. 4 BDSG). Die Antragsfrist beträgt nach dem Strafgesetzbuch sechs Monate. Die unbefugte Übermittlung ist mit Strafe bedroht. Allerdings ist nur die vorsätzliche Handlung strafbar. Im vorliegenden Fall dürfte ein Irrtum über das Vorliegen eines tatsächlichen Tatbestandsmerkmals bestanden haben. Dann käme nur die Verfolgung als Fahrlässigkeitsdelikt in Betracht. Die hier relevanten Straftatbestände sind jedoch ausschließlich Vorsatzdelikte, so daß eine Strafbarkeit auszuschließen sein dürfte.

22.5 Kontoauszüge in Sichtfenster-Briefumschlägen

Ein Sparkassenkunde trug folgende Beschwerde vor: Die Kontoauszüge würden ihm halbmonatlich in einem Fensterumschlag übersandt. Es habe sich gezeigt, daß bei dem benutzten Fensterumschlag der alte Kontostand im Adreßfenster deutlich sichtbar sei. Die Sparkasse sei von ihm schriftlich auf diesen Mißstand hingewiesen worden.

Daraufhin habe diese erklärt, ab sofort würden Briefumschläge eingesetzt, bei denen eine Wiederholung des Fehlers ausgeschlossen sei.

Dennoch habe er weiterhin Kontoauszüge in der gleichen mangelhaften Form erhalten. Darauf habe er die Sparkasse telefonisch hingewiesen. Ihm sei zugesichert worden, ihm würden in Zukunft seine Bankauszüge in anderen Umschlägen zugesandt werden. Trotz aller Zusagen habe er erneut Kontoauszüge in der alten Form mit lesbarem Kontostand im Adreßfenster erhalten.

Aufgrund der Recherchen des LfD ergab sich, daß zunächst noch trotz verschiedener Anweisungen der Zentrale weiter alte Fensterumschläge eingesetzt worden waren, deren Rand zu schmal war. In der betroffenen großen Filialorganisation hatte es längere Zeit gedauert, bis allen beteiligten Stellen klar wurde, daß sie nur noch die neuen DIN C 6-Umschläge benutzen durften, die einen breiteren Papierstreifen unter dem Fenster besitzen, so daß auch bei Verschiebung des Inhalts die Beträge verdeckt blieben. Alle Umschläge, bei denen der gerügte Fehler auftreten konnte, wurden vernichtet.

23. Sonstiges

23.1 Die korrekte Adressierung als Datenschutzproblem

23.1.1 Nutzung der Dienstanschrift für ein Schreiben in Personalangelegenheiten

Ein öffentlich Bediensteter rügte, daß sein ehemaliger Arbeitgeber, eine rheinland-pfälzische Stadt, seine neue Dienstanschrift benutzt habe, um ihm ein persönliches Schreiben (eine Rechnung privater Telefonate) zu übermitteln.

Das Schreiben der Stadtverwaltung war wie folgt adressiert:

Behörde xy
z. H. Herrn xy
PLZ Stadt xy

Aus dieser Adressierung wird nicht hinreichend deutlich, daß es sich um einen den Empfänger privat betreffenden Vorgang gehandelt hat. Deshalb kam es zu dem Mißverständnis der neuen Dienstbehörde, die dieses Schreiben für ein dienstliches Schreiben gehalten, geöffnet und mit der Dienstpost an den Letztempfänger weitergeleitet hat.

Der LfD hat die Absenderbehörde darauf hingewiesen, daß Schreiben in privaten Angelegenheiten von Mitarbeitern einer anderen Behörde oder eines Unternehmens dann, wenn sie an die dienstliche oder berufliche Anschrift gerichtet sind, eindeutig persönlich zu adressieren sind. So hätte im vorliegenden Fall die eindeutige Adressierung wie folgt lauten müssen:

Herrn XY persönlich
c/o Behörde xy
PLZ Stadt xy

Die Nutzung einer dienstlichen Anschrift wird allerdings einer Behörde auch dann nicht untersagt werden können, wenn persönliche Angelegenheiten des Adressaten betroffen sind.

23.1.2 Der Weg von Verurteilungsmitteilungen an das Wahlamt

Eine Stadt hat den LfD darauf hingewiesen, daß die Staatsanwaltschaft Strafurteile an das Wahlamt der Stadt übersende, ohne daß ein verschlossener Umschlag benutzt werde. Es werde vielmehr nur ein Übersendungszettel an das Urteil angeheftet, auf dem die Adresse „Stadtverwaltung, Wahlamt" angebracht sei. Ein Hinweis „Vertraulich zu behandeln" befinde sich auf dem Übersendungszettel. Da der Eingang über die zentrale Poststelle erfolge, hätte eine größere Zahl von Bediensteten Gelegenheit, Kenntnis vom Inhalt der Urteile zu nehmen.

Das Ministerium der Justiz hat dazu erklärt, daß es in Nr. 8 Abs. 4 der Verwaltungsvorschrift über „Mitteilungen in Strafsachen" (MiStra) ausdrücklich vorgeschrieben sei, Mitteilungen in Strafsachen in einem verschlossenen Umschlag zu übersenden. In einem besonderen Vermerk sei außerdem auf eine vertrauliche Behandlung hinzuweisen. Bei der betroffenen Staatsanwaltschaft sei diese Regelung nicht hinreichend beachtet worden. Durch eine klarstellende Anordnung des Leitenden Oberstaatsanwaltes sei diese von der MiStra abweichende Praxis bei der Staatsanwaltschaft abgestellt worden.

Damit wurde dem Anliegen des Datenschutzes entsprochen.

23.2 Gibt es ein Einsichtsrecht des beleidigenden Bürgers in behördliche Aufzeichnungen über sein Fehlverhalten?

Im Zusammenhang mit einer Eingabe hatte der LfD zu beurteilen, ob ein Nutzer einer Bibliothek, der Bibliotheksbedienstete beleidigt haben soll, einen Anspruch auf Akteneinsicht in diejenigen Vermerke besaß, die das ihm vorgeworfene Fehlverhalten betreffen.

Die Bibliothek war ursprünglich der Auffassung, ein solcher Anspruch bestehe nicht.

Demgegenüber hat der LfD folgende Rechtsauffassung formuliert:

a) Der Beschwerdeführer hat einen Auskunftsanspruch gem. § 18 Abs. 1 Satz 1 LDSG über die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft oder die Personen oder Stellen beziehen, an die die Daten übermittelt worden sind, sowie den Zweck und die Rechtsgrundlage der Speicherung.
Darüber hinaus hat er gem. § 18 Abs. 1 Satz 3 LDSG einen Anspruch auf Ausübung des pflichtgemäßen Ermessens der Bibliothek, ob ihm nicht Einsicht in die entsprechenden Akten gewährt wird.

b) Gründe, die zum Unterbleiben der Auskunftserteilung gem. § 18 Abs. 3 LDSG führen könnten, lagen nicht vor.

c) Bei den in Rede stehenden schriftlichen Vorgängen handelt es sich um Akten im Sinne des LDSG (§ 3 Abs. 6 LDSG). Danach ist eine Akte jede amtlichen oder dienstlichen Zwecken dienende Unterlage. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorganges werden sollen und alsbald vernichtet werden. Die vorliegenden Aktenteile bestehen aus Vermerken über das Verhalten des Bibliotheksbenutzers. Diese Unterlagen haben im dienstlichen Verkehr bereits Bedeutung erlangt, denn sie waren Gegenstand eines Gesprächs mit dem Betroffenen. Außerdem sollen sie aufbewahrt werden, um bei Wiederholungen des in Rede stehenden Verhaltens herangezogen werden zu können.

d) Die Personen, die die Vermerke angefertigt haben, haben in ihrer dienstlichen Eigenschaft gehandelt, denn die entsprechenden Vermerke sollten Gegenstand des weiteren dienstlichen Vorgehens sein. Damit haben sie in dieser Eigenschaft gegenüber dem betroffenen Bürger keinen Anspruch auf Wahrung des informationellen Selbstbestimmungsrechts, soweit Unterlagen betroffen sind, die das Verhalten des Bürgers zum Gegenstand haben. Zu den hier maßgeblichen Überlegungen wird auf den 13. Tätigkeitsbericht, Tz. 17.3, verwiesen.

e) Auf ausdrücklichen Wunsch des Ministeriums für Bildung, Wissenschaft und Weiterbildung hat der LfD auch zur Frage der „Rechtsschutzmöglichkeiten der von der Entscheidung des LfD negativ Betroffenen" Stellung genommen: Die vorstehend geäußerte Auffassung des LfD war und ist für die Behörden nicht bindend. Bei einem Verhalten der Behörde, das dieser datenschutzrechtlichen Wertung nicht entspricht, hat der LfD allerdings die Möglichkeit einer förmlichen Beanstandung dieses Verhaltens gegenüber der zuständigen Aufsichtsbehörde. Rechtsmittel existieren für die Behörde weder gegen die Stellungnahme noch gegen eine etwaige Beanstandung. Auch einzelne Bedienstete, die sich negativ betroffen fühlen, haben keine entsprechenden Rechte gegenüber dem LfD. Der betroffene Bürger kann gegen die Ablehnung der Gewährung von Auskunft oder Akteneinsicht den Verwaltungsrechtsweg beschreiten.

Dem Beschwerdeführer war also umfassend mitzuteilen, welchen Inhalt die ihn betreffenden schriftlichen Vorgänge bei der Bibliothek haben. Vorab war eine Ermessensentscheidung über die Gewährung von Akteneinsicht zu treffen; sollte Akteneinsicht gewährt werden, konnte selbstverständlich eine Auskunftserteilung über den Inhalt der Akte unterbleiben. Die Bibliothek hat aufgrund dieser Stellungnahme die Akteneinsicht gewährt.

23.3 Ermittlungsbefugnisse, Datenübermittlungen und Auskunftserteilung an den Betroffenen durch Kreishandwerkerschaften bei der Verfolgung der Schwarzarbeit

Eine Kreishandwerkerschaft hatte von einem Informanten erfahren, daß in einem Haus „schwarz" Handwerksarbeiten ausgeführt werden sollten. Der Hauseigentümer weigerte sich, der Kreishandwerkerschaft hierüber Informationen zu geben.

In der Zeit, in der nach den Angaben des Informanten Handwerksarbeiten ausgeführt wurden, waren in unmittelbarer Nähe des fraglichen Hauses zwei Fahrzeuge abgestellt, darunter das Fahrzeug des Beschwerdeführers. Die Kreishandwerkerschaft hatte dies festgestellt und war damit der Überzeugung, daß die Handwerker mit diesen Fahrzeugen angereist waren. Zum Zweck der weiteren Aufklärung schrieb sie zunächst den Hausbesitzer an und bat ihn um Auskunft, „welche Arbeiten die Herren mit den Fahrzeugen Kfz-Kennzeichen XY, 3er BMW schwarz und XY, Peugeot 505, ausgeführt haben". Sie teilte dem Auftraggeber weiter mit, hierbei handele es sich vermutlich um die namentlich benannten Kfz-Halter. Es liege der Verdacht nahe, daß im Haus des Befragten Schwarzarbeit von den benannten Personen ausgeführt wurde. Die benannten Herren hätten vermutlich die Maler- und Lackiererarbeiten dort ausgeführt.

Die Stadtverwaltung, Amt für öffentliche Ordnung, erhielt eine Kopie.

Außerdem schrieb die Kreishanderwerkerschaft die Ehefrau eines der betroffenen Kfz-Halter unmittelbar an. Sie verlangte von ihr eine Unterlassungserklärung, unberechtigt Handwerksarbeiten auszuführen.

Eine Durchschrift dieses Abmahnungsschreibens wurde an die Verbandsgemeindeverwaltung ihres Wohnsitzes als Ortspolizeibehörde zur Kenntnis übersandt.

Es stellte sich heraus, daß die beiden Kfz-Halter und die Ehefrau mit der fraglichen Schwarzarbeit nichts zu tun hatten, sondern Benutzer des nahegelegenen Sportplatzes waren.

Der Beschwerdeführer, einer der betroffenen Kfz-Halter, begehrte Auskunft von der Kreishandwerkerschaft, wer ihr die unzutreffende Information mitgeteilt habe, daß er Schwarzarbeiten ausführen würde.

Außerdem stellte er folgende Fragen:

Durfte die Kreishandwerkerschaft die fraglichen Informationen überhaupt in personenbezogener Form erheben?

Durfte die Kreishandwerkerschaft die ihr vorliegenden Informationen nutzen, um ein Abmahnungsschreiben zu verfassen?

Durfte die Kreishandwerkerschaft die Ordnungsbehörden des Wohnsitzes der Betroffenen über ihren Verdacht unterrichten?

Zunächst ist die Frage zu beantworten, ob die Kreishandwerkerschaft überhaupt Informationen zum Zweck der Bekämpfung der Schwarzarbeit in personenbezogener Form erheben und speichern darf.

Nach Auffassung des LfD ist in diesem Zusammenhang festzuhalten, daß die Kreishandwerkerschaft den konkreten Fall aufgegriffen hat, um Maßnahmen gegen die unerlaubte Ausübung der Schwarzarbeit zu treffen bzw. zu veranlassen. Die Abmahnung war in diesem Zusammenhang offensichtlich nur eine von mehreren von der Kreishandwerkerschaft durchgeführten bzw. nach ihrer Auffassung in Erwägung zu ziehenden Möglichkeiten. Dies wird schon daraus deutlich, daß die Kreishandwerkerschaft ergänzend andere Behörden (sowohl die Stadt- wie die Verbandsgemeindeverwaltung) informiert hat. Insofern ist weder allein noch auch nur vorrangig auf die Frage abzustellen, ob die Datenerfassung zum Zweck der Abmahnung zulässig war. Bei der weiteren Beurteilung ist vielmehr vom Ziel der Bekämpfung der Schwarzarbeit durch die Kreishandwerkerschaft auszugehen.

Sowohl die Kreishandwerkerschaft wie die Handwerksinnungen und die Handwerkskammern haben die Aufgabe, im Interesse des Handwerks die Schwarzarbeit zu bekämpfen. Dazu gehört auch die Aufgabe, konkrete Fälle der Schwarzarbeit aufzuklären und insbesondere die für die bußgeldrechtliche sowie gewerbeordnungsrechtliche Ahndung zuständigen Stellen zu unterrichten. Der LfD verweist hierzu auf den 12. Tätigkeitsbericht Tz. 11.2.

Die im vorliegenden Zusammenhang erfolgte Datenerhebung durch die Kreishandwerkerschaft hält der LfD demzufolge gem. § 12 Abs. 1 Landesdatenschutzgesetz für grundsätzlich zulässig.

Die Frage, ob die Abmahnung als konkrete Maßnahme zulässig gewesen ist, war von ihm nicht zu entscheiden. Diese Frage ist nicht datenschutzrechtlicher Natur, da die Kreishandwerkerschaft mit den erhobenen Daten auch andere, zweifelsfrei zulässige Maßnahmen zur Bekämpfung der Schwarzarbeit (insbesondere die Anzeigeerstattung bei den für die Bekämpfung der Schwarzarbeit zuständigen Behörden) durchführen wollte und durfte.

Aus datenschutzrechtlicher Sicht ist es jedoch unabdingbar, daß sich die Informationen, die den zuständigen Behörden zu Anzeigezwecken übermittelt werden, im Rahmen einer zutreffenden und vollständigen Darstellung der Tatsachen halten.

Im vorliegenden Fall wurden die jeweils zuständigen Behörden mit folgendem Wortlaut informiert: „Die von uns benannten Herren haben vermutlich die Maler- und Lackiererarbeiten ... ausgeführt." „Nach uns zugegangenen Informationen soll Frau xy in erheblichem Umfang Handwerksarbeiten selbständig ausüben."

Beide Aussagen enthalten als Kern eine Tatsachenbehauptung. Diese war von den festgestellten und der Kreishandwerkerschaft bekannten Tatsachen nicht gedeckt: Die Kreishandwerkerschaft hatte Kenntnis davon, daß vor einem Haus, in dem nach ihrer nachvollziehbaren Überzeugung Schwarzarbeit ausgeführt wurde, zwei Kraftfahrzeuge geparkt haben. Weitere Anhaltspunkte, daß die Halter oder Nutzer der Kraftfahrzeuge konkret mit der Ausübung von Schwarzarbeit beschäftigt waren, lagen der Kreishandwerkerschaft nicht vor. Insbesondere die geäußerte Vermutung, Maler- und Lackiererarbeiten seien ausgeführt worden, hat den unzutreffenden Eindruck erweckt, die Kreishandwerkerschaft habe genauere und deutlichere Hinweise für ihren Verdacht. Es wurde nicht deutlich, daß es sich hier um eine völlig ungesicherte Behauptung gehandelt hat. Die zugrundeliegenden Tatsachen konnten zwar einen vagen Verdacht, nicht aber die Überzeugung in bezug auf die behauptete Ausübung der Schwarzarbeit durch die betroffenen Kfz-Halter begründen. Es wäre allenfalls zulässig gewesen, den zuständigen Behörden den konkret bekannten Sachverhalt mitzuteilen.

Eine förmliche Beanstandung gegenüber der Kreishandwerkerschaft ist gem. § 25 Abs. 2 LDSG im vorliegenden Fall unterblieben, da diese die unterrichteten Stellen zwischenzeitlich auch von der Aufklärung der Angelegenheit und von ihrer Entschuldigung gegenüber den Betroffenen selbst informiert hat. Der LfD hat aber die obigen Feststellungen der Kreishandwerkerschaft mitgeteilt und sie auf die Pflicht zur künftigen Beachtung der genannten Kriterien hingewiesen.

Zur Pflicht, Auskunft über den Informanten zu erteilen, hat der LfD folgende Auffassung vertreten: Nach § 18 Abs. 1 LDSG ist den Betroffenen auf Antrag unentgeltlich Auskunft zu erteilen über die zu ihrer Person gespeicherten Daten, auch soweit sie sich auf die Herkunft oder die Personen oder Stellen beziehen, an die die Daten übermittelt worden sind. Allerdings unterbleibt die Auskunftserteilung nach § 18 Abs. 3, wenn die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der datenverarbeitenden Stelle liegenden Aufgaben gefährden würde.

Das Urteil des Bundesverwaltungsgerichts vom 3. September 1991 (NJW 92, 451) konkretisiert in aus der Sicht des LfD zutreffender Weise die Bedingungen, unter denen eine Auskunftserteilung über die Person eines Informanten die Aufgaben der auskunftserteilenden Stelle gefährden würde. Sie können in vergleichbarer Weise auf die Behörden angewendet werden, die mit der Bekämpfung der Schwarzarbeit befaßt sind. Dabei sind nicht nur die Fälle zu berücksichtigen, in denen der Informant an Leib und Leben gefährdet ist (wie dies möglicherweise in dem vom Bundesverwaltungsgericht entschiedenen Fall anzunehmen war), sondern es ist auch zu berücksichtigen, daß gerade im Bereich der Bekämpfung der Schwarzarbeit die hier tätigen Behörden auf Informationen aus dem Kreis der Bürger angewiesen sind. Entsprechende Informationen würden wohl den Behörden in noch erheblich geringerem Umfang zukommen, wenn grundsätzlich damit zu rechnen wäre, daß die Identität des Informanten den Betroffenen mitgeteilt wird. Nur dann kann das Interesse des Betroffenen Vorrang vor den Geheimhaltungsinteressen der Behörde haben, wenn die Information offensichtlich bzw. willentlich falsch gegeben wurde oder wenn durch die Information ein Straftatbestand (etwa Beleidigung, üble Nachrede, Verleumdung, Vortäuschen einer Straftat o. ä.) erfüllt worden wäre.

Im hier zu beurteilenden Fall hatte der Informant weder offensichtlich falsche noch willentlich und wissentlich unzutreffende Informationen übermittelt. Anhaltspunkte dafür, daß er den Straftatbestand der Beleidigung, der üblen Nachrede, der Verleumdung, des Vortäuschens einer Straftat o. ä. erfüllt hätte, sind nicht ersichtlich. Der Informant hat sich vielmehr auf die Mitteilung eines Verdachts unter Nennung von bestimmten Tatsachen beschränkt. Dann aber war ein auf die Identität des Informanten zielender Auskunftsanspruch des Betroffenen entfallen.

23.4 Mahnung per Postnachnahmeauftrag

Sowohl die Abgabenordnung (§ 259) wie auch das Landesverwaltungsvollstreckungsgesetz (§ 22 Abs. 2) lassen die Mahnung per Postnachnahmeauftrag zu. Eine Kreisverwaltung fragte beim LfD an, ob eine Postkarte mit Nachnahme den datenschutzrechtlichen Bestimmungen entspricht. Die Datenschutzrelevanz dieser Form der Mahnung ist darin zu sehen, daß die Art der rückständigen Forderung beispielsweise Familienangehörigen oder anderen in Hausgemeinschaft lebenden Personen bekannt werden kann.

Erkundigungen bei der Deutschen Bundespost – Telekom, Direktion Koblenz, ergaben, daß außer der Postkarte mit Nachnahme keine andere Versendungsform zugelassen und geeignet ist. Es ist insbesondere nicht zugelassen, die Nachnahme mit einem verschlossenen Brief zu verbinden, der, unabhängig von der sofortigen Einlösung der Nachnahme, ausgeliefert wird.

Bisher hat der Gesetzgeber davon abgesehen, die zitierten Bestimmungen unter Datenschutzgesichtspunkten und im Blick auf die nach den Postbestimmungen einzig mögliche Versendungsform zu ändern. Es ist demnach davon auszugehen, daß die Mahnung durch Postnachnahmekarte dem gesetzgeberischen Willen entspricht und ein mit der Verwendung der Postnachnahmekarte möglicherweise verbundener Eingriff in das informationelle Selbstbestimmungsrecht zulässig ist.

Auf die Bezeichnung der Forderung auf der Postnachnahmekarte kann nicht verzichtet werden. Diese Bezeichnung muß einerseits so präzise sein, daß sie vom Empfänger des Postnachnahmeauftrags verstanden und zugeordnet werden kann, andererseits muß – insbesondere bei Freitextangaben – der Erforderlichkeitsgrundsatz beachtet werden.

23.5 Aufzeichnung von Telefonaten in Rettungsleitstellen

Zur Zulässigkeit der automatischen Aufzeichnung von Telefonaten und des Funksprechverkehrs mit Rettungsleitstellen von Polizei, Feuerwehr und anderen Rettungsdiensten äußerte sich der LfD auf Anfrage wie folgt:

„Bei Telefongesprächen, die über Notruf 112 bzw. 110 oder den bundeseinheitlichen Rettungsstellennotruf 19222 oder einen sonstigen offiziellen, für Notrufe vorgesehenen Leitstellenanschluß geführt werden, bestehen gegen eine automatische Aufzeichnung keine Bedenken. Das gleiche gilt für Dienstgespräche, z. B. mit Krankenhäusern, Ärzten, der Feuerwehr, der Polizei oder der Rettungswachen, die der Einsatzsteuerung oder Einsatzabwicklung in Notfällen dienen.

Auch der Funksprechverkehr kann, soweit er der Aufgabenerfüllung der Leitstelle dient, aufgezeichnet werden.

Gespräche, die auf sonstigen, nicht für Notfallmeldungen oder Notfallabwicklung vorgesehenen Leitungen in der Leitstelle eingehen oder von dort hinausgehen, dürfen grundsätzlich nur dann aufgezeichnet werden, wenn der Gesprächspartner auf die Aufzeichnung ausdrücklich hingewiesen wird und er sein Einverständnis zur Aufzeichnung gibt.

Die Aufzeichnungen in dem o. g. Umfange dienen ausschließlich der zuverlässigen Durchführung des Einsatzauftrages im Interesse der Hilfesuchenden und der Beweissicherung. Eine Strafbarkeit nach § 201 Abs. 1 StGB ist nicht gegeben. Nach § 201 Abs. 1 StGB wird nur bestraft, wer unbefugt das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt. Die Rechtswidrigkeit entfällt danach bei gesetzlicher Erlaubnis, bei Einwilligung des Sprechenden oder überwiegendem Interesse an der Aufzeichnung im Rahmen einer Güter- und Pflichtenabwägung. Die Dokumentation der Gespräche mit den Leitstellen ist zwar nicht ausdrücklich gesetzlich erlaubt; es kann jedoch davon ausgegangen werden, daß bei dem heutigen Stand der Technik der Anrufer weiß, daß sein Gespräch aufgezeichnet werden kann. Zumindest aber kann davon ausgegangen werden, daß der Anrufer im Interesse einer effektiven Hilfeleistung stillschweigend die Aufzeichnung seiner Notrufmeldung billigt. Darüber hinaus dürfte in diesen Fällen im Rahmen der Güter- und Pflichtenabwägung das Interesse des Betreibers der Leitstelle und das Interesse des durch den Notfall betroffenen Bürgers an einer beweiskräftigen Dokumentation der Notfallbehandlung höher zu bewerten sein als ein evtl. Interesse des Anrufers an einer Nichtaufzeichnung seiner Notfallmeldung.

Bei den Leitstellen sollten jedoch technische Möglichkeiten geschaffen werden, das Aufzeichnungsgerät außer Betrieb zu setzen, wenn der Diensthabende erkennt, daß die Voraussetzungen für eine Aufzeichnung nicht erfüllt sind. Ferner sollte sichergestellt sein, daß die Mitarbeiter der Leitstellen über gesonderte Nebenstellen Gespräche führen können, die nicht aufgezeichnet werden.

Die Aufzeichnungsdauer bestimmt sich nach der Erforderlichkeit für die mit der Aufzeichnung verfolgten Zwecke. Eine Zeitdauer von sechs Wochen ist angemessen."

23.6 Katasterwesen – Auszug aus dem Veränderungsnachweis und Eigentümernachweis

Aus Gründen eines schlüssigen datumsbezogenen Nachweises und der Transparenz für den Bürger werden Veränderungsnachweise im Liegenschaftskataster als Gegenüberstellung des Flurstücksbestandes vor und nach der Fortführung aufgestellt. Dazu ist es in der Regel erforderlich, alle gespeicherten Angaben zum Flurstück – auch die nicht veränderten – aufzuführen. Als zusätzliche Serviceleistung übermittelt die Vermessungs- und Katasterverwaltung den Betroffenen zusätzlich zum Veränderungsnachweis noch einen aktualisierten Eigentümernachweis.

Diese Verfahrensweise war Gegenstand der Eingabe von Angehörigen einer Wohnungseigentümergemeinschaft. Sie wandten sich dagegen, daß allen Miteigentümern ein vollständiger aktualisierter Eigentümernachweis übermittelt wurde, der die Eigentumsverhältnisse darstellte und das Geburtsdatum enthielt.

Den zuständigen Fachbehörden war in der Auffassung zuzustimmen, daß die Übersendung des vollständigen Auszugs aus dem Veränderungsnachweis mit dem neuen Bestand in Form eines Flurstücks- und Eigentümernachweises eine sinnvolle Serviceleistung gegenüber den Betroffenen darstellt, denn diese besitzen häufig keine schlüssigen Nachweise der Flurstücksangaben, die es ihnen ermöglichen, Veränderungsmitteilungen nachzuvollziehen. Im Rechtssinne erforderlich, also für die Aufgabenerfüllung unerläßlich, war diese Serviceleistung indessen nicht, denn die Übersendung des Auszugs aus dem Veränderungsnachweis genügt, den Eigentümern die katastermäßigen Vorgänge verständlich zu machen.

Das Ministerium des Innern und für Sport als die zuständige oberste Landesbehörde wird der Empfehlung des LfD, die Verfahrensweise zu ändern, entsprechen.

23.7 Datenschutzbürokratie

Das novellierte LDSG statuiert in § 10 die Pflicht zur Führung von Verzeichnissen über Verfahren, in denen personenbezogene Daten automatisiert gespeichert werden: Verfahrensbeschreibung, Verfahrensverzeichnis und Geräteverzeichnis. Nach § 11 ist ein behördlicher Datenschutzbeauftragter zu bestellen, der die öffentlichen Stellen bei der Ausführung des LDSG sowie anderer Vorschriften über den Datenschutz zu unterstützen hat. Es kann nicht in Abrede gestellt werden, daß die Umsetzung dieser gesetzlichen Bestimmungen mit einer gewissen Mehrarbeit verbunden ist. Gelegentlich wird gegenüber dem LfD aber auch der Vorwurf erhoben, mit dem neuen LDSG habe sich eine völlig unangemessene Datenschutzbürokratie etabliert.

Das LDSG sieht in der Transparenz der Datenverarbeitung ein Gestaltungsprinzip des Datenschutzes. Insoweit dienen die Verzeichnisse nach § 10 dem Datenschutz; sie erleichtern beispielsweise die Datenschutzkontrolle, weil die für diese Arbeiten relevanten Informationen schnell und – wenn die Verzeichnisse ordentlich geführt werden – auch vollständig zur Verfügung stehen. Gleichermaßen nützlich sind sie aber auch für die Behördenleitung, die diesen Verzeichnissen wichtige Planungs- und Leitungsinformationen entnehmen kann. Die Doppelt- und Mehrfachbeschaffung teurer Softwareprodukte ist in größeren Verwaltungseinheiten durchaus ein Problem. Die zentrale Führung eines Verfahrensverzeichnisses beispielsweise kann hier Abhilfe schaffen. Im übrigen kann der Verwaltungsaufwand durch automatisierte Führung der Verzeichnisse minimiert werden; bei zentral entwickelten Verfahren kann auf Musterverfahrensbeschreibungen zurückgegriffen werden. Das Verfahrensverzeichnis kann aus einer Zusammenfassung der Verfahrensbeschreibungen bestehen und das Geräteverzeichnis kann mit dem nach haushaltsrechtlichen Bestimmungen zu führenden Inventarverzeichnis verbunden werden, so daß der Verwaltungsaufwand auch insoweit nicht unvertretbar groß ist.

Die Pflicht zur Bestellung eines Datenschutzbeauftragten bestand auch in der Vergangenheit schon in Teilbereichen der öffentlichen Verwaltung: für den Sozialleistungsbereich, für Krankenhäuser und für öffentlich-rechtliche Wettbewerbsunternehmen. Selbstverständlich können die nach den einschlägigen gesetzlichen Bestimmungen bestehenden Pflichten jetzt in Personalunion von einem behördlichen Datenschutzbeauftragten wahrgenommen werden. Ebenso selbstverständlich können dem behördlichen Datenschutzbeauftragten auch noch andere Aufgaben übertragen werden; nur in sehr großen Verwaltungen wird ein leistungsfähiger Mitarbeiter mit der Wahrnehmung von Aufgaben nach § 11 LDSG vollständig ausgelastet sein.

Im übrigen ist der behördliche Datenschutzbeauftragte, der in der Wahrnehmung dieses Amtes unmittelbar der Behördenleitung untersteht, geradezu prädestiniert, als Berater in Automationsfragen herangezogen zu werden, der die Fachinformationen der Systementwicklung und Systembetreuung ergänzt.

23.8 Das Datenschutzregister

Nach § 27 Abs. 1 LDSG sind öffentliche Stellen verpflichtet, Verfahren, in denen personenbezogene Daten verarbeitet werden, sowie Art und Umfang ihrer Nutzung beim LfD anzumelden. Für den LfD bilden diese Anmeldungen eine wichtige Grundlage der Kontrollarbeit; der behördliche Datenschutzbeauftragte kann den Anmeldungen die Informationen entnehmen, die er für die Wahrnehmung seiner Aufgaben nach § 11 benötigt.

Um den mit der Anmeldung verbundenen Verwaltungsaufwand zu reduzieren, wurde in § 27 Abs. 2 LDSG die seit einigen Jahren praktizierte Verfahrensweise bei der Anmeldung von zentralen Verfahren (verkürzte Anmeldung) gesetzlich geregelt. Danach wird ein Verfahren, das erstmals zur Eintragung in das Datenschutzregister angemeldet wird und bei mehreren öffentlichen Stellen eingesetzt werden soll, in die Liste der zentral entwickelten Verfahren mit einer laufenden Nummer aufgenommen. Dies hat zur Folge, daß bei weiteren Anmeldungen die Angabe der entsprechenden Schlüsselnummer ausreichend ist; eine komplette Beschreibung des Verfahrens ist entbehrlich.

Zur Erleichterung des Anmelde- und Änderungsverfahrens hat der LfD den bereits bisher vorhandenen Vordruck an die Anforderungen des neuen Landesdatenschutzgesetzes angepaßt. Er dient der Anmeldung von Verfahren und kann gleichzeitig von der anmeldenden Behörde zur Führung des Geräte- und des Verfahrensverzeichnisses verwendet werden. Der Vordruck wird – neben weiteren datenschutzrechtlichen Informationen (z. B. Text des Landes- und Bundesdatenschutzgesetzes, Hinweise des Innenministeriums, der jeweils letzte Tätigkeitsbericht usw.) – vom LfD den Behörden auch in maschinenlesbarer Form (Winword-Format) zur Verfügung gestellt. Damit soll ein leichteres Ausfüllen des Vordrucks erreicht und die Möglichkeit geschaffen werden, durch eine Ablage der Seiten 2 und 3 des Vordrucks für jedes einzelne Verfahren das Verfahrensverzeichnis mit geringem Aufwand auch maschinell zu führen. Dem LfD ist es jedoch nicht möglich, Anmeldungen zum Datenschutzregister in maschinenlesbarer Form entgegenzunehmen. Vielmehr ist es weiterhin erforderlich, die Anmeldungen in ausgedruckter Form dem LfD vorzulegen.

In der Vergangenheit war immer wieder festzustellen, daß die Anmeldungen zum Datenschutzregister nicht oder nicht rechtzeitig erfolgten. Auch im Berichtszeitraum ist dies zu beklagen. Zugleich ist aber auch festzustellen, daß sich die Zahl der

Anmeldungen drastisch erhöht. Insbesondere 1995 liegt die Zahl der Anmeldungen mit über 460 weit über dem Durchschnitt der vergangenen Jahre. Der LfD geht davon aus, daß dies nicht zuletzt auf die Initiative bzw. Mitwirkung der behördlichen Datenschutzbeauftragten im Anmeldeverfahren zurückzuführen ist.

24. Schlußbemerkung

Dieser 15. Tätigkeitsbericht ist wieder sehr umfangreich. Dies ist nicht gewollt, sondern eher zu bedauern; denn es ist ein Indiz dafür, daß die Zahl der Konfliktfelder im Datenschutz nicht abnimmt. Trotz der gebotenen Fülle an Informationen wird dem aufmerksamen Leser nicht verborgen bleiben, daß in Teilbereichen der Kontrollzuständigkeit, wie dem Sozialleistungs- oder Kommunalbereich, zwar verhältnismäßig breit über die Behandlung von Eingaben und die Beratungstätigkeit des LfD, jedoch nur wenig über die Ergebnisse örtlicher Feststellungen berichtet wird.

Die Behörde des LfD soll nach dem Willen des Gesetzes Kontrollbehörde sein, sie soll aber auch Beratungsaufgaben wahrnehmen. Tatsache ist aber, daß die Begleitung von Gesetzesvorhaben, die Beratung bei der Einführung und Nutzung von DV-Systemen und die Bearbeitung von Eingaben die vorhandenen Arbeitskapazitäten in immer stärkerem Maße in Anspruch nehmen. Die zunehmende Beratungstätigkeit hat zweifellos einen präventiven Effekt: Je stärker das Engagement des LfD bei der Rechtssetzung ist, desto besser und klarer ist der Datenschutz in den geltenden Normen verankert und desto weniger Datenschutzprobleme werden im Vollzug der Normen durch die Verwaltung entstehen. Es ist besser und leichter zu verhindern, daß ein Kind in den Brunnen fällt, als das Kind aus dem Brunnen zu ziehen. Trotzdem ist die Kontrolltätigkeit sehr wichtig, um den Datenschutz in der Verwaltungspraxis zu gewährleisten. Für nicht anlaßbezogene systematische örtliche Kontrollen bleibt aber immer weniger und in einzelnen Arbeitsbereichen inzwischen zu wenig Zeit.

Sicherlich ist auch die Bearbeitung der zunehmenden Menge der Eingaben, die damit verbundene Befragung der betroffenen Behörden nach datenschutzrelevanten Sachverhalten und deren datenschutzrechtliche Bewertung – die nicht selten zu Beanstandungen führt – eine Form der Datenschutzkontrolle. Diese müßte indessen in einem weitaus stärkeren Maße, als dies tatsächlich der Fall ist, durch eine nicht anlaßbezogene örtliche Kontrollarbeit flankiert werden. Dies ist aber nicht möglich: Bürger, die sich ratsuchend oder beschwerdeführend an den LfD wenden, erwarten zu Recht, daß sie in angemessener Zeit eine Antwort erhalten, und eine Behörde, die eine Stellungnahme des LfD zu einem konkreten Datenschutzproblem erbittet, kann auch nicht auf einen fernen Termin vertröstet werden; denn nur ein schneller Rat ist auch ein guter Rat.

Die zunehmenden Defizite bei der Wahrnehmung gesetzlicher Kontrollaufgaben lassen sich auch durch rationelle Strukturierung, Technikeinsatz und effiziente Ausübung der Tätigkeit der Mitarbeiterinnen und Mitarbeiter des LfD auf Dauer nicht ausgleichen. Der LfD hat im Blick auf die Haushaltslage des Landes bei Personalanforderungen bisher größte Zurückhaltung geübt; seine Behörde verfügt mit dem Saarland über die mit Abstand geringste Personalausstattung aller Datenschutz-Kontrollbehörden in Deutschland. Setzt sich die oben beschriebene Entwicklung aber fort, so sind zusätzliche Personalanforderungen für den Haushalt 1997 unvermeidlich.

Anlage 1

Entschließung
der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 zu kartengestützten Zahlungssystemen im öffentlichen Nahverkehr

Mit der Weiterentwicklung von Chipkarten werden kartengestützte Zahlungssysteme zunehmend auch im Verkehrsbereich eingesetzt. Damit besteht die Gefahr, daß sehr detaillierte Bewegungsprofile entstehen, die den persönlichen Bereich jedes einzelnen einschränken und z. B. auch für Strafverfolgungsbehörden, Finanzämter und für die Werbewirtschaft von Interesse sein könnten. Da sämtliche Fahrten für einen gewissen Zeitraum aufgelistet werden können, hat jeder Kontoinhaber die Möglichkeit, Fahrten sämtlicher Familienmitglieder jederzeit nachzuvollziehen.

So sind im öffentlichen Nahverkehr zahlreiche sogenannte Postpaid-Verfahren in Erprobung, bei denen dem Fahrgast am Monatsende die aufsummierten Fahrpreise vom Konto abgebucht werden. Diese Zahlungsweise erfordert die Speicherung umfangreicher personenbezogener Daten: Neben der Konto-Nr. und Bankleitzahl des Fahrgastes werden sowohl Datum, Uhrzeit des Fahrscheinkaufes bzw. des Fahrantritts als auch Automatennummer und Preisstufe der jeweiligen Fahrt erhoben.

Eine solche Vorgehensweise ist um so problematischer, als technische Alternativen existieren, die weitaus datenschutzfreundlicher sind. Im öffentlichen Nahverkehr können – wie skandinavische und auch deutsche Projekte aufzeigen – Wertkartensysteme eingesetzt werden, bei denen im voraus bezahlt wird und die daher gänzlich ohne personenbezogene Daten auskommen.

Die Datenschutzbeauftragten halten es daher für dringend erforderlich, daß mehr als bisher bei der Einführung kartengestützter Zahlungssysteme darauf geachtet wird, die „datenfreie Fahrt" zu ermöglichen. Im Öffentlichen Nahverkehr sollte weiterhin auch die datenschutzfreundliche Lösung angeboten werden: der Kauf einer Fahrkarte am Automaten mit Bargeld.

Die Konferenz fordert weiter, daß noch vor der Pilotierung der dargestellten Technikvorhaben im Verkehrsbereich eine Untersuchung möglicher Alternativen, eine Analyse der von ihnen ausgehenden Gefahren für das informationelle Selbstbestimmungsrecht und eine Darstellung der technischen und organisatorischen Möglichkeiten zur Gewährleistung des Persönlichkeitsschutzes zu erstellen ist (Technikfolgen-Abschätzung). Nur Verfahren mit dem geringsten Eingriff in das allgemeine Persönlichkeitsrecht sollten eine Chance zur Erprobung erhalten.

Anlage 2

Entschließung
der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 zur Gefährdung der Vertraulichkeit der Funkkommunikation von Sicherheitsbehörden und Rettungsdiensten

Durch die Aufhebung der bisher gültigen Beschränkungen der zulässigen Empfangsbereiche für Rundfunkempfänger zum 30. Juni 1992 werden zunehmend Empfangsgeräte betrieben, die das Abhören des Funkverkehrs ermöglichen. Dies stellt eine erhebliche Bedrohung des Fernmeldegeheimnisses dar.

Die Datenschutzbeauftragten des Bundes und der Länder beobachten die damit verbundene Gefährdung der Vertraulichkeit der Funkkommunikation von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) mit Sorge. Sie erkennen die Bemühungen der Polizeiverwaltungen der Länder an, durch zusätzliche technische Maßnahmen die Sicherheit des Sprechfunks zu erhöhen. Sie stellen jedoch fest, daß die erforderliche Vertraulichkeit bisher nicht gewährleistet werden konnte. Auch Sprachverschleierungssysteme erreichen diese nicht hinreichend.

Daher begrüßt die Konferenz die im Rahmen des Schengener Abkommens getroffene grundsätzliche Entscheidung, im BOS-Bereich eine europäische Normierung zu erarbeiten, die die Digitalisierung und eine Verschlüsselung des BOS-Funkverkehrs vorsieht.

Die Konferenz hält es für erforderlich, daß das Normierungsverfahren so zügig wie möglich durchgeführt wird und auch schon vor der Umsetzung dieser Norm alle Möglichkeiten für einen effektiven Schutz der Vertraulichkeit des BOS-Funkverkehrs entsprechend dem jeweiligen Stand der Technik genutzt werden.

Die Konferenz weist weiter darauf hin, daß nicht nur bei den Behörden der Polizei, sondern auch in anderen BOS-Bereichen, wie z. B. dem Rettungswesen, eine Vertraulichkeit des Funkverkehrs zu gewährleisten ist. Daher sind auch in den übrigen BOS-Bereichen frühestmöglich entsprechende Absicherungen zur Vertraulichkeit des Funkverkehrs gefordert.

Anlage 3

Entschließung
der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 zu regelmäßigen Datenübermittlungen an die öffentlich-rechtlichen Rundfunkanstalten und die Gebühreneinzugszentrale (GEZ) (gegen die Stimme Bayerns und bei Stimmenthaltung Sachsens)

Die öffentlich-rechtlichen Rundfunkanstalten drängen seit langem auf die Schaffung einer Rechtsgrundlage für die regelmäßige Übermittlung von Meldedaten aller Einwohner an die gemeinsame Gebühreneinzugszentrale (GEZ). Sie verweisen dazu auf bereits bestehende Regelungen in den Ländern Hessen und Nordrhein-Westfalen. Auf Bitten der Konferenz der Regierungschefs der Länder hat deshalb nunmehr der zuständige Arbeitskreis der Innenministerkonferenz einen Musterentwurf für eine bundesweite Lösung im Melderecht erarbeitet. Der Entwurf sieht vor, daß künftig alle Meldebehörden in der Bundesrepublik im Fall der Anmeldung, Abmeldung oder des Todes eines volljährigen Bewohners bis zu acht Monaten an die GEZ übermitteln dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen eine derartige Regelung aus folgenden Gründen ab:

Die Regelung könnte im Ergebnis zu einem bundesweiten Melderegister bei Volljährigen führen. Sie könnte außerdem gegen das verfassungsrechtlich garantierte Verhältnismäßigkeitsprinzip verstoßen. Den Rundfunkanstalten stünde möglicherweise der unkontrollierte Zugriff auf Millionen personenbezogener Daten volljähriger Einwohner der Bundesrepublik zu, obwohl es für die Rundfunkanstalten nur von Interesse ist, welcher Einwohner bei ihnen gebührenpflichtig ist und bislang seine Gebührenpflicht nicht angemeldet hat. Das vorgesehene generelle Übermittlungsverfahren kennt keine Unterscheidung zwischen erforderlichen und nicht erforderlichen Daten, sondern überläßt diese Unterscheidung der GEZ. Über die Frage, ob ein Volljähriger überhaupt gebührenpflichtig ist, geben die Meldedaten keine Auskunft. Das muß nach wie vor im herkömmlichen Verfahren durch Befragung ermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder sind bereit, an geeigneten und verfassungskonformen Lösungen der Landesregierungen zur Sicherung des Gebührenaufkommens der Rundfunkanstalten mitzuwirken.

Anlage 4

Entschließung
der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 zur Gewährleistung des Datenschutzes bei Mobilkommunikation

Die Verbreitung mobiler Sprach- und Datenübertragungsdienste hat in jüngster Vergangenheit stark zugenommen. So gibt es bereits jetzt in Deutschland mehr als eine Million Teilnehmer der Funktelefonnetze C und D; mit der Aufnahme des Regelbetriebs von MODACOM ist seit Juni dieses Jahres auch ein öffentlicher mobiler Datenübertragungsdienst in Deutschland verfügbar. Es ist zu erwarten, daß sich die Teilnehmerzahl mobiler Kommunikationsdienste in Zukunft vergrößern wird.

Die mit der Nutzung von Mobilfunkdiensten verbundenen Vorteile gehen mit Gefährdungen für den Datenschutz einher. Neben den auch bei anderen Telekommunikationsdiensten gespeicherten Angaben, wer wann mit wem in Verbindung war, wird bei der Mobilkommunikation auch erhoben, wo sich der mobile Teilnehmer jeweils aufhält. Die Speicherung dieser Daten ermöglicht die Bildung von problematischen Bewegungsprofilen.

Darüber hinaus ist vielfach auch die Vertraulichkeit der Kommunikationsinhalte gefährdet, insbesondere dann, wenn Daten unverschlüsselt per Funk übertragen werden. Dies gilt sowohl für die analogen Funktelefon-Netze B und C als auch für den von der Deutschen Bundespost Telekom betriebenen mobilen Datenübertragungsdienst MODACOM. Bei satellitengestützten Diensten ist es sogar möglich, die übertragenen Daten im gesamten, teilweise viele tausend Quadratkilometer umfassenden Abstrahlbereich des Satelliten unbemerkt anzuhören und aufzuzeichnen.

Von den Herstellern und Betreibern mobiler Kommunkationsdienste ist zu fordern, daß sie diesen Gefahren für das Fernmeldegeheimnis und für den Datenschutz durch eine entsprechende Gestaltung entgegenwirken und technische Vorkehrungen für eine sichere Kommunikation treffen.

Die Teilnehmer mobiler Kommunikationsdienste müssen von den Anbietern, Herstellern und Betreibern über die mit der Nutzung verbundenen Risiken und das erreichte Sicherheitsniveau aufgeklärt werden. Sofern bei bestimmten Diensten Sicherheitsmerkmale realisiert sind – wie z. B. in den digitalen D-Netzen –, muß die Sicherheit für die Aufsichts- und Kontrollorgane auch nachprüfbar sein. Falls durch den Dienstbetreiber nicht die erforderliche Sicherheit gewährleistet werden kann, ist eine Übertragung personenbezogener oder sonstiger sensibler Daten mit dem jeweiligen Dienst nur dann vertretbar, wenn der Benutzer zusätzlich Sicherheitsvorkehrungen trifft, also z. B. die übertragenen Daten anwendungsseitig verschlüsselt.

Zusätzlich kompliziert wird die Datenschutzproblematik bei der Mobilkommunikation dadurch, daß unter Umständen bei verschiedenen Dienst- und Netzbetreibern, aber auch bei anderen Unternehmen – den sogenannten Service-Providern, die lediglich Dienste vermarkten –, personenbezogene Daten gespeichert werden.

Hier muß im Zuge der anstehenden Überarbeitung des Telekommunikationsrechts dafür Sorge getragen werden, daß sich die Verarbeitung der Kommunikationsdaten auf das wirklich erforderliche Maß beschränkt und daß die Nutzer darüber aufgeklärt werden, bei welcher Stelle welche personenbezogenen Daten gespeichert oder sonst verarbeitet werden.

Besonders problematisch ist es, wenn bei der internationalen Mobilkommunikation auch in solchen Staaten personenbezogene Daten gespeichert werden, in denen kein ausreichendes Datenschutzniveau gewährleistet ist oder in denen das Fernmeldegeheimnis nicht sichergestellt wird. Deshalb ist es erforderlich, auf internationaler Ebene Regelungen zu treffen, die den Datenschutz bei mobilen Kommunikationsdiensten gewährleisten.

Die Konferenz unterstreicht aus diesem Grunde ihre Forderung, die Arbeiten der EG-Richtlinie über den Datenschutz im ISDN und in öffentlichen digitalen Mobilfunknetzen zu einem datenschutzrechtlich befriedigenden Abschluß zu bringen. Auch für den noch gänzlich datenschutzrechtlich ungeregelten Bereich der Satellitenkommunikation müssen endlich völkerrechtlich verbindliche Regelungen getroffen werden.

Anlage 5

Entschließung
der 46. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 26./27. Oktober 1993
zum Integrierten Verwaltungs- und Kontrollsystem (InVeKoS)
(Verordnungen der EWG Nrn. 3508/92 und 3887/92)

Die vom Ministerrat der EG 1992 beschlossene Reform der gemeinsamen Agrarpolitik sieht die Angleichung der gemeinschaftlichen Preise für bestimmte Kulturpflanzen an den Weltmarkt vor und gewährt auf Antrag als Ausgleich für die dadurch bedingten Einkommenseinbußen flächen- und tierbezogene Zuwendungen an die Erzeuger. Zur Verhinderung einer mißbräuchlichen Verwendung von Fördermitteln hat die EG die Mitgliedstaaten dabei zur Einführung eines „Integrierten Verwaltungs- und Kontrollsystems (InVeKoS) verpflichtet. Diese haben danach integrierte Datenbanken mit Angaben über Flurstücke, deren kulturartige Nutzung sowie den Tierbestand einzurichten und in einem Mindestumfang entsprechende Kontrollen durchzuführen.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder hat die EG mit dem „Integrierten Verwaltungs- und Kontrollsystem" den Landwirtschaftsverwaltungen der Länder ein Überwachungssystem verordnet, das dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot, widersprechen kann. Insbesondere legt das EG-Recht für die Kontrolldichte nur ein Mindestmaß an Kontrollen, jedoch keine Obergrenze fest.

Zur Vermeidung unverhältnismäßiger Einschränkungen des informationellen Selbstbestimmungsrechts der betroffenen Landwirte fordern daher die Datenschutzbeauftragten des Bundes und der Länder,

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

Anlage 6

Entschließung
der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993
Datenschutz bei der Privatisierung der Deutschen Bundespost Telekom und bei der europaweiten Liberalisierung des Telefonnetzes und anderer Telekommunikationsdienste

Im Zuge der sog. Postreform II soll die Deutsche Bundespost Telekom – nach der dafür notwendigen Änderung des Grundgesetzes – in Form einer Aktiengesellschaft privatisiert werden. Zugleich hat der Ministerrat der Europäischen Gemeinschaft in seiner Entschließung vom 22. Juli 1993 (Amtsblatt der EG Nr. C 213 vom 6. August 1993) seine Entschlossenheit bekräftigt, die Monopole im öffentlichen Sprachtelefondienst (Festnetz) der Mitgliedstaaten bis zum 1. Januar 1998 zu beseitigen.

In absehbarer Zeit werden daher in Deutschland neben der „Telekom AG" auch im Telefondienst andere private Unternehmen Telekommunikationsdienstleistungen anbieten. Diese Privatisierung hat Konsequenzen für den Datenschutz, der bisher für die Deutsche Bundespost Telekom auf einem vergleichsweise hohen Niveau geregelt ist. Insbesondere das grundgesetzlich garantierte Fernmeldegeheimnis würde für private Netzbetreiber und Dienstanbieter jedenfalls nicht mehr unmittelbar gelten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für unabdingbar, daß durch die Privatisierung und Liberalisierung der Schutz der Bürger insbesondere in solchen Bereichen nicht verringert wird, die – wie der Telefondienst – der Daseinsvorsorge zuzurechnen sind. So wie bisher die konkurrierenden privaten Betreiber der Mobilfunknetze einen gleichmäßig hohen Datenschutzstandard gewährleisten müssen, hat dies auch zu gelten, wenn in Zukunft private Unternehmen im Wettbewerb miteinander stationäre Telefonnetze betreiben und entsprechende Dienste anbieten. Die Einhaltung von datenschutzrechtlichen Bestimmungen bei Telekommunikationsnetzen und -diensten muß zukünftig von einer unabhängigen Stelle nach bundesweit einheitlichen Kriterien und von Amts wegen kontrolliert werden können.

Da der Wettbewerb zwischen privaten Netzbetreibern und Dienstanbietern nicht nur national begrenzt, sondern im europäischen Binnenmarkt stattfinden wird, sind auch Rechtsvorschriften der Europäischen Gemeinschaft erforderlich, die einen möglichst hohen, einheitlichen Datenschutzstandard in der Telekommunikation gewährleisten.

Anlage 7

Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 zu Chipkarten im Gesundheitswesen

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

Chipkarte als gesetzliche Krankenversichertenkarte

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

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

Chipkarte als freiwillige Gesundheitskarte

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

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

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

So stellt beispielsweise eine Kasse ihren Mitgliedern Bonuspunkte in Aussicht, wenn sie auf sog. Aktionstagen der Kasse Werte wie Blutzucker, Sauerstoffdynamik, Cholesterol sowie weitere spezielle medizinische Daten ohne ärztliche Konsultation messen und auf der Karte speichern und aktualisieren lassen. In Abhängigkeit von der Veränderung dieser Werte wird von der Kasse gegebenenfalls ein Arztbesuch empfohlen. Die Vergabe solcher Bonuspunkte widerspricht dem Prinzip der Freiwilligkeit bei der Erhebung der Daten für die Patienten-Chipkarte. Der Effekt wird noch verstärkt, indem die Kasse die „Möglichkeit einer Beitragsrückerstattung" in Aussicht stellt. Die Datenschutzbeauftragten des Bundes und der Länder sehen in dieser Art der Anwendung der Chipkarten-Technik das Risiko eines Mißbrauchs, solange der Inhalt und die Nutzung der Daten nicht mit den zuständigen Fachleuten – wie den Medizinern – und den Krankenkassen abgestimmt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält für den Einsatz und die Nutzung freiwilliger Patienten-Chipkarten zumindest – vorbehaltlich weiterer Punkte – die Gewährleistung folgender Voraussetzungen für erforderlich:

- Die Zuteilung einer Gesundheitskarte und die damit verbundene Speicherung von Gesundheitsdaten bedarf der schriftlichen Einwilligung des Betroffenen. Er ist vor der Erteilung der Einwilligung umfassend über Zweck, Inhalt und Verwendung der angebotenen Gesundheitskarte zu informieren.
- Die freiwillige Gesundheitskarte darf nicht – etwa durch Integration auf einem Chip – die Krankenversichertenkarte nach dem Sozialgesetzbuch verdrängen oder ersetzen.
- Die Karte ist technisch so zu gestalten, daß für die einzelnen Nutzungsarten nur die jeweils erforderlichen Daten zur Verfügung gestellt werden.

- Der Betroffene muß von Fall zu Fall frei und ohne Benachteiligung – z. B. gegenüber dem Arzt, der Krankenkasse oder der Versicherung – entscheiden können, die Gesundheitskarte zum Lesen der Gesundheitsdaten vorzulegen und ggf. den Zugriff auf bestimmte Daten zu beschränken. Er muß ferner frei entscheiden können, wer welche Daten in seinen Datenbestand übernehmen darf. Der Umfang der Daten, die gelesen oder übernommen werden dürfen, ist außerdem durch die gesetzliche Aufgabenstellung bzw. den Vertragszweck der Nutzer beschränkt.
- Der Kartenaussteller muß sicherstellen, daß der Betroffene jederzeit vom Inhalt der Gesundheitskarte unentgeltlich Kenntnis nehmen kann.
- Der Betroffene muß jederzeit Änderungen und Löschungen der gespeicherten Daten veranlassen können.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dafür aus, daß der Gesetzgeber dies durch bereichsspezifische Rechtsgrundlagen sicherstellt.

Anlage 8

Entschließung
der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 zur Informationsverarbeitung im Strafverfahren (bei Stimmenthaltung Bayerns)

Die Datenschutzbeauftragten des Bundes und der Länder erinnern an ihre Vorschläge zu gesetzlichen Regelungen der Informationsverarbeitung im Strafverfahren, die sie seit 1981 unterbreitet haben.

Während die Befugnisse von Polizei und Staatsanwaltschaft zur Datenerhebung bei Ermittlungen mittlerweile in weitreichender Form gesetzlich abgesichert wurden, fehlen weiterhin Regelungen in der Strafprozeßordnung, wie die erhobenen Daten in Akten und Dateien weiter verarbeitet werden dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder halten die Beachtung folgender Grundsätze für notwendig, die in den Entwürfen des Bundes (Art. 4 §§ 474 ff. StPO des Entwurfs für ein Verbrechensbekämpfungsgesetz – Bundestagsdrucksache 12/6853) und der Länder (Entwurf eines Strafverfahrensänderungsgesetzes 1994 des Strafrechtsausschusses der Justizministerkonferenz) nicht ausreichend berücksichtigt sind:

1. Strafrechtliche Ermittungsakten enthalten eine Vielzahl höchstsensibler Daten insbesondere auch über Opfer von Straftaten und Zeugen, die deshalb eines wirksamen Schutzes bedürfen. Es würde den Besonderheiten der im Strafverfahren – auch mit Zwangsmitteln – erhobenen Daten nicht entsprechen, wenn Strafakten als Informationsquelle für jegliche Zwecke anderer Behörden oder von nicht am Strafverfahren Beteiligten dienten. Die einzelnen Zwecke und die zugriffsberechtigten Stellen sind daher abschließend normenklar festzulegen.

1.1 Insgesamt ist sicherzustellen, daß der in anderen Zweigen der öffentlichen Verwaltung verbindlich geltende Standard des Datenschutzes für Übermittlungen keinesfalls unterschritten wird.

1.2 Soweit ein unabweisbarer Bedarf anderer Stellen an Informationen aus Strafverfahren besteht, ist er in erster Linie durch Erteilung von Auskünften zu befriedigen. Akteneinsichtnahmen oder Aktenübersendungen können erst dann zugelassen werden, wenn eine Auskunftserteilung nicht ausreicht. Nicht erforderliche Aktenteile müssen ausgesondert werden. An Privatpersonen dürfen Informationen aus strafrechtlichen Ermittlungen nur weitergegeben werden, wenn deren rechtliche Interessen davon abhängen.

2. Bei Regelungen zur dateimäßigen Speicherung ist zu unterscheiden zwischen Systemen zur Vorgangsverwaltung (wie z. B. zentrale Namensdateien) und Dateien, die der Unterstützung strafprozessualer Ermittlungen dienen (z. B. Spurendokumentations- und Recherchesysteme).

2.1 Der Datensatz zur Vorgangsverwaltung ist auf die Angaben zu beschränken, die zum Auffinden der Akten und zur Information über den Verfahrensstand erforderlich sind. Daten über Personen, die keine Beschuldigten sind, dürfen nur dann erfaßt werden, wenn dies zur Vorgangsverwaltung zwingend erforderlich ist. In diesen Fällen bedarf es besonderer Zugriffs- und Verwendungsbeschränkungen.

In jedem Fall sind die Daten entsprechend dem Verfahrensstand zu aktualisieren. Vom Gesetzgeber sind konkrete Löschungsfristen vorzusehen. Die Speicherung ist längstens auf den Zeitpunkt zu begrenzen, für den die Akte aufbewahrt wird. Vorgangsverwaltungssysteme können so auch für eine wirksame Kontrolle der Aufbewahrungsfristen genutzt werden.

2.2 Die Staatsanwaltschaft kann sich zur Verwaltung ihres konventionell gespeicherten Datenmaterials grundsätzlich eines behördeninternen, automatisierten Nachweissystems bedienen. Länderübergreifende automatisierte Informationssysteme dürfen in Beachtung des Erforderlichkeitsprinzips demgegenüber allenfalls für solche Vorgänge errichtet werden, bei denen bestimmte Tatsachen die Prognose begründen, daß auf die erfaßten Daten zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben (erneut) zugegriffen werden muß.

Eine solche Prognose wird in der Regel dann nicht gerechtfertigt sein, wenn das zugrundeliegende Verfahren mit einer Einstellung nach § 170 Abs. 2 StPO oder einem rechtskräftigen Freispruch abgeschlossen worden ist, sofern nicht auch nach Abschluß des Verfahrens noch tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte eine strafbare Handlung begangen hat. Eine Bereitstellung von Daten jedenfalls zu Zwecken der Strafverfolgung wird ferner grundsätzlich

dann nicht in Betracht kommen, wenn die Ermittlungen konkrete Anhaltspunkte dafür bieten, daß der Beschuldigte nicht erneut strafbare Handlungen begehen wird. Dies kann z. B. bei Fahrlässigkeitstaten der Fall sein. Bei laufenden Verfahren kann die Zulässigkeit der Aufnahme von Daten im Hinblick auf die Möglichkeiten einer Verbindung von Verfahren, die Einstellung nach § 154 StPO oder die Gesamtstrafenbildung gegeben sein.

2.3 Für einen Informationsverbund zwischen verschiedenen speichernden Staatsanwaltschaften mit der Möglichkeit eines Direktzugriffs auf die Daten der jeweils anderen Behörden ergibt sich als Voraussetzung, daß die Weitergabe aller dem Zugriff unterliegenden Daten zumindest bei abstrakter Betrachtung zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben der übermittelnden oder der zugriffsberechtigten Stellen geeignet und angemessen sein muß.

Für den Bereich der Strafverfolgung gilt ein umfassendes Aufklärungsgebot (§§ 152 Abs. 2, 160 StPO). Die Staatsanwaltschaft kann im Rahmen ihrer Ermittlungen grundsätzlich ohne Rücksicht auf das Gewicht des Tatvorwurfs von allen öffentlichen Behörden – also auch von anderen Staatsanwaltschaften – Auskunft verlangen (§ 161 Satz 1 StPO). Diese Auskunftspflicht besteht über das Ermittlungsverfahren hinaus bis zum Abschluß des Strafverfahrens. Daten, die im Falle einer entsprechenden Anfrage zu mit einem Strafverfahren zusammenhängenden Zwecken offenbart werden müßten, können damit – ungeachtet der besonderen Voraussetzungen für die Errichtung eines Direktabrufverfahrens – von jeder Staatsanwaltschaft für andere Staatsanwaltschaften grundsätzlich auch in einem Informationssystem mit Direktabrufmöglichkeit bereitgestellt werden, sofern nur bestimmte Tatsachen die Annahme rechtfertigen, daß die Daten in einem Verfahren einer anderen Behörde verwertet werden müssen. Eine solche Annahme wird regelmäßig wiederum in den unter 2.2 dargestellten Fällen nicht zu begründen sein. Eine Bereitstellung von Daten wird darüber hinaus auch dann nicht erfolgen können, wenn diese einem besonderen Amtsgeheimnis unterliegen und deshalb auch auf Anforderung nicht ohne weiteres übermittelt werden dürften. Auf § 78 SGB X ist in diesem Zusammenhang hinzuweisen. Ein Direktabruf durch andere Stellen als Staatsanwaltschaften ist schon nach der Zweckbestimmung des Systems ausgeschlossen.

2.4 In der Praxis dienen derzeit die bestehenden polizeilichen Informationssysteme auch den Zwecken der Strafverfolgung. Eine Abstimmung der polizeilichen und der staatsanwaltschaftlichen Informationssysteme ist geboten. Eine weitere Abstimmung wird im Hinblick auf das Bundeszentralregister zu erfolgen haben, das ebenfalls Daten zu Zwecken der Strafverfolgung, aber auch der Strafvollstreckung speichert.

Die Datenschutzbeauftragten halten daher eine grundlegende Überarbeitung dieser Entwürfe für notwendig und bieten hierfür ihre Unterstützung an (vgl. Beschlüsse der Datenschutzkonferenzen vom 28./29. September 1981 zu „Mindestanforderungen für den Datenschutz bei den Zentralen Namenskarteien der Staatsanwaltschaften", vom 24./25. November 1986 „Überlegungen zu Regelungen der Informationsverarbeitung im Strafverfahren" und vom 5./6. April 1989 zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts vom 3. November 1988).

Anlage 9

Entschließung
der 47. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 9./10. März 1994
zum Gesetzentwurf der Bundesregierung
zur Neuordnung des Postwesens und der Telekommunikation
(Postneuordnungsgesetz – PTNeuOG, Bundesratsdrucksache 115/94 = Bundestagsdrucksache 12/6718)
und zu der dafür erforderlichen Änderung des Grundgesetzes
(Bundesratsdrucksache 114/94 = Bundestagsdrucksache 12/6717)

I.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, daß mit der Umwandlung der Deutschen Bundespost POSTDIENST in die Deutsche Post AG und der Deutschen Bundespost TELEKOM in die Deutsche Telekom AG zwei staatliche Einrichtungen aufhören zu existieren, gegenüber denen sich der Bürger bisher unmittelbar auf das Post- und Fernmeldegeheimnis berufen kann. Sie treten deshalb dafür ein, in der Verfassung sicherzustellen, daß jeder, der Post- und Fernmeldedienstleistungen erbringt, das Post- und Fernmeldegeheimnis zu wahren hat.

II.

Im Gesetz zur Neuordnung des Postwesens und der Telekommunikation ist ein den Vorgaben des Bundesverfassungsgerichts in seinem Volkszählungsurteil vom 15. Dezember 1983 und in seinem Fangschaltungsbeschluß vom 25. März 1992 entsprechender Schutz von Individualrechten zu gewährleisten.

Die Datenschutzbeauftragten halten inbesondere folgende Änderungen des Gesetzentwurfs für erforderlich:

a) Der Umfang der zulässigen Verarbeitung personenbezogener Daten im Post- und Telekommunikationswesen ist im Gesetz selbst festzulegen; lediglich deren konkrete Ausgestaltung kann der Regelung durch Rechtsverordnungen überlassen bleiben.

b) Die Gewährleistung des Datenschutzes und des Post- und Fernmeldegeheimnisses muß in den Katalog der Ziele der Regulierung aufgenommen werden.

c) Das Post- und Telekommunikationswesen muß auf Dauer – auch nach dem Wegfall der Monopole – einer effektiven, unabhängigen datenschutzrechtlichen Kontrolle von Amts wegen nach bundesweit einheitlichen Kritierien unterworfen bleiben, auch soweit personenbezogene Daten nicht in Dateien verarbeitet werden.

d) Die Frist für die Speicherung von Verbindungsdaten zur Ermittlung und zum Nachweis der Entgelte ist präzise festzulegen.

e) Die vorgesehene Vorschrift zum Einzelentgeltnachweis schränkt den Kreis der Einrichtungen, die Telefonberatung durchführen und die nicht auf Einzelentgeltnachweisen erscheinen sollen, in unakzeptabler Weise ein. Dem Schutz des informationellen Selbstbestimmungsrechtes und des Fernmeldegeheimnisses der Angerufenen würde es dagegen am ehesten entsprechen, wenn jeder inländische Anschlußinhaber selbst entscheiden kann, ob und gegebenenfalls wie seine Rufnummer auf Einzelentgeltnachweisen erscheinen soll. Damit wäre auch die Anonymität von Anrufen bei Beratungseinrichtungen unbürokratisch sicherzustellen. Ein entsprechendes Verfahren wird in den Niederlanden bereits praktiziert.

f) Es wäre völlig unangemessen, wenn in Zukunft erlaubt würde, daß die Telekommunikationsunternehmen Nachrichteninhalte über die Befugnisse des § 14 a Fernmeldeanlagengesetz hinaus auch für die Unterbindung von Leistungserschleichungen und sonstiger rechtswidriger Inanspruchnahme des Telekommunikationsnetzes und seiner Einrichtungen sowie von Telekommunikations- und Informationsdienstleistungen erheben, verarbeiten und nutzen dürften.

III.

Die Datenschutzbeauftragten betonen, daß angesichts der neuen technischen Möglichkeiten digitaler Kommunikations- und Informationsdienste und der mit ihrer Nutzung zwangsläufig verbundenen Datenverarbeitung eine grundlegende Überarbeitung des § 12 Fernmeldeanlagengesetz, der die Weitergabe vorhandener Telekommunikationsdaten in Strafverfahren erlaubt, überfällig ist. Sie erinnern an die Umsetzung der entsprechenden Entschließung des Bundesrates vom 27. August 1991 (Bundesratsdrucksache 416/91).

Anlage 10

Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 zum Ausländerzentralregister (gegen die Stimme Bayerns)

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

Die Datenschutzbeauftragten des Bundes und der Länder haben immer wieder darauf hingewiesen, daß die Führung eines derartigen Registers ohne gesetzliche Regelung mit dem vom Grundgesetz Deutschen wie Ausländern gleichermaßen garantierten Recht auf informationelle Selbstbestimmung unvereinbar ist. Sie begrüßen daher, daß mit dem am 2. März 1994 vom Bundeskabinett beschlossenen Entwurf für ein Ausländerzentralregistergesetz eine gesetzliche Grundlage geschaffen werden soll.

Zwar enthält dieser Gesetzentwurf gegenüber früheren Entwürfen eine Reihe datenschutzrechtlicher Verbesserungen, Bedenken bestehen jedoch weiterhin: Die Datenschutzbeauftragten wenden sich insbesondere dagegen, daß das Ausländerzentralregister nicht nur als Informations- und Kommunikationssystem für die mit der Durchführung ausländer- und asylrechtlicher Vorschriften betrauten Behörden dienen, sondern darüber hinaus als Informationsverbund für Aufgaben der Polizei, Strafverfolgungsorgane und Nachrichtendienste zur Verfügung stehen soll.

Die Funktionserweiterung wird deutlich durch die Speicherung von Erkenntnissen der Sicherheitsbehörden zu Ausländern in das Register. So soll der INPOL-Fahndungsbestand des BKA, soweit er Ausschreibungen zur Festnahme und zur Aufenthaltsermittlung von Ausländern enthält, in das Ausländerzentralregister übernommen werden. Gleiches gilt für die vorgesehene Speicherung von Angaben zu Personen, bei denen Anhaltspunkte für den Verdacht bestehten, daß sie im einzelnen bezeichnete Straftaten planen, begehen oder begangen haben. Diese Informationen dienen nicht einem Informationsbedarf zur Erfüllung ausländerbehördlicher Aufgaben, sondern – worauf die Entwurfsbegründung hinweist – der Kriminalitätsbekämpfung. Für diese Zwecke stehen den Sicherheitsbehörden aber eigene Informationssysteme zur Verfügung. Nach Auffassung der Datenschutzbeauftragten dürfen deshalb derartige Erkenntnisse nicht in das Register aufgenommen werden.

Die im Entwurf vorgesehenen Voraussetzungen, unter denen u. a. für Polizeibehörden, Staatsanwaltschaften und Nachrichtendienste automatisierte Abrufverfahren eingerichtet werden können, stellen keine wirksamen Vorkehrungen für eine Begrenzung der Abrufe dar. Besonders problematisch ist der geplante automatisierte Zugriff durch die Nachrichtendienste auf einen – wenn auch reduzierten – Datensatz. Für die Dienste ist in den jeweiligen bereichsspezifischen Gesetzen der automatisierte Abruf aus anderen Datenbeständen ausgeschlossen. Die Erforderlichkeit derartiger Abrufe ist in keiner Weise belegt. Die Datenschutzbeauftragten sprechen sich deshalb dafür aus, zumindest auf den automatisierten Abruf durch Nachrichtendienste zu verzichten.

Anlage 11

Entschließung
der 48. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 26./27. September 1994
zum Vorschlag der Kommission der Europäischen Union
für eine Verordnung (EG) des Rates
über die Tätigkeit der Gemeinschaft im Bereich der Statistik
– EG-Statistikverordnung –
(KOM [94] 78 endg.; Ratsdok. 5615/94 = Bundesratsdrucksache 283/94)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, daß die Europäische Union eine allgemeine Regelung für die Gemeinschaftsstatistik trifft, weisen allerdings darauf hin, daß die datenschutzrechtliche Entwicklung bei der Europäischen Union mit dem Aufbau der europäischen Statistik keineswegs Schritt gehalten hat.

Sie stellen mit Besorgnis fest, daß der vorliegende Vorschlag einer EG-Statistikverordnung die nationalen datenschutzrechtlichen Grundsätze und wesentliche Standards des Statistikrechts weitgehend nicht berücksichtigt. Sie fordern daher zur Wahrung des Rechts der Betroffenen auf informationelle Selbstbestimmung mit Nachdruck, daß die Bundesregierung ihre Bedenken gegen diesen Vorschlag geltend macht und diese bei den Beratungen auf europäischer Ebene zum Tragen bringt.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen ausdrücklich den Beschluß des Deutschen Bundesrates vom 8. Juli 1994 (Bundesratsdrucksache 283/94 – Beschluß –).

Gegen den vorgelegten Vorschlag einer Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik (EG-Statistikverordnung) erheben sie insbesondere die folgenden datenschutzrechtlichen Bedenken:

1. In Artikel 1 sollte als die zuständige Gemeinschaftsdienststelle unmißverständlich das Statistische Amt der Europäischen Gemeinschaften (EUROSTAT) bestimmt werden, weil die erforderlichen rechtlichen, administrativen, technischen und organisatorischen Maßnahmen – insbesondere zur Sicherung der Zweckbindung der zu statistischen Zwecken erhobenen Daten sowie zur Wahrung der statistischen Geheimhaltung – bei dieser Stelle bereits aufgrund der EG-Übermittlungsverordnung 1588/90 vom 11. Juni 1990 getroffen werden können. Eine jederzeit revidierbare Organisationsentscheidung der Kommission darüber, welche Dienststelle der Europäischen Union für statistische Aufgaben zuständig ist, birgt dagegen die Gefahr, daß Daten an unterschiedliche Stellen der Kommission zu unterschiedlichen Zwecken übermittelt werden.

   Zugleich sollte EUROSTAT zumindestens einen der Selbständigkeit der Statistischen Ämter in der Bundesrepublik Deutschland vergleichbaren organisationsrechtlichen Status erhalten, der die unter dem Gesichtspunkt der Objektivität und Neutralität gebotene Eigenständigkeit bei der Aufgabenerfüllung garantiert. Dies könnte anläßlich der für 1996 vorgesehenen Revision des Vertrages über die Europäische Union geschehen.

2. Das mehrjährige statistische Programm sollte nicht wie in Artikel 3 vorgesehen von der Kommission beschlossen werden. Die grundlegenden Entscheidungen über die Bürger belastende Datenerhebungen sollten dem Rat mit Zustimmung des Europäischen Parlaments vorbehalten bleiben. Dabei sollte der Planungscharakter des Programms in den Vordergrund gestellt werden.

3. Artikel 5 sollte festlegen, daß statistische Einzelmaßnahmen durch einen Rechtsakt gemäß dem Verfahren nach Artikel 189 b EG-Vertrag angeordnet werden. Dies gilt auch für die statistische Auswertung von Daten, die bei den administrativen Stellen bereits vorliegen (sog. Sekundärstatistik). Die im Vorschlag vorgesehene generelle Befugnis der Kommission, statistische Einzelmaßnahmen zu regeln, ist viel zu weitgehend.

4. Die in Artikel 12 vorgesehene Übertragung der Befugnis zur Organisation der Verbreitung der statistischen Daten auf die Kommission widerspricht dem Grundsatz der Subsidiarität nach Artikel 3 b EG-Vertrag, aus dem folgt, daß grundsätzlich die Mitgliedstaaten nach ihrem nationalen Recht zur Verbreitung der statistischen Daten zuständig sind. Ferner sollte in Artikel 12 festgelegt werden, daß an Stellen außerhalb der statistischen Gemeinschaftsdienststelle nur nichtvertrauliche statistische Daten übermittelt werden dürfen.

5. Der in Artikel 13 gegenüber der Definition in der EG-Übermittlungsverordnung 1588/90 neu definierte Begriff „statistische Geheimhaltung" muß präzisiert werden. Dazu gehört insbesondere, daß festgelegt wird, unter welchen Voraussetzungen statistische Daten vertraulich sind und nicht nur als vertraulich gelten. Dies gilt um so mehr, als im Verordnungsvorschlag dieser Begriff nicht nur in Artikel 13, sondern auch in Artikel 9 Abs. 2 – allerdings mit einem anderen Begriffsinhalt –

definiert wird. Der Begriff „statistische Geheimhaltung" sollte an einer Stelle in der Verordnung und so definiert werden, daß er Artikel 2 Nr. 1 der EG-Übermittlungsverordnung 1588/90 und damit den derzeit geltenden nationalen Begriffsbestimmungen entspricht. Dies stände auch im Einklang mit dem Grundsatz der Subsidiarität nach Artikel 3 b EG-Vertrag.

6. Gemäß dem Grundsatz der Subsidiarität sollte – ebenso wie die Befugnis zur Verbreitung statistischer Ergebnisse (Art. 11 Abs. 1) – auch die Festlegung der Zuständigkeit für die Durchführung der statistischen Einzelmaßnahmen (Art. 7) den Mitgliedstaaten überlassen bleiben.

7. Auch die in Artikel 16 vorgesehene generelle Zugangsregelung einzelstaatlicher Stellen und der Gemeinschaftsdienststelle zu Registern der Verwaltung widerspricht dem Grundsatz der Subsidiarität nach Artikel 3 b EG-Vertrag. Dieser gebietet hier, daß – jedenfalls grundsätzlich – die Mitgliedstaaten zu bestimmen haben, in welcher Weise sich die für die Erstellung der Gemeinschaftsstatistiken zuständigen nationalen Stellen Daten beschaffen. Damit ist aber nicht zu vereinbaren, daß auch Stellen der Kommission unmittelbar Zugang zu nationalen Verwaltungsregistern haben sollen.
   Ferner bleibt unklar, ob die nach Artikel 16 erhobenen Daten Erhebungs- oder Hilfsmerkmale sein sollen. Im übrigen darf über Artikel 16 ein Zugang zu solchen personenbezogenen Daten, die nach nationalem Recht einer besonderen Geheimhaltung, z. B. dem Steuer- oder auch dem Sozialgeheimnis unterliegen, nicht eröffnet werden.

8. Die Regelung des Artikels 17 ist mißglückt. Allem Anschein nach soll hier eine weitgehende Ausnahmeregelung von der statistischen Geheimhaltung zugunsten von Forschungsinstituten, einzelner Forscher und von für die Erstellung von Nichtgemeinschaftsstatistiken zuständigen Stellen vorgesehen werden, die die Möglichkeit eröffnet, die in diesem Bereich geltenden strengeren nationalen Regelungen zu umgehen. Außerdem würde von der für EUROSTAT geltenden EG-Übermittlungsverordnung 1588/90 abgewichen werden. Artikel 17 sollte deshalb so gefaßt werden, daß die nationalen Zugangsregelungen für Einrichtungen mit der Aufgabe der unabhängigen wissenschaftlichen Forschung nicht umgangen werden können.

9. Der Vorschlag der Kommission sieht weder eine alsbaldige Trennung und Aufbewahrung von Erhebungs- und Hilfsmerkmalen noch eine alsbaldige Löschung personenbezogener Hilfsmerkmale vor. In der Bundesrepublik Deutschland dagegen gehören entsprechende Regelungen (vgl. § 12 BStatG) zum Kernbereich des Statistikrechts. Im Volkszählungsurteil hat das Bundesverfassungsgericht ihnen grundrechtssichernde Bedeutung beigemessen.

10. Schließlich fehlt es für die Organe der Europäischen Union noch immer an einer unabhängigen und effektiven Datenschutzkontrollinstanz, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der Europäischen Union in seinen Rechten verletzt zu sein.

Anlage 12

Entschließung
der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994
zu:
Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen

Angesichts der aktuellen Diskussion über die innere Sicherheit weisen die Datenschutzbeauftragten des Bundes und der Länder darauf hin, daß umfangreiche polizeiliche Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten, insbesondere im technischen Bereich, gesetzlich verankert worden sind.

Zum Kreis der Betroffenen zählen dabei nicht nur Personen, gegen die Verdachtsgründe vorliegen, sondern auch nichtverdächtige Kontakt- und Begleitpersonen und Unbeteiligte, deren Schutz nach Auffassung der Datenschutzbeauftragten besonders wichtig ist.

Vor diesem Hintergrund schlagen die Datenschutzbeauftragten vor, den derzeitigen Erkenntnisstand über die Erforderlichkeit polizeilicher Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten sowie ihre Auswirkungen auf die Rechte der Betroffenen durch folgende Maßnahmen zu verbessern:

1. Die Datenschutzbeauftragten teilen die von einigen Innenministern vertretene Auffassung, daß bloße Angaben über Einsatzzahlen der besonderen Befugnisse zur Datenerhebung nur einen begrenzten Aussagewert haben. Aufschluß über die tatsächliche Praxis, ihre Erforderlichkeit und Verhältnismäßigkeit läßt sich nur durch Überprüfung und Auswertung der einzelnen Einsätze gewinnen. Hierzu müssen unter Beteiligung der Datenschutzbeauftragten und der Wissenschaft, insbesondere der Kriminologie und des Polizeirechts, objektive und nachprüfbare Auswertungskriterien entwickelt werden.
   Die Datenschutzbeauftragten begrüßen daher die Initiative für eine sog. Rechtstatsachensammlung, die Erhebungen zu polizeilichen Ermittlungsmethoden und Eingriffsbefugnissen durchführen soll. Sie schlagen vor, in diese Rechtstatsachensammlung insbesondere Angaben über den Anlaß einer Datenerhebung mit besonderen Mitteln, die Örtlichkeit und die Dauer der Maßnahme, den Umfang der überwachten Gespräche, den betroffenen Personenkreis sowie die Anzahl der ermittelten, verurteilten, aber auch der entlasteten Personen einzubeziehen. Derartige Aufstellungen wären nicht nur für elektronische Überwachungsmethoden, sondern auch für Observationen, den Einsatz verdeckter Ermittler und V-Personen sowie für Rasterfahndungen denkbar.

2. Einige Polizeigesetze verpflichten dazu zu überprüfen, ob es notwendig ist, bestehende Dateien weiterzuführen oder zu ändern. Dabei soll nicht nur darauf eingegangen werden, ob die Anwendungen, d. h. die Dateien, weiterhin erforderlich sind, sondern auch auf ihren Nutzen sowie auf ihre Schwachstellen und Mängel. Ferner sind Vorschläge zu machen, wie festgestellte Defizite beseitigt oder minimiert werden können.

3. Die Datenschutzbeauftragten gehen davon aus, daß sie bei den Überlegungen zur Rechtstatsachensammlung rechtzeitig beteiligt und die jeweiligen Materialien und Zwischenergebnisse mit ihnen erörtert werden.

Anlage 13

Entschließung
der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994
zu:
Fehlende bereichsspezifische gesetzliche Regelungen bei der Justiz

Obwohl seit dem Volkszählungsurteil des Bundesverfassungsgerichts mehr als zehn Jahre vergangen sind, werden im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet. Statt dessen sind in den letzten Jahren in zunehmendem Maße automatisierte Verfahren neu eingesetzt worden. Die Eingriffe in das Recht auf informationelle Selbstbestimmung stützen die Justizverwaltungen auf die Rechtsprechung des Bundesverfassungsgerichts zum sog. Übergangsbonus.

Die Datenschutzbeauftragten des Bundes und der Länder weisen im Hinblick auf die kommende Legislaturperiode den Bundesgesetzgeber erneut darauf hin, daß gesetzliche Regelungen im Bereich der Justiz überfällig sind. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Der zur Zeit dem Bundesrat vorliegende Entwurf eines Strafverfahrensänderungsgesetzes beispielsweise wird datenschutzrechtlichen Anforderungen in keiner Weise gerecht.

Im Bereich der Justiz fehlen ausreichende gesetzliche Regelungen für die

- Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien,
- Datenerhebung, -verarbeitung und -nutzung im Strafvollzug,
- Übermittlung von Daten aus den bei Gerichten geführten Registern (z. B. Grundbuch) und deren Nutzung durch die Empfänger,
- Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen (Justizmitteilungsgesetz),
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien.

Eine Berufung auf den sog. Übergangsbonus auf unbegrenzte Zeit steht nicht in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts. Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe in der neuen Legislaturperiode unverzüglich bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes des Bürgers entgegenwirken.

Anlage 14

Entschließung
der 48. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 26./27. September 1994
zu:
Datenschutzrechtliche Anforderungen
an ein Übereinkommen der Mitgliedstaaten der Europäischen Union
über die Errichtung eines europäischen Polizeiamtes (EUROPOL)

Die Datenschutzbeauftragten der Länder gehen gemeinsam mit dem Bundesdatenschutzbeauftragten davon aus, daß bei den Verhandlungen mindestens folgende Punkte berücksichtigt werden:

- Das Übereinkommen muß der verfassungsrechtlichen Kompetenzverteilung in Bund und Ländern für die Polizei entsprechen. Die materielle Verantwortung für die Datenverarbeitung muß, soweit die Daten von Landesbehörden erhoben worden sind, weiterhin bei den Ländern liegen. Davon bleiben die Zuständigkeiten und die dazugehörigen Befugnisse des BKA als nationale Stelle für den Informationsverkehr mit EUROPOL unberührt.

- Die Regelungen zur Verarbeitung personenbezogener Daten müssen präzise sein und dem Grundsatz der Verhältnismäßigkeit entsprechen. Beispielsweise erfüllen die in den bisherigen Entwürfen vorgesehenen Befugnisse zur europaweiten Speicherung von Daten unbeteiligter Personen diese Voraussetzungen nicht.

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

Anlage 15

Entschließung
der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 zu Artikel 12 Verbrechensbekämpfungsgesetz, zur Trennung von Polizei und Nachrichtendiensten

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

- Der BND erhält danach bei der Fernmeldeaufklärung auch Befugnisse, die auf eine gezielte Erhebung von Daten für polizeiliche Zwecke hinauslaufen können. Deshalb ist bei dem Vollzug des Gesetzes darauf zu achten, daß nicht gezielt Informationen gesammelt werden, die vom Auftrag des BND nicht umfaßt werden.

- Zwischen nachrichtendienstlichen Vorfelderkenntnissen und polizeilichen Zwangsmaßnahmen ist ein Filter erforderlich, der vor allem Unbeteiligte vor überzogenen Belastungen schützt.

Die Datenschutzbeauftragten fordern, für die Zusammenarbeit von Nachrichtendiensten und Polizei in der Durchführung und Gesetzgebung das Trennungsgebot strikt zu beachten. Dies gilt auch bei der Fernmeldeaufklärung des BND. Eine wirksame Kontrolle durch den Datenschutzbeauftragten in diesem sensiblen Bereich ist auch nach der Rechtsprechung des Bundesverfassungsgerichts sicherzustellen.

Anlage 16

Entschließung
der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994
zu:
Geänderter Vorschlag für eine Europäische Richtlinie zum Datenschutz im ISDN und in Mobilfunknetzen vom 13. Juni 1994
(KOM [94] 128 endg. – COD 288)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, daß die Europäische Kommission mit der Vorlage des geänderten Vorschlags für eine Richtlinie zum Datenschutz im ISDN ihre Absicht bekräftigt hat, unionsweit bereichsspezifische Regelungen für den Datenschutz in Telekommunikationsnetzen zu schaffen. Es kann kein Zweifel daran bestehen, daß die digitalen Telekommunikationsnetze in der Europäischen Union zunehmend zur wichtigsten Infrastruktur für die Verarbeitung personenbezogener Daten werden. Der Regelungsdruck wird erhöht durch die Tatsache, daß die Europäische Union die rechtlichen und technischen Voraussetzungen für die Liberalisierung der Telekommunikationsmärkte in weiten Bereichen bereits geschaffen hat und mehrere Mitgliedstaaten, darunter Deutschland, derzeit ihr nationales Telekommunikationsrecht auf die Vorgaben der EU umstellen.

Aus diesem Grund sollte der geänderte Vorschlag für eine ISDN-Richtlinie so bald wie möglich vom Ministerrat und vom Europäischen Parlament abschließend beraten werden. Die Bundesregierung sollte die deutsche Ratspräsidentschaft dazu nutzen, den geänderten Vorschlag für eine ISDN-Richtlinie im Rat behandeln zu lassen.

Dabei sollte sich die Bundesregierung insbesondere für folgende Verbesserungen des Richtlinienvorschlags aus datenschutzrechtlicher Sicht einsetzen:

1. Für Telekommunikationsorganisationen und Diensteanbieter müssen die gleichen gemeinschaftsrechtlichen Regelungen zum Datenschutz gelten. Die Verarbeitung personenbezogener Daten durch Diensteanbieter darf nicht privilegiert werden.

2. Die Beschränkung der Datenverarbeitung auf Zwecke der Telekommunikation sollte wieder in die Richtlinie aufgenommen werden. Der allgemeine Zweckbindungsgrundsatz der Datenschutzrichtlinie läßt die Zweckentfremdung schon bei „berechtigten Interessen" der Verarbeiter zu. Das ist angesichts zunehmender Diversifizierung der Aktivitäten von Netzbetreibern und Diensteanbietern eine zu weitgehende Lockerung der Zweckbindung im Telekommunikationsbereich.

3. Das ursprünglich vorgesehene Verbot, personenbezogene Daten zur Erstellung von elektronischen Profilen der Teilnehmer zu nutzen, sollte wieder in die Richtlinie aufgenommen werden.

4. Die Speicherung von Inhaltsdaten nach Beendigung der Übertragung sollte – wie im ursprünglichen Richtlinienentwurf vorgesehen – untersagt werden.

5. Die Vertraulichkeit der Kommunikationsbeziehungen und -inhalte (Fernmeldegeheimnis) sollte – wie es der ursprüngliche Richtlinienvorschlag ebenfalls vorsah – auf Unionsebene garantiert werden.

6. Um eine Harmonisierung des Gemeinschaftsrechts beim Einzelgebührennachweis zu erreichen, sollten konkrete Vorgaben in die Richtlinie aufgenommen werden, z. B. indem den angerufenen Teilnehmern die Aufnahme ihrer Rufnummer in Einzelgebührennachweise freigestellt wird.

7. Im Fall der Anrufweiterschaltung sollte die automatische Information des anrufenden Teilnehmers darüber, daß sein Anruf (z. B. bei einem Arzt) an einen Dritten weitergeschaltet wird, gewährleistet sein.

Die Konferenz begrüßt die im geänderten Vorschlag vorgesehene Kostenfreiheit für die verschiedenen Optionen der Anzeige der Rufnummer des Anrufers und für die Nichtaufnahme von Daten in das Teilnehmerverzeichnis (Telefonbuch).

Diese Vorschläge berücksichtigen das Subsidiaritätsprinzip und beschränken sich auf Änderungen, die zur Gewährleistung der Vertraulichkeit der Kommunikation in der Europäischen Union realisiert werden müssen. Zudem wird die Europäische Union insoweit im Rahmen ihrer ausschließlichen Zuständigkeit tätig. Die Konferenz bittet auch die Entscheidungsträger auf Unionsebene sowie die Datenschutzbehörden der anderen Mitgliedstaaten, diese Anregungen zu unterstützen.

Anlage 17

Entschließung
der 49. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 9./10. März 1995
zu:
Eingeschränkter Zugriff auf Versichertendaten
bei landesweiten oder überregionalen
gesetzlichen Krankenkassen

Die gesetzlichen Krankenkassen schließen sich zunehmend zu landesweiten oder überregionalen gesetzlichen Krankenkassen zusammen. Es stellt sich daher verstärkt die Frage, welche bzw. wie viele Geschäftsstellen solcher Krankenkassen umfassend auf alle gespeicherten Daten eines Versicherten zugreifen können. Die Datenschutzbeauftragten halten nur folgendes für vertretbar:

1. Geschäftsstellen einer Krankenkasse können ohne schriftliches Einverständnis des Versicherten nur auf einen „Stammdatensatz" zugreifen. Dieser „Stammdatensatz" darf nur den Namen, das Geburtsdatum, die Anschrift, die Krankenversichertennummer und die betreuende Geschäftsstelle des Versicherten umfassen.

2. Lediglich eine Geschäftsstelle kann umfassend auf den Datensatz eines Versicherten zugreifen, sofern der Versicherte nicht ausdrücklich und eindeutig schriftlich in derartige Zugriffsmöglichkeiten durch weitere Geschäftsstellen eingewilligt hat.

3. Vor der Einwilligung ist der Betroffene umfassend aufzuklären. Die Daten dürfen nur zweckgebunden verwendet werden.

Anlage 18

Entschließung
der 49. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 9./10. März 1995
zum
Entwurf eines Gesetzes über das Bundeskriminalamt (BKA-Gesetz)
– Bundesratsdrucksache 94/95 –

Zu den Beratungen des Entwurfs für ein Gesetz über das Bundeskriminalamt erklären die Datenschutzbeauftragten des Bundes und der Länder:

Auch aus Sicht des Datenschutzes ist es zu begrüßen, daß die seit langem überfälligen bereichsspezifischen Regelungen zur bundesweiten polizeilichen Datenverarbeitung insbesondere im polizeilichen Informationssystem (INPOL) nunmehr in das Gesetzgebungsverfahren eingebracht werden. Der Gesetzentwurf enthält im Vergleich zu den Vorentwürfen eine Reihe von Vorschriften, die datenschutzrechtlich positiv zu werten sind. Hierzu gehören:

- der Verzicht auf die im Vorentwurf vorgesehenen Befugnisse zur sog. „Feststellung des Anfangsverdachts";
- das Erfordernis der Einwilligung für die Speicherung von Daten über Zeugen und mögliche Opfer;
- Übermittlungsverbote bei überwiegenden schutzwürdigen Interessen der Betroffenen oder bei entgegenstehenden gesetzlichen Verwendungsregelungen;
- die Beachtung landesgesetzlicher Löschungsfristen.

Andererseits begegnet der Gesetzentwurf jedoch nach wie vor gewichtigen Bedenken, da er tiefe Eingriffe in die Rechte von Betroffenen ermöglicht, deren Voraussetzungen und Reichweite unklar oder nicht durch überwiegende Interessen der Allgemeinheit gerechtfertigt sind. Dies gilt insbesondere für

- die Verwendung des Begriffs der Straftaten von erheblicher Bedeutung ohne Definition, um welche Tatbestände es sich handelt, weil damit nicht mehr voraussehbar ist, wann die an diesen Begriff anknüpfenden Eingriffsbefugnisse zur Datenverarbeitung eröffnet sind;
- die Befugnisse der Zentralstelle zu selbständigen Datenerhebungen und Übermittlungen bis hin zum automatisierten Datenverbund mit ausländischen und zwischenstaatlichen Stellen ohne Einvernehmen mit den jeweils verantwortlichen Länderpolizeien;
- die unklare Abgrenzung der Datenverarbeitungsbefugnisse im Hinblick auf die unterschiedlichen Befugnisse zur Strafverfolgung, Gefahrenabwehr, Verhütung von Straftaten und Vorsorge für künftige Strafverfolgung sowie die fehlende klare Zweckbindungs- und Zweckänderungsregelung;
- die Befugnis zur verdeckten Datenerhebung aus Wohnungen ohne eindeutige Begrenzung auf den Schutz gefährdeter Ermittler.

Die Datenschutzbeauftragten fordern den Gesetzgeber auf, die Schwachstellen des Entwurfs auszuräumen. Insbesondere fordern sie klare verfassungskonforme Regelungen zur Auskunftserteilung an Betroffene und der Prüfrechte für INPOL-Daten dahin gehend, daß die Datenschutzkontrollrechte bei der datenschutzrechtlichen Verantwortung der Stellen anknüpfen, die die Speicherung im INPOL-System selbst vornehmen oder veranlassen.

Anlage 19

Entschließung
der 49. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 9./10. März 1995
zu:
Automatische Erhebung von Straßennutzungsgebühren

Gegenwärtig werden Systeme zur automatischen Erhebung von Straßenbenutzungsgebühren in mehreren Versuchsfeldern erprobt. Sie können im Rahmen der weiteren Entwicklung zu zentralen Komponenten umfassender Verkehrstelematiksysteme (z. B. Verkehrsinformation und -leitung) werden.

Mit der Einführung derartiger Verkehrstelematiksysteme besteht die Gefahr, daß personenbezogene Daten über den Aufenthaltsort von Millionen Verkehrsteilnehmern erhoben und verarbeitet werden. Exakte Bewegungsprofile können dadurch erstellt werden. Damit wären technische Voraussetzungen geschaffen, daß Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Derartige Datensammlungen wären aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil das Grundrecht auf freie Entfaltung der Persönlichkeit auch das Recht umfaßt, sich möglichst frei und unbeobachtet zu bewegen. Vor diesem Hintergrund ist es besonders wichtig, elektronische Mautsysteme datenschutzgerecht auszugestalten. Bei den anstehenden Entscheidungen sind andere Verfahren, wie z. B. die Vignette, einzubeziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, daß der Grundsatz der datenschutzgerechten Ausgestaltung von Systemen zur automatischen Erhebung von Straßenbenutzungsgebühren von allen Beteiligten am Feldversuch auf der BAB A 555 akzeptiert wird. Zur Umsetzung dieses Grundsatzes fordern die Datenschutzbeauftragten:

- Der Grundsatz der „datenfreien Fahrt" muß auch künftig gewährleistet sein. Über Verkehrsteilnehmer, die ordnungsgemäß bezahlen, dürfen keine Daten erhoben oder verarbeitet werden, die die Herstellung eines Personenbezugs ermöglichen. Es sind ausschließlich solche Zahlungsverfahren anzuwenden, bei denen die Abrechnungsdaten nur dezentral beim Verkehrsteilnehmer gespeichert werden. Die Verkehrsteilnehmer dürfen jedoch nicht gezwungen werden, einen lückenlosen Nachweis über ihre Bewegungen zu führen.

- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Möglichkeit einer flächendeckenden Kontrolle ist von vornherein technisch und rechtlich auszuschließen. Die Gebührenkontrolle ist so zu gestalten, daß die Identität des Verkehrsteilnehmers nur dann aufgedeckt wird, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Gebühren nicht entrichtet worden sind.

- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Verkehrsteilnehmer durchschaubar sein. Der Verkehrsteilnehmer muß jederzeit über sein Guthaben, die Abbuchung und den eventuellen Kontrollvorgang informiert sein.

- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, daß sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können. Die hierbei anzuwendenden Verfahren wären gesetzlich abschließend vorzugeben. Dabei ist sicherzustellen, daß anfallende personenbezogene Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen. Ferner ist zu gewährleisten, daß Betreiber derartiger Systeme – unabhängig von ihrer Rechtsform – einer Datenschutzkontrolle nach einheitlichen Kriterien unterliegen. Die Bundesregierung wird aufgefordert, bei der anstehenden internationalen Normierung elektronischer Mautsysteme die datenschutzrechtlichen Anforderungen durchzusetzen.

Anlage 20

Entschließung
der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995
zu
Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich

Bisher ist der Gesetzgeber im Bereich der Justiz den verfassungsrechtlichen Forderungen nach ausreichenden normenklaren Regelungen über die Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien nicht nachgekommen. So enthalten z. B. die bislang bekanntgewordenen Entwürfe zu einem Strafverfahrensänderungsgesetz nur unzureichende Generalklauseln. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder*) erklärt deshalb:

1. Aufbewahrung, Aussonderung und Vernichtung der Akten und die Speicherung personenbezogener Daten in Dateien im Bereich der Justiz müssen nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil für die Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden gesetzlich geregelt werden, wobei sich die Aufbewahrungsdauer am Recht auf informationelle Selbstbestimmung und am Zweck der Speicherung zu orientieren hat. Hierbei hat der Gesetzgeber die grundlegenden Entscheidungen zur Aufbewahrungsdauer selbst zu treffen. Aufgrund einer hinreichend konkreten Verordnungsermächtigung können die Einzelheiten durch Rechtsverordnung bestimmt werden.

2. Die derzeit bestehenden Aufbewahrungsfristen sind konsequent zu vereinfachen und zu verkürzen. Soweit geboten sind Verkürzungen vorzunehmen.

3. Die derzeit geltende generelle 30jährige Aufbewahrungsfrist für Strafurteile und Strafbefehle mit der Folge der umfassenden Verfügbarkeit der darin enthaltenen Informationen ist nicht angemessen. Bei der Bemessung der Aufbewahrungsfrist von Strafurteilen und Strafbefehlen sowie für die Bestimmung des Zeitpunkts der Einschränkung der Verfügbarkeit ist vielmehr nach Art und Maß der verhängten Sanktionen zu differenzieren.

   Bei der Festlegung des Beginns der Aufbewahrungsfrist sollte – abweichend von der bisherigen Praxis, nach der es auf die Weglegung der Akte ankommt – regelmäßig auf den Zeitpunkt des Eintritts der Rechtskraft der ergangenen gerichtlichen Entscheidung abgestellt werden.

   Ergeht keine rechtskraftfähige Entscheidung, so sollte die Aufbewahrungsfrist mit dem Erlaß der Abschlußverfügung beginnen.

4. Wird der Akteninhalt auf Bild- oder Datenträgern, die an die Stelle der Urschrift treten, aufbewahrt, so sind gleichwohl unterschiedliche Löschungsfristen für einzelne Aktenteile zu beachten. Aus datenschutzrechtlicher Sicht sind Datenträger zu wählen, die eine differenzierte Löschung gewährleisten. Ist bei Altbeständen eine teilweise Aussonderung technisch nicht möglich oder nur mit unverhältnismäßigem Aufwand zu bewerkstelligen, so hat eine Sperrung der an sich auszusondernden Teile zu erfolgen.

5. Sind in einer Akte Daten mehrerer beteiligter Personen gespeichert, so ist eine Sperre hinsichtlich solcher Aktenteile, die einzelne beteiligte Personen betreffen, vorzusehen, wenn diese Aktenteile eigentlich ausgesondert werden müßten, aus praktischen Gründen aber keine Vernichtung erfolgen kann.

6. Bei Freisprüchen und Einstellungen des Verfahrens wegen Wegfalls des Tatverdachts ist dafür Sorge zu tragen, daß ein Zugriff auf die automatisiert gespeicherten Daten nur noch zu Zwecken der Aktenverwaltung erfolgen kann.

7. Für die Daten von Nebenbeteiligten (z. B. Anzeigeerstatter, Geschädigte) ist eine vorzeitige Löschung vorzusehen. Hinsichtlich der Hauptbeteiligten sollte eine Teillöschung der Personen- und Verfahrensdaten stattfinden, sobald die vollständigen Daten zur Durchführung des Verfahrens nicht mehr erforderlich sind.

8. Soweit Daten verschiedener Gerichtszweige oder verschiedener speichernder Stellen in gemeinsamen Systemen verarbeitet werden, ist durch rechtliche, technische und organisatorische Maßnahmen sicherzustellen, daß die Zweckbindung der gespeicherten Daten beachtet wird.

*) Bei Stimmenthaltung von Hamburg.

Anlage 21

Entschließung
der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995
Anforderungen an den Persönlichkeitsschutz im Medienbereich

Die unabhängige und unzensierte Berichterstattung durch Presse, Rundfunk und Film (Art. 5 Abs. 1 Satz 2 GG) dient der freien individuellen und öffentlichen Meinungsbildung. Das Bundesverfassungsgericht hat die freie Meinungsbildung als Voraussetzung sowohl der Persönlichkeitsentfaltung als auch der demokratischen Ordnung bezeichnet. Insofern besteht ein enger Zusammenhang zwischen der Selbstbestimmung des einzelnen und der Medienfreiheit.

Die rasante Entwicklung der Medientechnik, die Zunahme interaktiver Teledienste und die verstärkte kommerzielle Nutzung von Pressedatenbanken eröffnen einerseits neue Informationsmöglichkeiten für den Bürger, verschärfen aber die Gefährdungen des Rechts auf informationelle Selbstbestimmung. Diesen Gefährdungen muß der Datenschutz auf rechtlicher und technisch-organisatorischer Ebene angemessen begegnen.

Electronic Publishing und Medienarchive

Neue Formen der Verbreitung von Informationen über Netze und auf elektronischen Datenträgern führen in bisher unbekanntem Maß zu großen Informationsbeständen, in denen potentiell jedermann gezielt auf personenbezogene Daten zugreifen kann. Zudem öffnen Medienarchive, die bislang ausschließlich für journalistische Zwecke genutzt wurden, riesige Datensammlungen für medienfremde Nutzer. In Persönlichkeitsrechte wird dann besonders tief eingegriffen, wenn auch lange zurückliegende Publikationen praktisch von jedermann recherchiert werden können. Damit droht das in verschiedenen Rechtsbereichen vorgesehene Recht auf Vergessen wirkungslos zu werden, das z. B. durch die Löschungsvorschriften für das Bundeszentralregister gewährleistet werden soll. Angesichts dieser Entwicklungen muß die Reichweite der datenschutzrechtlichen Sonderstellung der Medien (Medienprivileg) neu bestimmt werden. Es ist zumindest gesetzlich klarzustellen, daß die geschäftsmäßige Verwendung personenbezogener Daten außerhalb des eigenen Medienbereichs, insbesondere durch kommerzielle Pressedatenbanken, nicht unter das „Medienprivileg" fällt.

Interaktive Dienste und Mediennutzungsprofile

Auch beim Ausbau neuer digitaler Kommunikationsformen (interaktive Dienste, wie z. B. Video on Demand) müssen die Persönlichkeitsrechte der Nutzer gewahrt werden. Dabei ist stärker als bisher von vornherein Wert darauf zu legen, daß datenschutzfreundliche Techniken entwickelt werden und zum Einsatz kommen, bei denen personenbezogene Verbindungs- und Nutzungsdaten erst gar nicht entstehen. Von besonderer Bedeutung sind hier anonyme Zahlverfahren, z. B. Prepaid-Karten, auf denen Informationen über die Nutzung ausschließlich dezentral gespeichert werden. Entsprechend den Bestimmungen im Bildschirmtextstaatsvertrag und in den neueren Mediengesetzen ist sicherzustellen, daß sich die Erhebung und die Aufzeichnung von Verbindungs- und Abrechnungsdaten auf das erforderliche Maß beschränken. Dieser strikte Verarbeitungsrahmen darf auch nicht dadurch ausgeweitet werden, daß die Nutzung eines Dienstes von der Einwilligung in eine zweckfremde Verwendung der Daten abhängig gemacht wird. Die Länder sollten entsprechende einheitliche Regelungen für alle interaktiven Dienste treffen.

Da es sich bei den angesprochenen Diensten um Bestandteile einer entstehenden globalen Informationsinfrastruktur handelt, wird die Bundesregierung aufgefordert, sich auf internationaler Ebene für entsprechende Regelungen einzusetzen.

Rechte der Betroffenen gegenüber den Medien

Während die von der Berichterstattung Betroffenen – neben dem für alle Bereiche geltenden Gegendarstellungsrecht – gegenüber den öffentlich-rechtlichen und privaten Rundfunkveranstaltern inzwischen weitere elementare Datenschutzrechte besitzen, gibt es gegenüber der Presse keine vergleichbaren Regelungen.

So kann derjenige, der durch die Berichterstattung der Rundfunkveranstalter in seinem Persönlichkeitsrecht beeinträchtigt wird, in den meisten Fällen nach der Publikation Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Gegenüber der Presse hat er kein entsprechendes Auskunftsrecht. Die meisten Rundfunkveranstalter sind – anders als die Presse – zudem verpflichtet, etwaige Gegendarstellungen zu den gespeicherten Daten zu nehmen, auf die sie sich beziehen (Mitspeicherungspflicht). Ein sachlicher Grund für diese Unterscheidungen ist nicht erkennbar. Das Presserecht sollte insofern der Rechtslage nach dem Rundfunkrecht (z. B. § 41 Abs. 3 BDSG und Art. 17 Abs. 2 ZDF-Staatsvertrag) angeglichen werden. Gegenüber Pressedatenbanken, die nicht nur dem eigenen internen Gebrauch dienen, sollte der Betroffene darüber hinaus ein Auskunftsrecht bezüglich des zu seiner Person gespeicherten veröffentlichen Materials haben.

Öffentlichkeitsarbeit der Behörden

Personenbezogene Veröffentlichungen von Behörden können das Recht auf informationelle Selbstbestimmung erheblich beeinträchtigen. Das gilt für die Personen, auf die die Aktivitäten der Behörde unmittelbar gerichtet sind, wie auch für andere Verfahrensbeteiligte (wie z. B. Einwender, Opfer von Straftaten, Zeugen) und im besonderen Maße für unbeteiligte Personen aus dem sozialen Umfeld des Betroffenen. Deshalb ist bei der Weitergabe von Daten aus Strafermittlungsverfahren an die Medien besonders zurückhaltend zu verfahren.

Für den Umfang des Anspruchs der Medien auf Weitergabe personenbezogener Daten in Form von Presseerklärungen und Auskünften gibt es keine konkreten gesetzlichen Festlegungen. Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für geboten, daß der Gesetzgeber Kriterien für die Abwägung zwischen dem Persönlichkeitsrecht des Betroffenen und der Freiheit der Berichterstattung durch Rundfunk und Presse deutlicher als bisher festlegt. Dafür kommen die Vorschriften des Landespresserechts, in besonders sensiblen Bereichen aber auch spezialgesetzliche Regelungen, wie etwa die Strafprozeßordnung, in Betracht.

Gerichtsfernsehen

Die Datenschutzbeauftragten des Bundes und der Länder treten den in jüngster Zeit zunehmend erhobenen Forderungen nach einer Aufhebung des Verbots der Hörfunk- und Fernsehberichterstattung aus Gerichtsverhandlungen entgegen. Insbesondere bei Strafprozessen vor laufenden Mikrofonen und Kameras würde es unweigerlich zu einer gravierenden Beeinträchtigung des Persönlichkeitsrechts der Angeklagten, der Opfer, der Zeugen und ihrer Angehörigen kommen. Selbst mit Einwilligung aller Prozeßbeteiligten darf die Hörfunk- und Fernsehberichterstattung nicht zugelassen werden.

Die Gerichtsverhandlung darf nicht zu einem masssenmedial vermittelten „modernen Pranger" werden.

Anlage 22

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995 zum Sozialgesetzbuch VII

Verfassungsgemäßer Datenschutz für Unfallversicherte erforderlich

Durch die Träger der gesetzlichen Unfallversicherung werden oft Daten der Versicherten hinter deren Rücken oder zumindest ohne deren konkrete Kenntnis erhoben und weitergegeben. Der vorliegende Referentenentwurf des Bundesministeriums für Arbeit und Sozialordnung zum Unfallversicherungs-Einordnungsgesetz – SGB VII sieht dazu keine Änderungen vor.

Aus dem Recht auf informationelle Selbstbestimmung der Versicherten, insbesondere auf Transparenz der einzelnen Verfahrensschritte, ergeben sich mehrere grundlegende Forderungen, die bei einer Überarbeitung des Referentenentwurfes berücksichtigt werden müssen:

1. Auskunftspflicht behandelnder Ärzte gegenüber Unfallversicherungsträgern

   Für behandelnde Ärzte sollte eine gesetzliche Auskunftspflicht gegenüber Unfallversicherungsträgern nur festgelegt werden, soweit dies erforderlich ist für eine sachgerechte und schnelle Heilung (§ 557 Abs. 2 RVO – § 34 Referentenentwurf SGB VII). Die gesetzliche Auskunftspflicht ist daher auf Angaben über die Behandlung und den Zustand des Verletzten zu beschränken. Danach dürfen Vorerkrankungen, die aus Sicht des Arztes mit dem aktuellen Status in keinem Zusammenhang stehen oder keine Bedeutung im Zusammenhang mit dem Arbeitsunfall oder der Berufskrankheit haben, nicht übermittelt werden (Beispiel: Handverletzung und Salmonellenvergiftung).

2. Datenerhebung, -verarbeitung und -nutzung durch Durchgangsärzte und Berufskrankheitenärzte

   Soweit von den Unfallversicherungsträgern bestellte Durchgangsärzte personenbezogene Daten über den Unfallverletzten erheben und Unfallversicherungsträgern und anderen Stellen mitteilen, muß dies auf eine normenklare gesetzliche Grundlage gestellt werden; die bisherige Regelung in dem zwischen den Verbänden der Kassenärzte und der Unfallversicherungsträger geschlossenen „Ärzteabkommen" reicht für die damit verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen nicht aus. Entsprechendes gilt für die geplante Einführung eines Berufskrankheitenarztes.

3. Mitteilung personenbezogener Patientendaten durch Unfallversicherungsträger an ärztliche Gutachter

   Im Hinblick auf das Recht der Betroffenen, der Bestellung eines bestimmten Gutachters im Einzelfall aus wichtigem Grund – z. B. wegen möglicher Befangenheit – zu widersprechen, haben die Betroffenen ein besonderes berechtigtes Interesse an der Transparenz dieser Datenübermittlungen. Gesetzlich festzulegen ist daher, daß dem Betroffenen vor Übermittlung seiner Daten an einen Gutachter der Zweck des Gutachtens und die Person des Gutachters unter Hinweis auf sein Widerspruchsrecht nach § 76 Abs. 2 SGB X mitzuteilen sind.

4. Eingriffe der Unfallversicherungsträger und ihrer Verbände in das Recht auf informationelle Selbstbestimmung

   Aufgaben der Unfallversicherungsträger und ihrer Verbände und ihre Befugnisse zur Datenerhebung, -verarbeitung und -nutzung – einschließlich der Aufbewahrungsfristen – sind differenziert in der verfassungsrechtlich gebotenen Klarheit gesetzlich zu regeln. Der vorliegende Referentenentwurf erscheint in diesem Punkt weitgehend unzureichend. So werden undifferenziert Unfallversicherungsträger und ihre Verbände behandelt, die Fachaufgaben dieser Stellen nicht oder nicht hinreichend deutlich genannt und andererseits Selbstverständlichkeiten wie das Führen von Dateien über erforderliche Daten aufgeführt. Außerdem beschränkt sich die Regelung auf die Datenverarbeitung in Dateien und übergeht die gerade im Bereich der Berufsgenossenschaften mit Gutachten und ähnlichen Unterlagen stark ausgeprägte Datenverarbeitung in Akten. Die Zuweisung von Aufgaben und Befugnissen an Verbände der gesetzlichen Unfallversicherung muß zudem wie bei allen anderen Verbänden von Leistungsträgern durch die Einrichtung einer staatlichen Aufsicht ergänzt werden. Soweit Vorschriften der Unfallversicherungsträger und ihrer Verbände (z. B. Unfallverhütungsvorschriften) durch Regelungen über die Erhebung, Verarbeitung und Nutzung sensibler medizinischer Daten in das Recht auf informationelle Selbstbestimmung eingreifen, sind diese Eingriffe gesetzlich zu regeln.

5. Anzeige eines Berufsunfalls und einer Berufskrankheit

   Bei Datenschutzkontrollen der bisherigen Anzeigen von Berufsunfällen und -krankheiten hat sich gezeigt, daß der Umfang der an die verschiedenen Stellen übermittelten Daten zum Teil dem Grundsatz der Verhältnismäßigkeit, insbesondere der Erforderlichkeit, nicht Rechnung trägt. Der Inhalt dieser Anzeigen muß an diesen Grundsätzen gemessen neu festgelegt werden.

6. Zentraldateien mehrerer Unfallversicherungsträger oder ihrer Verbände

   Zweck und Inhalt zentral geführter Dateien sind in angemessenem Umfang gesetzlich präzise zu regeln. Dasselbe gilt für die Datenverarbeitung und -nutzung sowie die Festlegung der jeweils speichernden Stelle. Die rechtzeitige Beteiligung des jeweils zuständigen Bundes- oder Landesbeauftragten für den Datenschutz vor Einrichtung einer Zentraldatei ist vorzusehen.

7. Anforderung medizinischer Unterlagen bei anderen Sozialleistungsträgern

   Der in § 76 Abs. 2 SGB X vorgesehene Hinweis auf das Widerspruchsrecht gegen die Übermittlung medizinischer Daten geht stets dann ins Leere, wenn bei der speichernden bzw. übermittelnden Stelle kein Verwaltungsverfahren läuft. Es ist daher festzulegen, daß ein Unfallversicherungsträger vor der Anforderung von Sozialdaten im Sinne des § 76 SGB X bei anderen Sozialleistungsträgern den Versicherten auf dessen Widerspruchsrecht nach § 76 Abs. 2 SGB X gegenüber der übermittelnden Stelle hinzuweisen hat.

8. Akteneinsichtsrecht der Versicherten

   Hinsichtlich des gesetzlichen Akteneinsichtsrechts nach § 25 SGB X treten in der Praxis seitens der Unfallversicherungsträger Unsicherheiten auf, ob zum Schutz von Betriebs- und Geschäftsgeheimnissen oder Urheberrechten das Einsichtsrecht beschränkt werden muß. Hierzu ist eine gesetzliche Klarstellung geboten, daß diese Rechte dem Akteneinsichtsrecht nicht entgegenstehen.

Anlage 23

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995 zum Datenschutz bei Wahlen

Bei der Durchführung von Wahlen haben sich Probleme bei der Verarbeitung personenbezogener Daten ergeben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu die folgende Entschließung*) gefaßt:

1. Durchführung von Wahlstatistiken

Diejenigen Wahlberechtigten, in deren Wahlbezirk eine repräsentative Wahlstatistik durchgeführt werden soll, sind bereits mit der Wahlbenachrichtigung hierüber zu informieren. In allgemeiner Form ist auch im Wahllokal ein gut sichtbarer Hinweis auf die Einbeziehung in die Wahlstatistik anzubringen.

Die Statistik sollte nur in solchen Wahlbezirken durchgeführt werden, in denen jede Geschlechts- und Altersgruppe wenigstens so viele Wahlberechtigte aufweist, daß das Wahlgeheimnis mit Sicherheit gewahrt bleibt. Das Kriterium ist vom Landeswahlleiter vor der Festlegung der Auswahlbezirke zu prüfen. Gegebenenfalls sind ungeeignete Wahlbezirke auszutauschen.

Die Auszählung der Wahlberechtigten und der Wahlbeteiligung auf der Grundlage der Wählerverzeichnisse sollte durch den Wahlvorstand erfolgen, während die statistische Auszählung der Stimmzettel durch die jeweils für die Durchführung der Statistik zuständige Stelle vorzunehmen ist.

Untersuchungen, bei denen Angaben über die Wahlbeteiligung oder die Stimmabgabe aus verschiedenen Wahlen einzelfall- und personenbezogen zusammengeführt werden, gefährden das Wahlgeheimnis und sind daher unzulässig.

2. Auslegung von Wählerverzeichnissen

Durch die Einsicht in das Wählerverzeichnis besteht nach der jetzigen Rechtslage die Gefahr, daß Daten sowohl von Bürgern, über die in Melderegistern eine Auskunftssperre eingetragen ist, als auch von Bürgern, die in einer speziellen sozialen Situation leben (z. B. Justizvollzugsanstalten, Frauenhäuser, psychiatrische Kliniken, Obdachlose), offenbart werden. Um einerseits die Kontrollmöglichkeit durch die Öffentlichkeit im Vorfeld einer Wahl weiterhin zu gewährleisten, andererseits die datenschutzrechtlichen Belange der genannten Betroffenen zu wahren und dem Mißbrauch einer Adreßrecherche vorzubeugen, fordern die Datenschutzbeauftragten des Bundes und der Länder, daß bei allen Wahlen

- entweder in den öffentlich ausliegenden Wählerverzeichnissen nur Name, Vorname und Geburtsdatum der Wahlberechtigten aufgeführt werden
- oder aber bei Wiedergabe der Adressen im Wählerverzeichnis nur Auskünfte zu bestimmten Personen an den Auskunftssuchenden erteilt werden, wenn er vorher die Adresse dieser Person aufgegeben hat.

Im übrigen sind Daten von Bürgern, für die in Melderegistern eine Auskunftssperre eingetragen ist, im Wählerverzeichnis nicht zu veröffentlichen.

3. Gewinnung von Wahlhelfern

Bei der Gewinnung von Wahlhelfern sind folgende Grundsätze zu beachten: Es dürfen nur die zur Bestellung erforderlichen Daten wie Name, Vorname und Wohnanschrift erhoben werden. Die Betroffenen sind über den Zweck der Datenerhebung und die weitere Datenverarbeitung umfassend zu unterrichten.

Über die Abwicklung der jeweiligen Wahl hinaus dürfen die Daten der Wahlhelfer, soweit sie nicht ausdrücklich widersprochen haben, in einer Wahlhelferdatei nur gespeichert werden, wenn sie dieser Speicherung nicht widersprochen haben. Die Wahlhelfer sind auf ihr Widerspruchsrecht hinzuweisen.

Beschäftigtendaten dürfen nur auf freiwilliger Basis übermittelt werden, sofern nicht eine besondere Rechtsvorschrift die Übermittlung zuläßt. Im Falle der Freiwilligkeit muß es den Beschäftigten möglich sein, selbst die Meldung unmittelbar gegenüber der Wahlbehörde abzugeben. Nach Gründen, die einer Übernahme des Ehrenamtes entgegenstehen, darf erst im förmlichen Verfahren durch die Wahlbehörde gefragt werden.

4. Erteilung von Wahlscheinen

Die in den Wahlordnungen des Bundes und der Länder enthaltene Regelung, nach der die Antragstellung für die Erteilung eines Wahlscheines auf einem Vordruck zu begründen ist und der Grund gegenüber der Gemeinde glaubhaft gemacht werden muß, ist aus datenschutzrechtlicher Sicht unverhältnismäßig. Da sich aus der geforderten Differenzierung der Begründung keine unterschiedlichen Rechtsfolgen ableiten, ist diese entbehrlich. Es genügt in der Antragstellung eine Erklärung des Wahlberechtigten, daß er am Tag der Wahl aus wichtigem Grund das für ihn zuständige Wahllokal nicht aufsuchen kann.

*) Bei Gegenstimme von Baden-Württemberg zu Nr. 4.

Anlage 24

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995 zum Datenschutz bei elektronischen Mitteilungssystemen

Es ist damit zu rechnen, daß in Zukunft mit Hilfe elektronischer Mitteilungssysteme rechtsverbindliche bedeutsame Informationen und insbesondere personenbezogene Daten über Netze ausgetauscht werden.

Die zunehmende Nutzung von elektronischen Mitteilungssystemen (Electronic-Mail, Dokumentenaustausch über Datenfernübertragung, Message Handling Systems MHS/X.400) hat zur Folge, daß Bedrohungen wie Verlust von Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit verschärft werden, weil Unbefugte Zugriffe auf Daten und Programme erhalten können und die Übertragungswege vom Kommunikationspartner nicht sicher zu kontrollieren sind. Deshalb ist beim Einsatz solcher Systeme das Risikobewußtsein bei den Verantwortlichen sowie den Anwendern zu schärfen. In diesem Zusammenhang gewinnt der Schutz der elektronisch gespeicherten, verarbeiteten und übertragenen Information durch eine Vielzahl umfassender aufeinander abgestimmter Sicherheitsmaßnahmen an Bedeutung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, daß den folgenden Sicherheitsaspekten beim Einsatz von elektronischen Mitteilungssystemen Rechnung getragen wird:

1. Authentizität von Benutzern, Nachrichten und Systemmeldungen

   Für den Empfänger einer Nachricht muß jederzeit die Möglichkeit bestehen, anhand bestimmter Kriterien die Authentizität des Absenders, der Nachricht sowie der an ihn gerichteten Systemmeldungen (z. B. Empfangs- und Weiterleitungsbestätigungen, Sendeanforderungen, Teilnehmerkennungen, Teilnehmereinstufungen) zu überprüfen.

2. Vertraulichkeit von übertragenen Daten

   Für alle Arten von Daten in elektronischen Mitteilungssystemen – Nachrichten sowie Verkehrs- und Verbindungsdaten – muß die Vertraulichkeit gewahrt bleiben. Sie ist durch geeignete Maßnahmen, z. B. kryptografische Verfahren, sicherzustellen.

3. Integrität von Nachrichten und Meldungen

   Es ist zu gewährleisten, daß bei Speicherung und Weiterleitung von Daten keine unbefugte, unerkannte Veränderung erfolgen kann.

4. Fälschungssichere Kommunikationsnachweise

   Die für die Anerkennung einer elektronischen Kommunikation erforderlichen fälschungssicheren Sende-, Empfangs- und Übertragungsnachweise müssen dem Anwender auf Wunsch zur Verfügung stehen.

5. Ausschluß von Kommunikationsprofilen

   Die Erstellung von Kommunikationsprofilen muß verhindert werden. Gespeicherte Protokollierungsdaten dürfen nur zu Zwecken des Datenschutzes und der Datensicherung (§§ 14 Abs. 4, 31 BDSG bzw. landesgesetzliche Regelungen) verwendet werden.

Empfehlungen zum Einsatz von elektronischen Mitteilungssystemen:

Zum sicheren Einsatz von elektronischen Mitteilungssystemen sind als Grundschutzmaßnahmen folgende Empfehlungen zu beachten:

Sicherheitsfunktionen

1. Grundsätzlich sind nur solche Produkte einzusetzen, die die X.400-Empfehlung aus dem Jahre 1988 erfüllen. Vorhandene Systeme – insbesondere solche, die noch auf Empfehlungen von 1984 basieren –, sollen künftig durch geeignete Zusatzprodukte hinsichtlich ihrer Sicherheit verbessert oder durch neuere Softwareversionen ersetzt werden.

2. Bei Übertragung von personenbezogenen Daten ist eine Verschlüsselung vorzusehen. Die Verschlüsselung der Daten muß mit einem hinreichend sicheren Verschlüsselungsverfahren erfolgen. Neben der Auswahl eines effektiven Verschlüsselungsalgorithmus (z. B. DES, IDEA) muß dabei insbesondere eine ordnungsgemäße Schlüsselerzeugung, -verwaltung und -ver-

teilung gewährleistet sein. Verschlüsselungskomponenten sind durch technische, bauliche und organisatorische Maßnahmen vor dem Zugriff Unbefugter zu schützen.

3. Zur Absicherung der Integrität der Daten sollte auf Verfahren der „elektronischen Unterschrift" zurückgegriffen werden.

4. Nach Möglichkeit ist die Funktion des Systemverwalters von der des Netzwerkverwalters – insbesondere der Verwaltung des elektronischen Mitteilungssystems – aus Sicherheitsgründen zu trennen.

5. Es ist grundsätzlich separat administrierbare Hard- oder Software – z. B. in Form eines Kommunikationsservers – für das elektronische Mitteilungssystem vorzusehen.

6. Bei Verwendungen von öffentlichen Übertragungswegen sind die vorhandenen Sicherheitsmechanismen dieser Netze, z. B. geschlossene Benutzergruppen, Rufnummernidentifikation, Teilnehmerzeichengabe und automatische Rückruffunktion zur Abwehr des Zugriffs durch Externe, zu nutzen.

7. Zur Beweissicherung einer stattgefundenen Kommunikation sollte die eingesetzte Software folgende Funktionen beinhalten:
   - Zustellung/Empfangsnachweise
   - Sende-/Empfangsübergabenachweise.

Anlage 25

Entschließung
der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995
Maßhalten beim vorbeugenden personellen Sabotageschutz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, bei Sicherheitsüberprüfungen zum personellen Sabotageschutz Augenmaß zu bewahren. Bei diesen Sicherheitsüberprüfungen werden sensible Daten, z. B. über politische Anschauungen oder Alkoholkonsum, vorbeugend erhoben, also ohne daß der Betroffene dazu Anlaß geboten hätte. Polizei und Verfassungsschutz sind routinemäßig beteiligt. Schon wenn der Betroffene im Verlauf der Überprüfung auch nur in den Verdacht der Unzuverlässigkeit gerät, kann dies bereits erheblichen Einfluß zumindest auf das berufliche Fortkommen nehmen.

Gegenwärtig sind solche Überprüfungen spezialgesetzlich für den Atombereich und für Flughäfen vorgesehen. Das Bundesministerium des Innern will jetzt klären, inwieweit Beschäftigte in anderen Einrichtungen überprüft werden sollen. Unstreitig können solche Überprüfungen unbescholtener Bürger nur zum Schutz von „lebens- und verteidigungswichtigen Einrichtungen" angemessen sein und nur Personen betreffen, die dort an „sicherheitsempfindlichen Stellen" tätig sind. Als „lebenswichtig" sehen die Innenminister und -senatoren aber bereits Stellen an, „die für das Funktionieren des Gemeinwesens unverzichtbar sind". Damit könnten Beschäftigte in weiten Bereichen des öffentlichen Dienstes und der Wirtschaft mit Sicherheitsüberprüfungen überzogen werden.

Die Datenschutzbeauftragten meinen, daß das Persönlichkeitsrecht hier größere Zurückhaltung gebietet. Die Sicherheitsüberprüfungen müssen auf Bereiche beschränkt bleiben, in denen einer erheblichen Bedrohung für das Leben zahlreicher Menschen vorgebeugt werden muß.

Soweit in solchen Bereichen Sicherheitsüberprüfungen durchgeführt werden sollen, bedarf es einer ebenso klaren gesetzlichen Grundlage wie bisher im Atomgesetz und im Luftverkehrsgesetz. Die zu schützenden Arten lebens- und verteidigungswichtiger Einrichtungen müssen durch Rechtsvorschrift abschließend festgelegt sein. Dabei sind für die jeweiligen Bereiche angemessene Regelungen zu treffen, die mit Rücksicht auf die Interessen Betroffener folgende allgemeine Grundsätze beachten:

- möglichst klare Vorgaben zur „Sicherheitsempfindlichkeit" in der Vorschrift und exakte Festlegung dieser Stellen durch die zuständige Behörde nach Anhörung der Personalvertretung der einzelnen Einrichtung,
- Zustimmung des Betroffenen als Verfahrensvoraussetzung,
- abschließender Katalog der regelmäßig durchzuführenden Maßnahmen, dabei Beschränkung auf vorhandene Erkenntnisse, keine Ausforschungsermittlungen,
- strenge Zweckbindung und angemessene organisatorische Vorkehrungen zu deren Gewährleistung, insbesondere Trennung von Personalakte,
- eigene Verfahrensrechte des Betroffenen, insbesondere rechtliches Gehör vor ablehnender Entscheidung und aktenkundige Gegendarstellung,
- angemessener Auskunftsanspruch, einschließlich Akteneinsicht,
- effektive Datenschutzkontrolle, auch zur Datenverarbeitung in Akten bei nichtöffentlichen Stellen.

Im Regelfall muß zusätzlich gelten:

- Überprüfung durch die zuständige Aufsichtsbehörde selbst, nicht durch Verfassungsschutzbehörden,
- keine Einbeziehung weiterer Personen (wie Ehegatten usw.).

Ausnahmetatbestände wären – auch zum Verfahren – präzise zu fassen. Die Praxis der Sicherheitsüberprüfungen zum personellen Sabotageschutz steht in Bund und Ländern vor einer wichtigen Weichenstellung. Sie muß klar und angemessen sein.

Anlage 26

Entschließung
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 19. September 1995
zum Entwurf einer
Telekommunikations- und Informationsdienstunternehmen-
Datenschutzverordnung (TIDSDV)
des Bundesministeriums für Post- und Telekommunikation
(Stand: 6. Juni 1995)

Das Bundesministerium für Post und Telekommunikation hat den Entwurf einer Telekommunikations- und Informationsdienstunternehmen-Datenschutzverordnung (TIDSV) vorgelegt, der auf der Grundlage des bereits seit Anfang dieses Jahres geltenden Gesetzes über die Regulierung der Telekommunikation und des Postwesens (PTRegG) den Schutz personenbezogener Daten der am Fernmeldeverkehr beteiligten Bürger regeln soll. Die Verordnung muß entsprechend der gesetzlichen Vorgabe dem Grundsatz der Verhältnismäßigkeit genügen, insbesondere hat sie die Erhebung, Verarbeitung und Nutzung der Daten auf das Erforderliche zu beschränken und ihre Zweckbindung zu gewährleisten. Die Datenschutzbeauftragten des Bundes und der Länder stellen fest, daß der vorliegende Entwurf diesen aus der Verfassung abgeleiteten gesetzlichen Vorgaben teilweise nicht genügt.

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung vom 8. März 1991 auf die Bedeutung des Grundrechts auf unbeobachtete Kommunikation hingewiesen und gefordert, daß das Telekommunikationsdatenschutzrecht dieses Grundrecht zu sichern hat. Im Zeitalter der elektronischen Information und Kommunikation ist es geboten, die Betreiber zur Bereitstellung anonymer Nutzungsmöglichkeiten zu verpflichten und den Bürger in die Lage zu versetzen, selbst zu entscheiden, ob er seine personenbezogenen Daten preisgeben und sich den damit verbundenen Risiken aussetzen will.

Im einzelnen halten die Datenschutzbeauftragten den vorliegenden Entwurf in folgenden Punkten für verbesserungsbedürftig, auch um eine Absenkung des Datenschutzniveaus gegenüber der gegenwärtigen Rechtslage zu verhindern:

Die Verarbeitung von Kundendaten muß auch in Zukunft ausdrücklich auf Telekommunikationszwecke und Zwecke der Informationsdienstleistung beschränkt werden; jede Aufweichung des Zweckbindungsgrundsatzes ist abzulehnen.

Auch im Bereich des Sprachtelefondienstes soll nach dem Entwurf die Speicherung der vollständigen Rufnummer des angerufenen Teilnehmers bis zu 80 Tagen nach Rechnungsversand zur Regel werden. Bislang war dies nur vorgesehen, wenn der Anrufer einen Einzelverbindungsnachweis beantragt hat; dabei sollte es auch in Zukunft bleiben.

Eine Auswertung der Verbindungsdaten nach Zielrufnummern auch außerhalb des Sprachtelefondienstes ohne Einwilligung des Kunden ist nach § 10 Abs. 2 Nr. 2 PTRegG unzulässig. Hiernach „dürfen Daten des Anrufenden nur mit dessen Einwilligung verwendet und müssen Daten des Angerufenen unverzüglich anonymisiert werden."

Die Übermittlung von Verbindungsdaten an Dienstanbieter darf auch für Zwecke des Entgelteinzuges weiterhin nur mit Einwilligung des Kunden zugelassen werden, wenn der Datenempfänger sich vertraglich zur Einhaltung des Fernmeldegeheimnisses verpflichtet hat.

Ein Einzelverbindungsnachweis sollte auch in Zukunft nur erteilt werden, wenn der Antragsteller das Einverständnis der zum Haushalt gehörenden Mitbenutzer des Anschlusses nachweisen kann.

Die Anonymität von Anrufern bei Beratungseinrichtungen muß auch dann gewährleistet sein, wenn sie über ein Mobilfunknetz anrufen. Es ist nicht nachzuvollziehen, daß gerade an den dynamischsten und modernsten Teilbereich der Telekommunikation geringere Datenschutzanforderungen gestellt werden sollen als an das traditionelle Festnetz. Ohnehin ist eine Entwicklung absehbar, die Mobilfunk- und Festnetze zusammenwachsen läßt.

Der Anrufer muß im Sprachtelefondienst die kostenfreie Möglichkeit haben, die Übermittlung seiner Rufnummer an den angerufenen Anschluß dauernd oder fallweise auszuschließen.

Beim angerufenen Anschluß im Sprachtelefondienst muß auch in Zukunft die Abschaltung der Rufnummernanzeige allgemein und im Einzelfall möglich sein, damit Personen, die sich in räumlicher Nähe zum Angerufenen aufhalten, nicht zwangsläufig Kenntnis vom jeweiligen Anrufer erhalten.

Die regelmäßige Herausfilterung der Daten solcher Verbindungen, für die tatsächliche Anhaltspunkte den Verdacht eines strafbaren Mißbrauchs von Fernmeldeanlagen oder der mißbräuchlichen Inanspruchnahme von Telekommunikations- oder Infor-

mationsdienstleistungen begründen, kommt einer präventiven Rasterfahndung der dem Fernmeldegeheimnis unterliegenden Verbindungsdaten gleich, in die bereits im Vorfeld eines konkreten Verdachts sämtliche Teilnehmer einbezogen werden. Die entsprechende Regelung sollte dieses Verfahren lediglich auf den Einzelfall beschränken.

Hinsichtlich der Erhebung, Verarbeitung und Nutzung von Nachrichteninhalten sind die strengen Vorgaben von § 10 Abs. 2 Sätze 2 bis 5 PTRegG einzuhalten. Insoweit fehlt in dem vorliegenden Entwurf eine Einschränkung auf den Einzelfall und die Verankerung der nach § 10 PTRegG vorgesehenen Informations- und Unterrichtungspflichten.

Die geplante Umwandlung der bisherigen Telefonauskunft ist datenschutzrechtlich nur vertretbar, wenn der Kunde über die Verwendungsmöglichkeit in der Telefonauskunft und sein Widerspruchsrecht hinreichend informiert wird. So muß er insbesondere wissen, daß nicht nur seine Rufnummern, sondern sämtliche Angaben, die er für die Teilnehmerverzeichnisse freigegeben hat, auch beauskunftet und verwendet werden können, sofern er dem nicht widersprochen hat.

Die vorgesehenen Regelungen über öffentliche Kundenverzeichnisse und die Telefonauskunft tragen den besonderen Risiken der Verbreitung von Kundendaten in elektronischer Form, etwa auf CD-ROM oder durch Abruf aus Online-Diensten (Adreß-Selektion, bundesweite Recherche, umgekehrte Rufnummernsuche) nicht Rechnung. Der Kunde muß ein differenziertes Widerspruchsrecht erhalten, das ihm ermöglicht, seine Daten zwar in das herkömmliche Telefonbuch aufnehmen oder von der Telefonauskunft mitteilen zu lassen, eine Aufnahme in elektronische Verzeichnisse mit qualitativ weitergehenden Verarbeitungsmöglichkeiten jedoch zu unterbinden.

Der Verordnungsentwurf läßt abweichend von der gegenwärtigen Praxis bei der Deutschen Telekom AG die Erstellung von Einzelverbindungsnachweisen mit vollständigen Zielrufnummern ohne Einflußmöglichkeit der angerufenen Kunden zu. Die Anonymität des Angerufenen wird aber auch durch die Verkürzung der Zielrufnummer um die letzten drei Ziffern nicht hinreichend gewährleistet. Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung vom 9./10. März 1994 darauf hingewiesen, daß dem Schutz des informationellen Selbstbestimmungsrechts und des Fernmeldegeheimnisses des Angerufenen am besten dadurch entsprochen würde, wenn jeder inländische Anschlußinhaber selbst entscheiden könnte, ob und gegebenenfalls wie seine Rufnummer auf Einzelverbindungsnachweisen erscheinen soll. Obwohl ein entsprechendes Verfahren in den Niederlanden bereits erfolgreich praktiziert wird, hat der Bundesminister für Post und Telekommunikation diesen Vorschlag bisher nicht aufgegriffen.

Die Vorschriften für Bildschirmtextdienste sollten, auch im Sinne der Rechtssicherheit, möglichst weitgehend mit denen des Bildschirmtext-Staatvertrages harmonisiert werden. Insbesondere sollte die Speicherung von Abrechnungsdaten so beschränkt werden, daß Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von den einzelnen Kunden in Anspruch genommener Angebote nicht erkennbar sind, es sei denn, der Kunde beantragt mit Einverständnis der Mitbenutzer einen Einzelverbindungsnachweis. Ferner ist vorzusehen, daß Abrechnungsdaten nicht erst sechs Monate nach Bekanntgabe der Entgeltrechnung gelöscht werden, sondern unverzüglich wenn sie für Abrechnungszwecke nicht mehr erforderlich sind.