LANDTAG RHEINLAND-PFALZ
13. Wahlperiode

Drucksache 13/2427
15. 12. 1997

Unterrichtung

durch den Landesbeauftragten für den Datenschutz

Sechzehnter Tätigkeitsbericht nach § 29 Abs. 2 Landesdatenschutzgesetz – LDSG – für die Zeit vom 1. Oktober 1995 bis 30. September 1997

Inhaltsverzeichnis

		Seite
1.	Vorbemerkung	11
2.	Weiterentwicklung des Datenschutzrechts	12
2.1	Grundsätzliche Tendenzen	12
2.2	Regelung des parlamentsspezifischen Datenschutzes in einer Datenschutzordnung	12
3.	Datenschutz in Europa	13
3.1	EG-Datenschutzrichtlinie	13
3.2	Die Umsetzung der Richtlinie in nationales Recht	14
3.3	Weiterentwicklung des Datenschutzes in der Europäischen Union	15
3.4	Datenschutz bei den Organen und Einrichtungen der Gemeinschaft	15
4.	Meldewesen	16
4.1	Datenschutzrechtliche Defizite im Zusammenhang mit der Einrichtung und Nutzung automatisierter Übermittlungsverfahren in EWOIS	16
4.1.1	Angemessenheit der Einrichtung und Nutzung von Online-Anschlüssen	17
4.1.2	Anpassung der Auskunftsformate an die Erforderlichkeit zur Aufgabenerfüllung	17
4.1.3	Stichprobenprüfung/Protokollierung	18
4.1.4	Anhörung des LfD	18
4.1.5	Unterrichtung der Aufsichtsbehörde und der Meldebehörden	18
4.2	Meldefähige Anschrift für wohnungslose Personen	18
4.3	Nutzung von Meldedaten für den Rundfunkgebühreneinzug	19
4.4	Erteilung von Melderegisterauskünften durch die Wegzugsbehörde	19
4.5	Meldedaten von Transsexuellen	20
4.6	Einwohnerverzeichnisse auf CD-ROM	20
4.7	Alters- und Ehejubiläen	21
4.7.1	Was ist ein Jubiläum?	21
4.7.2	Dürfen Jubiläumsdaten für Werbezwecke übermittelt werden?	21
5.	Polizei	22
5.1	Europol	22
5.2	Gesetz über das Bundeskriminalamt	23
5.3	Novellierung des Polizei- und Ordnungsbehördengesetzes	23
5.4	Nutzung von Protokolldaten zur Strafverfolgung	24
5.5	Personenbezogene Auswertung der polizeilichen Kriminalstatistik	24

Dem Präsidenten des Landtags mit Schreiben vom 11. Dezember 1997 zugeleitet. Der Bericht wurde in der Sitzung der Kommission beim Landesbeauftragten für den Datenschutz am 17. November 1997 nach § 26 Abs. 3 Satz 4 LDSG vorberaten.

Druck: Landtag Rheinland-Pfalz, 13. Februar 1998

		Seite
5.6	Richtlinien für die Führung von Kriminalakten überarbeitungsbedürftig	25
5.7	Kein Täterschutz durch die Aussonderungsregeln für Altkriminalakten	25
5.8	Automatisches Fingerabdruckidentifizierungssystem des BKA (AFIS)	26
5.9	Regelungen über die Zusammenarbeit der Polizei- und Zollbehörden in den Grenzgebieten	26
5.10	Kann die Polizei Daten aus einer Datei des Bundesgrenzschutzes nutzen?	27
5.11	Abfragen aus Ausländerzentralregister	27
5.12	Prüfungen bei Polizeidienststellen des Landes	27
5.13	Aufbewahrung von Zweitschriften bis zur Hauptverhandlung	28
5.14	Mitteilungen der Straßenverkehrsbehörden an die Polizei	29
5.15	Geisterautos und Schrottfrisierungen	29
5.16	Die Zusatzprotokollierung von POLIS-Abrufen ist stärker zu beachten	29
5.17	Dokumentation von Ermittlungen für eine andere Polizeidienststelle	30
5.18	Generalerrichtungsanordnungen	30
5.19	Ringalarmfahndungsdaten Unbeteiligter jahrelang im Computer	31
5.20	Nutzung der Telefon-Informationssoftware „D-Info" auf CD-ROM durch die Polizei	31
5.21	Wer rast, der spielt mit dem Leben unserer Kinder	32
5.22	Privates Sicherheitsgewerbe fahndet im Internet (System EuSIS)	33
5.23	Großer Lauscheingriff	33
6.	Verfassungsschutz	35
6.1	Dauerbrenner Neufassung des Verfassungsschutzgesetzes	35
6.2	Sicherheitsüberprüfungsgesetz gefordert	35
6.3	Verfassungsschutz beobachtet Scientology-Organisation	35
6.4	Prüfungen beim Verfassungsschutz	36
7.	Justiz	
	Vorbemerkung, Kompetenzkonflikte	37
7.1	Strafrecht	37
7.1.1	Ergänzung der Strafprozeßordnung um datenschutzrechtliche Grundnormen	37
7.1.2	DNS-Analyse im Strafverfahren, DNS-Dateien	38
7.1.3	Videoaufzeichnungen im Strafverfahren: Schutz der Opferzeugen oder Dokumentationsverbesserung?	39
7.1.4	Telekommunikationsüberwachung	39
7.1.4.1	Defizite bei der Durchführung der Telefonüberwachung gem. § 100 a StPO	39
7.1.4.2	Entwicklungen im Bereich der Telekommunikationsüberwachung	40
7.1.4.3	Überwachung von Telefondaten in digitalen Mobilfunknetzen	40
7.1.4.4	Datenschutzgerechte Ausgestaltung der Fangschaltung	41
7.1.5	Opferdatenschutz in bezug auf psychologische Gutachten in Akten der Staatsanwaltschaften und Gerichte	41
7.1.6	Eintragung der Schuldunfähigkeit in das Bundeszentralregister	41
7.1.7	Zustellung von Strafbefehlen und sonstigen gerichtlichen Schriftstücken an Wohnungslose	42
7.2	Zivilrecht	42
7.2.1	Übermittlung eines zivilgerichtlichen Urteils an eine Ordnungsbehörde	42
7.2.2	Datenschutzfragen im Zusammenhang mit dem Schuldnerverzeichnis	43
7.2.3	Regelmitteilungen der Grundbuchämter an die Nachlaßgerichte	43
7.2.4	Vollzugsdefizite bei Mitteilungen in Zivilsachen	44
7.3	Datenschutzfragen beim Vollzug des Betreuungsrechts	44
7.4	Organisatorisch-technischer Datenschutz in der Justiz	45
7.4.1	EDV-Einsatz im Bereich der Justiz	45
7.4.2	Zustellungsreformgesetz	46
7.4.3	Zugang von Mitarbeitern privater Unternehmen zu Archivräumen eines Gerichtsgebäudes	46
7.5	Neufassung der Presserichtlinien	47
7.6	Strafvollzug/Untersuchungshaft	48
7.6.1	Strafvollzugsgesetz	48
7.6.2	Untersuchungshaftvollzugsgesetz	48
7.6.3	Rückfalluntersuchung nach Vollzug der Jugendstrafe	48
7.6.4	Mithören bei Telefongesprächen von Gefangenen	49
7.6.5	Haftraumbeschilderung	50
7.6.6	Sonstige Eingaben	50

		Seite
8.	Schulen, Hochschulen, Wissenschaft	50
8.1	Schulen	50
8.1.1	Technisch-organisatorischer Datenschutz in Schulen	50
8.1.2	Besetzung der Schulleiterstelle einer Grundschule; Fragerecht von Mitgliedern eines Verbandsgemeinderats	51
8.1.3	Datenerhebungen und -übermittlungen durch eine Schule für das Sozialamt	51
8.1.4	Lehrerdaten im Schulbericht	51
8.1.5	Anfertigung von Klassen- und Schülerfotografien	52
8.1.6	Personaldatenübermittlung durch den Schulleiter an die Elternvertretungen	52
8.1.7	Darf der Schulträger kontrollieren, ob Lehrer dienstlich telefoniert haben?	53
8.1.8	Klassenbuchverwaltung durch Schüler	54
8.2	Hochschulen	54
8.2.1	Datenerhebung bei ausländischen Studenten für das Akademische Auslandsamt	54
8.2.2	Datenübermittlungen an andere Universitäten über abgelehnte Dissertationen	54
8.2.3	Adressenweitergaben zur Einladung ehemaliger Studenten	54
8.2.4	Veröffentlichung von studentischen Meinungsumfragen zum Lehrverhalten	55
8.2.5	Multifunktionskarte der Universität Trier (TUNIKA)	56
8.3	Wissenschaftliche Forschung	56
8.3.1	Vorwurf der Wissenschaftsbehinderung durch Datenschutz	56
8.3.2	Krebsregistergesetz	57
8.3.3	Eine Untersuchung über Zwangssterilisation in der NS-Zeit	57
8.3.4	Datenschutzanforderungen an eine wissenschaftliche Untersuchung in der Schule	58
8.3.5	Ärztliche Untersuchungen zu wissenschaftlichen Zwecken an einer Schule	58
8.3.6	Nutzung einer Liste ehemaliger KZ-Häftlinge des KZ Osthofen	59
8.4	Einsichtsrecht in das Denkmalbuch gem. § 10 Abs. 3 DSchPflG	60
8.5	Bibliotheksdaten	60
8.5.1	Übermittlung von Ausleihdaten durch eine Universitätsbibliothek an andere Nutzer	60
8.5.2	Löschung der Ausleihdaten	61
9.	Umweltschutz	61
9.1	Novelle des Landesabfallwirtschafts- und Altlastengesetzes	61
9.2	Datenübermittlung aus dem Klärschlammkataster	62
9.3	Einsicht in das Altlastenkataster	62
9.4	Zustellung von Gebührenbescheiden per Infopost	63
9.5	Datenschutzrechtliche Belange bei der Aufstellung eines Flächennutzungsplans	63
10.	Gesundheitswesen	64
10.1	Öffentlicher Gesundheitsdienst	64
10.1.1	Arztpost auf dem Schreibtisch des Landrats	65
10.1.2	Auskunft und Akteneinsicht nach den Vorschriften des Landesgesetzes über psychisch kranke Personen	65
10.1.3	Vorlage der Einwilligungserklärung bei der Übersendung von Arztbriefen	66
10.2	Methadonsubstitution; Anzeigen nach § 2 a Abs. 9 BtMVV	66
10.3	Schutz des Persönlichkeitsrechts der Frauen im Rahmen von Leistungen nach dem Schwangeren- und Familienhilfeänderungsgesetz	67
10.4	Datenschutz im Krankenhaus	67
10.4.1	Outsourcing und Fernwartung	67
10.4.2	Fehlbelegungsprüfungen in Krankenhäusern	69
10.4.3	Datenübermittlung zum Zwecke der Regulierung von Haftpflichtversicherungsschäden	69
10.5	Einbehaltung des Personalausweises von Besuchern in Maßregelvollzugseinrichtungen	69
10.6	Patientenchipkarten	70
10.6.1	Bestimmungen über die Einführung und Verwendung von Patientenchipkarten in der Berufsordnung für die Ärzte	70
10.6.2	Modellversuch Neuwied/Rhein	70
10.7	Arzt- und Zahnarztadressen in Informationsbroschüren von Gemeinden	71
11.	Sozialdatenschutz	71
11.1	Informationsrechte des Parlaments versus Sozialgeheimnis	72
11.2	Krankenkassen, Kassenärztliche Vereinigungen	73

		Seite
11.2.1	Übermittlung von ärztlichen Leistungsdaten	73
11.2.2	Kündigung aufgrund einer unzulässigen Datenübermittlung	73
11.2.3	Beschlagnahme und Auswertung maschinenlesbarer Datenträger bei Kassenärztlichen Vereinigungen	74
11.3	Gegenseitige Beauftragung der Träger der gesetzlichen Rentenversicherung mit der Versichertenbetreuung	75
11.4	Pflegeversicherung	76
11.4.1	Einwilligungserklärung nach § 18 Abs. 3 SGB XI	76
11.4.2	Gemeinsame Empfehlung nach § 75 Abs. 5 SGB XI	76
11.5	Sozialhilfe	76
11.5.1	Zusammenarbeit zwischen Sozialleistungsträgern und der Polizei	76
11.5.2	Abrechnung von Behandlungskosten	78
11.5.3	Übermittlung von Sozialdaten zur Durchführung einer Vollstreckung	78
11.5.4	Zulässiger Umfang der Datenerhebung bei Anfragen an den Arbeitgeber nach § 116 BSHG	78
11.5.5	Arbeit statt Sozialhilfe	79
11.5.6	Unterrichtung des Personalrats bei der Schaffung von Arbeitsgelegenheiten nach § 19 Abs. 1 BSHG im kommunalen Bereich	80
11.5.7	Abruf von Daten der Zulassungsstelle durch das Sozialamt	80
11.5.8	Verwendung von Vordrucken im Sozialleistungsbereich	80
11.5.9	Verweisung von Antragstellern auf Sozialhilfe an freie Träger	81
11.6	Archivierung von Akten einer Beratungsstelle für Kinder, Jugendliche und Erwachsene	82
11.7	Zahlung von Kriegsbeschädigtenrenten an ehemalige Mitglieder der Waffen-SS	82
12.	**Ausländer**	83
12.1	Verwaltungsvorschrift zum Ausländergesetz	83
12.2	Versehen der Behörde: Festnahme an der Grenze	83
12.3	Gruppenauskünfte aus dem Ausländerzentralregister	84
12.4	Förderung der freiwilligen Rückkehr bosnischer Flüchtlinge durch die Europäische Union	84
12.5	Verpflichtungserklärung vor Visum an ausländischen Gast	85
12.6	Machbarkeitsstudie für Asylcard	85
13.	**Finanzverwaltung**	86
13.1	Novellierung der Abgabenordnung	86
13.2	Die Steuerdatenabrufverordnung	86
13.3	Datenschutz in der Landesfinanzverwaltung	86
13.3.1	Ermittlung der Empfänger von Dorferneuerungsmitteln	86
13.3.2	Ermittlung der steuerlichen Verhältnisse noch nicht bekannter Vermieter	87
13.3.3	Personenverwechslungen aufgrund eines automatisierten Abgleichverfahrens bei der ZDFin	88
13.3.4	Befugnisse der Steuerfahndung gegenüber den Kunden von Kreditinstituten	88
13.3.5	Versand von Lohnsteuerkarten unter Nutzung des ePost-Dienstes	89
13.3.6	Zugriff der Finanzämter auf Melderegisterdaten	90
13.4	Datenschutz bei der gemeindlichen Abgabenerhebung	90
13.4.1	Berücksichtigung des Datenschutzes bei der Erhebung des „Fremdenverkehrsbeitrags A"	90
13.4.2	Weitergabe von Namen und Adressen der Steuerpflichtigen der Grundsteuer A an eine Jagdgenossenschaft	91
13.4.3	Gewerbesteuer: Beteiligung der Ortsgemeinden und Ortsbürgermeister	91
13.4.4	Datenerhebung eines Eigenbetriebs Wasser- und Abwasserwerk zu Planungs- und Veranlagungszwecken	92
14.	**Wirtschaft und Verkehr**	92
14.1	Überprüfung der persönlichen Zuverlässigkeit bei der Beschäftigung von Wachpersonen	92
14.2	Der geplante Erlaß einer Verwaltungsvorschrift zur Durchführung des Aufstiegsfortbildungsförderungsgesetzes (sog. „Meister-BAföG")	93
14.3	Untersagungsverfügung nach dem Gaststättengesetz	94
14.4	Übermittlung von Firmendaten der Industrie- und Handelskammer an eine Kreisverwaltung	94
14.5	Verwaltungsvorschrift der Landesregierung zur Bekämpfung der Korruption in der öffentlichen Verwaltung	95
14.6	Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes	96
14.7	Neukonzeption des automatisierten Ordnungswidrigkeitenverfahrens	96

		Seite
14.8	Halteranfragen im automatisierten Ordnungswidrigkeitenverfahren	97
14.9	Antragsvordruck zur Erteilung einer Parkberechtigung	97
14.10	Änderung der Fahrzeugscheine durch die Meldebehörde bei Umzug innerhalb des Zulassungsbezirks	97
14.11	Automatische Gebührenerhebung auf Autobahnen – der Feldversuch ist abgeschlossen	98
15.	**Landwirtschaft, Weinbau und Forsten**	98
15.1	Flurbereinigungsverfahren: „Sprechende Nummern" auf den Begrenzungspflöcken	98
15.2	Errichtung einer Tierhalterdatei bei einer Bezirksregierung	98
15.3	Betriebsdatenerhebung im Rahmen der Entsorgung von Reststoffen aus der Weinbereitung	99
15.4	Datenschutz bei der Versendung von landwirtschaftlichen Antragsformularen	100
15.5	Datenübermittlungen an die Landwirtschaftskammer Rheinland-Pfalz	100
15.6	Nutzung von Daten der EG-Weinbaukartei zu Zwecken gemeindlicher Abgabeerhebungen	101
16.	**Statistik**	101
16.1	Mikrozensus	101
16.2	Entwurf eines Statistikregistergesetzes	102
16.3	Nutzung von Melderegistern für künftigen Zensus?	102
17.	**Personaldatenverarbeitung**	103
17.1	Personalverwaltungssysteme	103
17.2	Bekanntgabe der Stundenreduzierungen von Lehrern an den Schulelternbeirat	103
17.3	Personaldaten im Internet	104
17.4	Weitergabe der Daten Schwangerer an den Personalrat/Betriebsrat	104
17.5	Verwaltungsvorschrift zur Erstellung der Frauenförderpläne	104
17.6	Nebentätigkeitsmeldungen	105
17.7	Personaldatenübermittlung durch die ZBV zu gemeindlichen Vollstreckungszwecken	105
17.8	Bescheinigungen über die Notwendigkeit der ärztlichen Behandlung während der Arbeitszeit	106
17.9	Zulässige Datenerhebungen durch den Arbeitgeber bei Kuranträgen	106
17.10	Auslagerung des Beihilfeverfahrens auf Privatunternehmen	107
17.11	Anforderungen an Mitarbeiterbefragungen	107
17.12	Herausgabe von Personalakten an die Staatsanwaltschaft	108
17.13	Die Verbreitung von Beförderungs- und Versetzungslisten innerhalb einer großen Behörde	108
17.14	Veröffentlichung von Personaldaten aus einem Dienstordnungsverfahren	109
17.15	Die Aufnahme von Pfändungsverfügungen in die Personalakte	110
17.16	Datenerhebungen durch die ZBV im Hinblick auf Kindergeld und Ortszuschlag	111
17.17	Datenschutz bei dienstlichen Telefonanlagen	111
17.18	Auskunftspflicht der Personalverwaltung gegenüber dem Petitionsausschuß des Landtags	112
17.19	Entwurf eines Landesgesetzes zur Neuregelung des Disziplinarrechts	113
18.	**Datenschutz im kommunalen Bereich**	113
18.1	Änderung der Kommunalwahlordnung	113
18.2	Bildung von Wahlvorständen	113
18.3	Tagesordnung von öffentlichen Gemeinderatssitzungen	114
18.4	Unterrichtungsrechte des Gemeinderates	114
18.5	Öffentliche Berichterstattung über Ratssitzungen	115
18.6	Schweigepflicht von Ehrenbeamten	115
18.7	Datenschutz und Familienforschung	115
18.8	Unterrichtung von Nachlaßgerichten durch die Standesämter	116
18.9	Die Ehefrau des Ortsbürgermeisters – ein Datenschutzproblem!	116
18.10	Bürgerbefragung	117
18.11	Datenerhebung zur Erstellung eines Mietspiegels	118
18.12	Outsourcing von Großrechneranwendungen	118
18.13	Datenübermittlungen an die Abwasserwerke	119
18.14	Interessenkonflikte bei behördlichen Datenschutzbeauftragten	119
19.	**Telekommunikation**	120
19.1	EG-Richtlinie zum Datenschutz im ISDN	120
19.2	Das Telekommunikationsrecht in Bewegung (Postreform III)	120
19.3	Grundsätzliches zum Telekommunikationsgesetz	121

		Seite
19.4	Das einfachgesetzliche Fernmeldegeheimnis	121
19.5	Sicherheitsanforderungen	122
19.6	Telekommunikationsdienstunternehmen-Datenschutzverordnung	122
19.6.1	Verbindungsdaten	123
19.6.2	Einzelverbindungsnachweis	123
19.6.3	Fangschaltung	123
20.	Medien	124
20.1	Datenschutz in der multimedialen Gesellschaft	124
20.1.1	Begriff und Anwendungsfelder	124
20.1.2	Datenverschlüsselung – ein „heißes Eisen"	124
20.2	Datenschutz im Internet	125
20.3	Die Regelungen des Informations- und Kommunikationsdienste-Gesetzes	126
20.3.1	Teledienstegesetz	126
20.3.2	Teledienstedatenschutzgesetz	126
20.3.3	Signaturgesetz	128
20.4	Der Staatsvertrag über Mediendienste	128
20.5	Das Landesgesetz zum Mediendienstestaatsvertrag	128
20.6	Digitales Fernsehen	129
20.7	Anwendung des neuen Rechts	129
21.	Technischer und organisatorischer Datenschutz	130
21.1	Kontroll- und Beratungstätigkeit	130
21.2	Technisch-organisatorische Datenschutzfragen in ausgewählten Verfahren	130
21.2.1	DNS-Spurendokumentation beim Landeskriminalamt	130
21.2.2	Überwachung des Fernmeldeverkehrs	131
21.2.2.1	Überwachung von ISDN- und Mobiltelefonaten beim Landeskriminalamt	131
21.2.2.2	Neukonzeption der Überwachung des Fernmeldeverkehrs	133
21.2.3	Elektronische Zeiterfassung bei den obersten Landesbehörden	133
21.2.4	Computerunterstützte Betriebsprüfung (CUB) bei der Landesversorgungsanstalt Rheinland-Pfalz	134
21.2.5	Verarbeitung medizinischer Daten bei einer Beratungsstelle	134
21.2.6	Zugriffskontrolle bei der Verarbeitung von Krankenversicherungsdaten	135
21.2.7	Bibliothekssystem einer Universität	135
21.2.7.1	Erfolgreicher „Hack" bei den Benutzerdaten	135
21.2.7.2	Was Paßwörter über ihre Benutzer erzählen	137
21.2.8	ISDN-Telekommunikationsanlage der Landesregierung	137
21.2.9	Verarbeitung von Krankenversicherungsdaten bei der Arbeitsgemeinschaft „AOK Rechenzentrum Mitte"	137
21.2.10	Einsatz von Chipkarten im Sozialamt einer Stadtverwaltung	138
21.3	Behinderung der Kontrolltätigkeit des LfD	138
21.4	Landesdaten- und Kommunikationsnetz Rheinland-Pfalz	139
21.4.1	Abkehr vom reinen Verwaltungsnetz	139
21.4.2	Die „Brandmauer" – das Firewall-Konzept des LDKN	139
21.5	Fernwartung	140
21.6	Anbindung öffentlicher Stellen an das Internet	140
21.7	Telearbeit und Datenschutz	141
21.8	Datenschutzregister	143
21.8.1	Entwicklung und gegenwärtiger Stand	143
21.8.2	Zentral entwickelte Verfahren	143
21.8.3	Anmeldepflicht nach § 27 LDSG	144
21.8.3.1	Textverarbeitung	144
21.8.3.2	Internet-Anschluß	144
22.	Öffentlich-rechtliche Wettbewerbsunternehmen, Sparkassen	145
22.1	Nutzung von Daten einer Direktmarketingfirma zu Werbezwecken	145
22.2	Beschränkung der filialübergreifenden Zugriffsmöglichkeiten auf Bankkonten	146
22.3	Personenverwechslung bei Kontenpfändung	146
22.4	Umsetzung des Geldwäschegesetzes, Personalausweiskopien durch Kreditinstitute	147
22.5	Übermittlung der Jahresabrechnung für Strom an einen Wohnungseigentümer	147

		Seite
23.	Sonstiges	147
23.1	Datenübermittlung aus Akten des Bauaufsichtsamtes	147
23.2	Einsichtnahme in eine Bauakte durch einen Nachbarn	148
23.3	Datenerhebungen und -übermittlungen im Zusammenhang mit der Aufstellung des Bebauungsplans	148
23.4	Datenübermittlungen durch die Lastenausgleichsämter	149
23.5	Härtefonds des Landes zur Unterstützung von Opfern des Nationalsozialismus	150
23.6	Wahlgeheimnis	151
23.7	Inhalt von Abmarkungsbenachrichtigungen	151
23.8	Weitergabe von Daten aus dem Waffenregister	151
24.	Schlußbemerkung	152
24.1	Zur Situation der Geschäftsstelle	152
24.2	Veröffentlichungen der Dienststelle	152
24.3	Zusammenarbeit mit anderen Datenschutzinstitutionen	152
24.4	Resümee und Ausblick	153

Anlagen

		Seite
1	Entschließung „Datenschutz bei elektronischen Geldbörsen und anderen kartengestützten Zahlungssystemen"	154
2	Entschließung „Weiterentwicklung des Datenschutzes in der Europäischen Union"	155
3	Entschließung „Datenschutz bei der Neuordnung der Telekommunikation (Postreform III)"	157
4	Entschließung „Planungen für ein Korruptionsbekämpfungsgesetz"	159
5	Entschließung „Datenschutzrechtliche Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen"	160
6	Entschließung „Forderungen an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien (außerhalb der Öffentlichkeitsfahndung der Ermittlungsbehörden)"	163
7	Entschließung „Modernisierung und europäische Harmonisierung des Datenschutzrechts"	164
8	Entschließung „Transplantationsgesetz"	165
9	Entschließung „Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen"	165
10	Entschließung „Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich"	166
11	Entschließung „Beratungen zum StVÄG 1996"	167
12	Entschließung „Genetische Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke"	168
13	Entschließung „Geplante Verpflichtung von Teledienstanbietern, Kundendaten an Sicherheitsbehörden zu übermitteln"	169
14	Entschließung „Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen"	170
15	Entschließung „Achtung der Menschenrechte in der Europäischen Union"	171
16	Entschließung „Informationelle Selbstbestimmung und Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren"	172
17	Thesenpapier „Staatliche Eingriffsbefugnisse in der modernen Informationsgesellschaft"	174

Abkürzungen

ABl.	Amtsblatt
AG	Amtsgericht
AFIS	Automatisiertes Fingerabdruck-Identifizierungssystem
AFBG	Aufstiegsfortbildungsförderungs-gesetz
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
AsylVfG	Asylverfahrensgesetz
AuslG	Ausländergesetz
AZR	Ausländerzentralregister
AZRG	Ausländerzentralregistergesetz
BAFl.	Bundesamt für die Anerkennung ausländischer Flüchtlinge
BAföG	Bundesausbildungsförderungsgesetz
BarchG	Bundesarchivgesetz
BauGB	Baugesetzbuch
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Daten-schutz
BFH	Bundesfinanzhof
BFHE	Sammlung der Entscheidungen des Bundesfinanzhofs
BFH/NV	Sammlung amtlich nicht veröffent-lichter Entscheidungen des Bundes-finanzhofs
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGS	Bundesgrenzschutz
BGSG	Bundesgrenzschutzgesetz
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BSHG	Bundessozialhilfegesetz
BtMVV	Betäubungsmittel Verschreibungs-verordnung
BVG	Bundesversorgungsgesetz
BVerfGE	Sammlung der Entscheidungen des Bundesverfassungsgerichts
BZRG	Bundeszentralregistergesetz
CR	Computer und Recht
CUST	Computerunterstützung der Staats-anwaltschaft
DIZ	Daten- und Informationszentrum Rheinland-Pfalz
DOG	Dienstordnungsgesetz
DÖV	Die öffentliche Verwaltung
Drs.	Drucksache
DSchPflG	Denkmalschutz- und -pflegegesetz
DSK	Datenschutzkommission
DuD	Datenschutz und Datensicherheit
EFG	Entscheidungen der Finanzgerichte
EGV	Vertrag über die Europäische Gemeinschaft
EStG	Einkommensteuergesetz
EU	Europäische Union
EWOIS	Einwohnerinformationssystem
FachhochschulG	Fachhochschulgesetz
ff.	(fort-)folgende
FÜV	Fernmeldeüberwachungsverordnung
GAST	Geschäftsstellenautomation der Staats-anwaltschaften
GEA	Generalerrichtungsanordnung
GemO	Gemeindeordnung
GewO	Gewerbeordnung
GG	Grundgesetz
GStB	Gemeinde- und Städtebund
GVBl.	Gesetz- und Verordnungsblatt
GVG	Gerichtsverfassungsgesetz
HFR	Höchstrichterl. Finanzrechtsprechung
IHK	Industrie- und Handelskammer
INPOL	Polizeiliches Informationssystem des Bundes und der Länder
i. S. v.	im Sinne von
ISD	Internationaler Suchdienst Arolsen
ISDN	Integrated Services Digital Network
IuKDG	Informations- und Kommunikations-dienste-Gesetz
i. V. m.	in Verbindung mit
JVA	Justizvollzugsanstalt
KAG	Kommunalabgabengesetz
KBA	Kraftfahrtbundesamt
KHG	Krankenhausfinanzierungsgesetz
KpS	Kriminalpolizeiliche personenbezogene Sammlung – Kriminalakten –
KV	Kassenärztliche Vereinigung
KWO	Kommunalwahlordnung
KZV	Kassenzahnärztliche Vereinigung
LAbfWAG	Landesabfallwirtschafts- und Altlasten-gesetz
LarchG	Landesarchivgesetz
LBG	Landesbeamtengesetz
LDKN	Landesdaten- und Kommunikationsnetz Rheinland-Pfalz
LDSG	Landesdatenschutzgesetz
LfD	Landesbeauftragter für den Datenschutz
LfUG	Landesamt für Umweltschutz und Gewerbeaufsicht
LHO	Landeshaushaltsordnung
LKA	Landeskriminalamt
LKG	Landeskrankenhausgesetz
LPersVG	Landespersonalvertretungsgesetz
LVA	Landesversicherungsanstalt
LVSG	Landesverfassungsschutzgesetz
MAJA	Mainzer Automatisierte Justiz-anwendungen
MDK	Medizinischer Dienst der Kranken-versicherung
MeldDÜVO	Meldedatenübermittlungsverordnung
MG	Meldegesetz
MiStra	Mitteilungen in Strafsachen
MRRG	Melderechtsrahmengesetz
NJW	Neue Juristische Wochenschrift
NVwZ	Neue Zeitschrift für Verwaltungsrecht
OFD	Oberfinanzdirektion
ÖGdG	Gesetz über den öffentlichen Gesundheits-dienst

OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz
PC	Personalcomputer
PKS	Polizeiliche Kriminalstatistik
POG	Polizei- und Ordnungsbehördengesetz
POLDOK	Polizeiliches Hinweis- und Spuren-dokumentationssystem
POLIS	Polizeiliches Informationssystem Rheinland-Pfalz
PPA	Pfälzische Pensionsanstalt
PStG	Personenstandsgesetz
RdNr.	Randnummer
RiA	Recht im Amt
RiStBV	Richtlinie für das Straf- und Bußgeld-verfahren
SchulG	Schulgesetz
SDÜ	Schengener Durchführungsüberein-kommen
SGB I	Sozialgesetzbuch – Erstes Buch –
SGB V	Sozialgesetzbuch – Fünftes Buch –
SGB VIII	Sozialgesetzbuch – Achtes Buch –
SGB X	Sozialgesetzbuch – Zehntes Buch –
SigG	Signaturgesetz
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVÄG	Strafverfahrensänderungsgesetz
StVG	Straßenverkehrsgesetz
StVO	Straßenverkehrsordnung
StVZO	Straßenverkehrs-Zulassungsordnung
Tb.	Tätigkeitsbericht
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikationsdienst-unternehmen-Datenschutzverordnung
TKG	Telekommunikationsgesetz
TÜ	Telefonüberwachung
Tz.	Textziffer
VGH	Verwaltungsgerichtshof
VO	Verordnung
VOB	Verdingungsordnung für Bauleistungen
VOL	Verdingungsordnung für Leistungen
VV	Verwaltungsvorschrift
VwVfG	Verwaltungsverfahrensgesetz
VwGO	Verwaltungsgerichtsordnung
ZEVIS	Zentrales Verkehrsinformations-System
ZPO	Zivilprozeßordnung

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
15. Tätigkeitsbericht	Drucksache 12/7589	vom	16. November	1995

1. Vorbemerkung

Wie alle vorangegangenen Tätigkeitsberichte ist auch der vorliegende kein bloßer „Mängelbericht". Er soll vielmehr das breite Spektrum der Tätigkeit der Behörde des LfD widerspiegeln. Natürlich wird auch über Verstöße gegen datenschutzrechtliche Vorschriften berichtet; überwiegend werden aber gutachtliche Stellungnahmen zu datenschutzrechtlichen Zweifelsfragen, die an den LfD herangetragen worden sind, veröffentlicht. Der Tätigkeitsbericht soll insofern der Verwaltungspraxis und damit auch dem Bürger bei der Klärung von Datenschutzfragen helfen. Dadurch ist der Umfang des Berichts erneut angewachsen. Zur durchgängigen zusammenhängenden Lektüre ist er kaum geeignet; er hat vielmehr in weiten Teilen den Charakter eines Handbuches mit Fällen und Lösungen zum Datenschutzrecht.

Der LfD hofft, daß aus den Mosaiksteinen des Berichts folgendes deutlich wird:

- Datenschutz ist praktizierter Grundrechtsschutz unter den Bedingungen moderner Datenverarbeitung;
- wie jedes Grundrecht gilt das auf Datenschutz nicht schrankenlos;
- im Kernbereich des informationellen Selbstbestimmungsrechts darf auch der moderne Gefahrenabwehr- und -verhütungsstaat keineswegs alles tun, was auf den ersten Blick wünschenswert erscheint (s. Großer Lauscheingriff oder Kryptographieverbot).

Eine Standortbestimmung des Datenschutzes muß die Entwicklung der Datenverarbeitungstechnik berücksichtigen. So richtig es ist, daß der Gesetzgeber den Geltungsbereich des Datenschutzgesetzes auf herkömmliche Formen der Datenverarbeitung ausgedehnt hat, die besondere Dimension der Gefährdung von Persönlichkeitsrechten beruht auf der automatisierten Datenverarbeitung. Die Einbeziehung der Aktenverarbeitung in den Schutzbereich berücksichtigt lediglich die Technikentwicklung, die eine Trennung und damit eine unterschiedliche rechtliche Beurteilung der herkömmlichen und der automatisierten Datenverarbeitung kaum noch zuließe.

In die Amtszeit des LfD fallen zwei technische Entwicklungen, die freilich aus der Sicht des Datenschutzes den Charakter von Quantensprüngen haben. Zum einen ist die Dezentralisierung der Datenverarbeitung zu nennen, die zwar schon Mitte der achtziger Jahre einsetzte, aber erst mit der Markteinführung außerordentlich leistungsfähiger Kleinrechner und peripherer Systeme in diesem Jahrzehnt die besondere Gefährdungsdimension erlangte, die ihr heute eignet. Hierzu zählen auch Datenträger, die die Adressen von mehr als 30 Mio. Telefonanschlußnehmern enthalten und die auf praktisch jedem halbwegs leistungsfähigen PC verarbeitet werden können. Zum anderen ist es die Vernetzung von Datenverarbeitungssystemen, die heute in einem vor wenigen Jahren noch völlig unvorstellbaren Ausmaß realisiert ist und sich mit rasender Geschwindigkeit weiter ausbreitet. Inzwischen gibt es Hunderttausende Internetzugänge in der Bundesrepublik. Ebenso viele Personen und Institutionen hinterlassen bei der Nutzung von Internet elektronische Datenspuren über Interessen und Lebensgewohnheiten und öffnen damit bislang tatsächlich geschützte Sphären dem potentiellen Zugriff. Jeder, der die Entwicklung der automatisierten Datenverarbeitung interessiert verfolgt, weiß, daß es den Rahmen einer zusammenfassenden Darstellung dieser Entwicklung sprengen würde, auch nur die wichtigsten Gefährdungskonstellationen zu nennen.

Eine Standortbestimmung des Datenschutzes muß als Koordinaten die Technikentwicklung sowie die Veränderung der gesellschaftlichen und rechtlichen Rahmenbedingungen zugrunde legen. Kurz zusammengefaßt ist die gegenwärtige Situation des Datenschutzes wie folgt einzuschätzen:

- Datenschutz hat sich als Grundrechtsschutz etabliert. Er ist als Äquivalent zur Technikentwicklung prinzipiell anerkannt.
- Es ist im wesentlichen gelungen, den Datenschutz mit anderen grundrechtlichen Gewährleistungen in praktische Konkordanz zu bringen.
- Der zeitliche Abstand zwischen technischer Entwicklung und Anpassung des Datenschutzrechts nimmt zu. Hier müßten im Interesse des Grundrechtsschutzes verstärkte Anstrengungen unternommen werden.
- Zunehmend werden Aufgaben von öffentlichen auf private Stellen mit der Folge verlagert, daß umfangreiche Datenbestände an Private übergeben werden; derzeit sind die konkreten Schranken einer solchen Einbeziehung Privater in die Aufgabenerfüllung des Staates noch nicht abschließend geklärt.
- Die mit den Stichworten „Multimedia" und „Internet" angesprochene technische Entwicklung hat auch für die der Kompetenz des LfD zuzurechnenden öffentlichen Stellen des Landes große Bedeutung. Hier stellen sich eine Reihe datenschutzrechtlicher Fragen, angefangen von den Verschlüsselungsmöglichkeiten für den Nutzer über die Zugriffsmöglichkeiten für Sicherheitsbehörden bis zur Frage, in welchem Umfang spurenlose Kommunikation möglich sein soll. Lösungen für diese und viele andere Fragen, die z. Z. in der Diskussion sind, müssen erst noch erarbeitet werden. Auch das Stichwort „Teleworking" ist in diesem Zusammenhang zu erwähnen: Hier stellen sich insbesondere Fragen des zulässigen Umfangs von Leistungskontrollen und des technischen Datenschutzes.

- Eine weitere wesentliche Entwicklung im Datenschutzbereich ist die mit der Europäisierung des Datenschutzes einhergehende Tendenz zur europäischen Vereinheitlichung des Datenschutzrechts. Hier entstehen erhebliche Schwierigkeiten: Traditionelle Grundpfeiler des deutschen Verfassungsrechts wie der Gewaltenteilungsgrundsatz, das Prinzip der parlamentarischen Verantwortlichkeit und die Trennung von öffentlichem und Privatrecht sind nur schwer vereinbar mit Regelungen aus ganz anderen Rechtssystemen, die das europäische Datenschutzrecht rezipiert hat.

- Im übrigen sind – wie auch sonst im Verwaltungsrecht – die Vollzugsdefizite im Datenschutz größer als die Regelungsdefizite. Vorhandenes Datenschutzrecht reicht für die Problemlösung meistens aus (Beispiel: Sozialdatenschutz). Der Gesetzgeber sollte sich stärker zurückhalten.

- Die Entwicklung des Datenschutzrechts kann trotz einer Unzahl bereichsspezifischer Regelungen auf Generalklauseln nicht verzichten; es ist eine vernünftige Symbiose zwischen generellen und Spezialregelungen anzustreben.

- Im exekutiven Bereich bietet der Datenschutz kein ganz einheitliches Bild. Vereinzelt wird er nicht als Gestaltungsaufgabe, sondern als Vollzugshindernis verstanden (s. auch die Kontroverse mit dem Ministerium der Justiz über die Reichweite des Datenschutzrechts, Vorbemerkung Tz. 7). Soweit dies nicht auf fehlendem politischem Durchsetzungswillen beruht, könnte die Intensivierung der Fortbildung hilfreich sein.

2. Weiterentwicklung des Datenschutzrechts

2.1 Grundsätzliche Tendenzen

Die Tendenz, für möglichst viele Bereiche der Datenverarbeitung bereichsspezifische Regelungen zu verlangen, hat zu einer inzwischen nahezu unüberschaubaren Flut von speziellen Datenschutzregelungen in einzelnen Fachgesetzen geführt. Heft 1 der „Informationen zum Datenschutz", Datenschutzrechtliche Vorschriften, Hrsg. vom LfD, verdeutlicht dies mit seiner umfangreichen Zahl bereichsspezifischer Gesetze.

Die Entwicklung ist durch zwei Linien gekennzeichnet: Veränderungen im allgemeinen Datenschutzrecht, zu denen auch die Verabschiedung der EG-Datenschutzrichtlinie zu zählen ist, erweitern den Anwendungsbereich des Datenschutzes und bewirken notwendige Klarstellungen, leisten freilich nicht in genügendem Maße die Anpassung an die neuen technischen Gegebenheiten. Als Beispiel für letzteres ist die Chipkartentechnik zu nennen, die sich noch weitgehend in einem datenschutzrechtsfreien Raum vollzieht. Weitaus gravierender sind indessen die Veränderungen, die der Datenschutz durch eine Fülle rechtlicher Detailregelungen außerhalb der Datenschutzgesetze erfährt. Diese Veränderungen kennzeichnen das Bemühen des Gesetzgebers, den Erfordernissen einer sich wandelnden Gesellschaft zu entsprechen. Zum Teil erweitern sie den Datenschutz, etwa durch detailliertere Regelungen über die Verwendung von Abhörprotokollen durch die Staatsanwaltschaften, zu einem nicht geringen Teil drängen sie ihn zurück, um andere wichtige Staatsziele zu fördern (Beispiel: Lauscheingriff). Dabei geht es fast immer um neue Formen der Datenerhebung und um die Verbesserung der Datenübermittlung durch Online-Zugriffe und Datenabgleiche.

Der erstrebte Vorteil dieser Regelungen, daß jeder Bürger grundsätzlich auf der Basis normenklarer Gesetze erkennen kann, welche Befugnisse die öffentlichen Stellen beim Umgang mit seinen Daten haben, droht sich zum Nachteil zu entwickeln: Die bereichsspezifischen Regelungen werden immer detaillierter, unüberschaubarer, aber auch unsystematischer und damit unverständlicher.

Vor diesem Hintergrund vertritt der LfD die Auffassung, daß das Augenmerk verstärkt darauf zu richten ist, nur dann und nur in dem Umfang Spezialregelungen zu schaffen, wenn und soweit das allgemeine Datenschutzrecht mit seinen nunmehr fein ziselierten und detaillierten Regelungen nicht zu befriedigenden Ergebnissen führt.

2.2 Regelung des parlamentsspezifischen Datenschutzes in einer Datenschutzordnung

Das Landesdatenschutzgesetz gilt nicht für den Landtag, seine Gremien, seine Mitglieder, die Fraktionen sowie deren Verwaltungen und deren Beschäftigte, soweit diese in Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten (§ 2 Abs. 2 LDSG). In dieser „Parlamentsklausel" wird das Parlament zugleich zum Erlaß einer Datenschutzordnung ermächtigt, die den Datenschutz bei der Wahrnehmung parlamentarischer Aufgaben regelt.

Die Datenschutzordnung muß den Anforderungen entsprechen, die das Bundesverfassungsgericht im Volkszählungsurteil (BVerfGE 65,1 ff.) an Eingriffe in das informationelle Selbstbestimmungsrecht gestellt hat: Diese bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit und dem Grundsatz der Verhältnismäßigkeit entspricht.

Der Landtag Rheinland-Pfalz hat eine solche Datenschutzordnung am 31. Oktober 1995 verabschiedet. Sie orientiert sich an

einem Thesenpapier zum parlamentsspezifischen Datenschutzrecht und an einer Musterdatenschutzordnung, die von der Konferenz der Präsidenten der deutschen Landesparlamente im Mai 1995 abschließend beraten wurde. Die Datenschutzkontrolle obliegt nach § 12 der Datenschutzordnung dem Ältestenrat des Landtags.

Bei der Regelung des parlamentsspezifischen Datenschutzes war die Grundsatzfrage zu entscheiden, ob die Datenschutzordnung des Landtags als formelles Gesetz zu verabschieden ist oder ob ein Gesetz im materiellen Sinne ausreicht. Eingriffe in das informationelle Selbstbestimmungsrecht bedürfen stets einer normenklaren gesetzlichen Grundlage (BVerfGE 65, 1). Dies gilt auch für Informationseingriffe durch das Parlament.

Dieser Gesetzesvorbehalt ist freilich vor dem Hintergrund der verfassungsrechtlich verbürgten Parlamentsautonomie (Art. 85, 82, 83 Abs. 6 und Art. 94 der Verfassung für Rheinland-Pfalz) zu sehen. Danach hat das Parlament das Recht, sich selbst zu organisieren und zu verwalten. Dazu gehört auch das Recht, die eigenen Angelegenheiten selbständig und ohne Mitwirkung anderer Staatsorgane zu regeln. Hätte die Datenschutzordnung des Landtags nur Binnenwirkung, würde sie nur die Abgeordneten binden, nicht aber auch Dritte berechtigen und verpflichten; sie wäre durch die sog. Geschäftsordnungsautonomie des Landtags gedeckt. Dies ist aber nicht der Fall, da die Datenschutzordnung des Landtags auch Außenwirkung hat; denn sie regelt Eingriffe in das informationelle Selbstbestimmungsrecht auch solcher Personen, die nicht dem Landtag angehören. Insoweit beruht die Datenschutzordnung des Landtags nicht auf der Geschäftsordnungsautonomie.

Rechtsfragen des Parlamentsdatenschutzes wurden in einer Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter der Federführung des LfD Rheinland-Pfalz im Juni 1995 erörtert. In der Grundsatzfrage, ob es zur Regelung des Parlamentsdatenschutzes eines (formellen) Gesetzes bedürfe, verblieben Meinungsverschiedenheiten. In bezug auf die vom Landesgesetzgeber Rheinland-Pfalz gewählte Regelungsform vertrat der LfD die Auffassung, daß diese verfassungskonform sei. Um Außenwirkung zu entfalten, genüge auch ein Beschluß des Landtages, wie es etwa bei Staatsverträgen Art. 72 Abs. 2 der Bayerischen Verfassung regelt. Eine explizite verfassungsrechtliche Ermächtigung ist in Rheinland-Pfalz nicht erforderlich. Es genügt vielmehr die Ermächtigung des Parlaments in § 2 Abs. 2 LDSG (Parlamentsklausel), den parlamentsspezifischen Datenschutz selbständig und eigenverantwortlich zu regeln. Verfassungsrechtlich ist dies deshalb unbedenklich, weil die außenwirksamen Regelungen der Datenschutzordnung des Landtags lediglich einen Annex zum Verfahrensrecht bilden, bei dem die Regelungsschwerpunkte liegen. Die in diesem Falle notwendige Veröffentlichung im Gesetz- und Verordnungsblatt für das Land Rheinland-Pfalz ist erfolgt (GVBl. 1995 S. 467 = BS 1101-7).

3. Datenschutz in Europa

3.1 EG-Datenschutzrichtlinie

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG L 281 vom 23. November 1995 S. 31 ff.) ist inzwischen verabschiedet worden.

Sie stützt sich auf die Regelungskompetenz „Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten zur Erreichung des Binnenmarktes" gem. Art. 100 a EGV. Dort wird auf Art. 7 a EGV Bezug genommen, der in seinem Satz 2 den Binnenmarkt umschreibt als einen Raum ohne Binnengrenzen, in dem der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital gewährleistet ist. An dieser Stelle ist es aber auch wichtig festzuhalten, daß die Union mit der Richtlinie im Bereich der Grund- und Freiheitsrechte gesetzgeberisch tätig wurde.

Bereits aus dem Titel „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" wird das Dilemma zwischen Datenschutz auf der einen Seite und funktionsfähigem Binnenmarkt bezüglich des Datenverkehrs auf der anderen Seite deutlich.

Als Rechtsgrundlage für die Datenschutzrichtlinie hat die Europäische Kommission Art. 100 a EGV gewählt, weil es für die Errichtung und das Funktionieren des Binnenmarktes gem. Art. 7 a EGV erforderlich ist, personenbezogene Daten von einem Mitgliedstaat in einen anderen Mitgliedstaat zu übermitteln. Hier wird erkennbar, daß es beim „EG- Datenschutz" nicht vorrangig um ein Abwehrrecht gegenüber dem Staat geht.

In diesem Zusammenhang ist auf die Beweggründe und die Interessen, welche bei der Gestaltung der Richtlinie mitgewirkt haben, hinzuweisen. Die bisherigen Aktivitäten der EG sind eher auf wirtschaftliche Gesichtspunkte fixiert. Dies drückt sich vor allem in Art. 1 Abs. 2 der Richtlinie aus, wonach die Mitgliedstaaten den freien Verkehr von personenbezogenen Daten aus Datenschutzgründen nicht beschränken oder untersagen dürfen. Danach sind Divergenzen bezüglich des Datenschutzniveaus nicht heranzuziehen, „um die freie Übermittlung von personenbezogenen Daten zwischen Mitgliedstaaten zu verbieten". Hoher Datenschutz bedeutet erhöhten technischen und personellen Aufwand, der wiederum die Kosten erhöht. Es leuchtet ein, daß die Europäische Kommission vermeiden möchte, daß Unternehmen ihre Datenverarbeitung aus Kostengründen außerhalb

der Europäischen Union ansiedeln. Aufgrund des Rahmens, den die Richtlinie setzt, verbleibt den Mitgliedstaaten ein gehöriger Spielraum bei der Regelung des Datenschutzrechts. Somit ist es möglich, daß erhebliche Unterschiede bei der Durchführung der Richtlinie auftreten. Ein Beispiel: Die Mitgliedstaaten können im Falle der Verarbeitung besonderer Kategorien sensibler personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben sogar andere als die in Art. 8 Abs. 2 der Richtlinie genannten Ausnahmen vorsehen (vgl. Art. 8 Abs. 4). Hier deutet sich die Entwicklung zu einem unterschiedlichen Schutzniveau innerhalb der Europäischen Union an. Daran wird deutlich, daß nicht ein gleiches, sondern ein unterschiedliches europäisches Schutzniveau im Rahmen der Richtlinie entsteht.

Nach Einschätzung des LfD ist die Effektivität des Datenschutzes in der Europäischen Union eher durch bereichsspezifische Lösungen zu gewährleisten. Eine begrüßenswerte Entwicklung ist mit der EG-Richtlinie zum Datenschutz im ISDN in Gang gekommen (vgl. Tz. 19.1).

Der LfD hat sich seit dem 13. Tb. mit der Entstehungsgeschichte der Richtlinie befaßt (vgl. 13. Tb., Tz. 3; 14. Tb., Tz. 3; 15. Tb., Tz. 3.1). Da der wesentliche Inhalt bereits im 15. Tb. ausführlich dargestellt wurde, kann darauf verwiesen werden.

3.2 Die Umsetzung der Richtlinie in nationales Recht

Die Richtlinie ist bis zum 24. Oktober 1998 in deutsches Recht umzusetzen. Richtlinien der EG sind gem. Art. 189 Satz 3 EGV für jeden Mitgliedstaat hinsichtlich des zu erreichenden Ziels verbindlich, überlassen jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel für die Umsetzung in nationales Recht.

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer Sitzung am 14./15. März 1996 Eckpunkte zur Modernisierung und europäischen Harmonisierung des Datenschutzrechts in einer Entschließung erarbeitet (vgl. Anlage 7). Im Zusammenhang mit der Umsetzung der EG-Richtlinie sind darin ihre Kernforderungen formuliert. Darüber hinaus wurde ein Positionspapier zur Umsetzung der EG-Datenschutzrichtlinie und zur Novellierung des Bundesdatenschutzgesetzes mit einer ganzen Reihe von konkreten Änderungsvorschlägen abgefaßt, das der BfD dem Bundesministerium des Innern zugeleitet hat.

Es zeichnet sich ab, daß die Bundesregierung keine Neigung verspürt, die gesetzliche Anpassung über das zwingend notwendige Maß hinaus vorzunehmen. So ist der Anwendungsbereich der Richtlinie beschränkt auf den Geltungsbereich des EG-Vertrages. Beispielsweise ist die Datenverarbeitung von Polizei und Nachrichtendiensten von der Richtlinie nicht berührt. Mithin ist eines der zentralen Probleme der aktuellen Diskussion, wie man Gesetzesmaterien behandelt, die nicht der Regelungskompetenz der EG unterliegen. Es ist offensichtlich vorgesehen, daß in einer Reihe von Fachgesetzen jeweils bestimmte Vorschriften des (novellierten) BDSG keine Anwendung finden sollen. Die entsprechenden Vorschriften seien auszuschließen, da die EG-Datenschutzrichtlinie für den Sicherheitsbereich keine Anwendung finde. In seinem 15. Tb. (Tz. 3.1.1.3) hat der LfD auf diese (von ihm befürchtete) Entwicklung hingewiesen und ausgeführt: „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' [der Europäischen Union] betroffen ist. (...). Datenschutz ist die klassische Querschnittsmaterie, die sämtliche Bereiche der modernen Informationsgesellschaft betrifft; er sollte sich grundsätzlich nicht an ‚Säulen' orientieren."

In erster Linie ist das Bundesdatenschutzgesetz wegen seiner Geltung im nichtöffentlichen Bereich von der Anpassungspflicht betroffen. Die Kontrollpflichten der Richtlinie werden vor allem Auswirkungen für den Privatsektor haben. Denn der Kontrollbehörde ist eine Untersuchungsbefugnis einzuräumen, die nicht wie nach § 38 BDSG an einen Anlaß gebunden ist. Damit wird berücksichtigt, daß die rasante Zunahme der Verarbeitung personenbezogener Daten im nichtöffentlichen Bereich zu einer starken Gefährdung des Persönlichkeitsrechts geführt hat. Nach dem akutellen Stand sind seitens des Bundesinnenministeriums u. a. folgende Überlegungen in bezug auf die Umsetzung angestellt worden:

- Der sachliche Anwendungsbereich des Bundesdatenschutzgesetzes ist mit Art. 3 Abs. 1 der EG-Richtlinie insoweit in Übereinstimmung zu bringen, als es bei automatisierten Verarbeitungen nicht mehr auf den Dateibegriff ankommt. Das Kriterium der Datei ist nur noch von Bedeutung, soweit es um die nichtautomatisierte Verarbeitung personenbezogener Daten geht.
- Die Richtlinie sieht die Erhebung personenbezogener Daten als Teil der Verarbeitung an. Das Bundesdatenschutzgesetz regelt aber nur die Erhebung für den öffentlichen Bereich, so daß es einer entsprechenden Anpassung für die Erhebung im nichtöffentlichen Bereich bedarf.
- Dem Begriff des „Empfängers" kommt nunmehr neben dem des „Dritten" eigenständige Bedeutung zu, so daß die bisherige Verwendung dem Bundesdatenschutzgesetz anzupassen ist.
- Die Meldepflicht für automatisierte Dateien ist neu zu regeln. Es entfällt die Meldepflicht, wenn die speichernde Stelle einen Datenschutzbeauftragten bestellt hat. Damit kann die Meldepflicht im öffentlichen Bereich vollständig entfallen, da der behördliche Datenschutzbeauftragte als obligatorische Institution eingeführt wird.

- Eine weitere Neuregelung betrifft die sog. Vorabkontrolle, wodurch bestimmte automatisierte Dateien vor Inbetriebnahme einer Prüfung durch den Datenschutzbeauftragten unterzogen werden.

- Regelungsbedarf ist in bezug auf die „automatisierte Einzelentscheidung" vorhanden. Es soll verhindert werden, daß Entscheidungen ausschließlich aufgrund von automatisiert erstellten Persönlichkeitsprofilen getroffen werden, ohne daß eine Person den Sachverhalt erneut überprüft hat.

Nachfolgend sind beispielhaft einige datenschutzrechtliche Forderungen im Hinblick auf die „Minimalumsetzung" angesprochen, die gegenwärtig diskutiert werden:

- Eine Änderung gegenüber dem BDSG ist die Ausweitung des Dateibegriffs auf alles, was nicht unstrukturiert ist. Datei ist damit schon die Akte, in der unter einem bestimmten Begriff, zum Beispiel einem Namen, Unterlagen abgelegt sind. Das Definitionsmerkmal „gleichartig aufgebaut" ist mithin aus der Definition der nichtautomatisierten Datei (§ 3 Abs. 2 Nr. 2 BDSG) herauszunehmen.

- Bezüglich der Definition der Übermittlung (§ 3 Abs. 5 Nr. 3 BDSG) sollte richtlinienkonform künftig auch die Weitergabe nicht gespeicherter Daten dem Übermittlungsbegriff unterfallen (wie in § 67 Abs. 6 Nr. 3 SGB X).

- Im Bereich der Erhebung beim Betroffenen ist die Unterrichtungspflicht um „Empfänger/Kategorien von Empfängern" zu ergänzen.

- Die Aufklärung der Betroffenen über die Folgen der Verweigerung von Angaben im Rahmen der Erhebung aufgrund einer Rechtsvorschrift und der Verweigerung einer Einwilligung hat auch ohne Verlangen der Betroffenen zu erfolgen.

- Bei der Datenübermittlung in das Ausland ist eine Regelung angebracht, die hinsichtlich der Datenübermittlung in das EU-Ausland innerhalb des Anwendungsbereichs der EG-Datenschutzrichtlinie, in das EU-Ausland außerhalb des Anwendungsbereichs der EG-Richtlinie und in Drittstaaten differenziert. Hinsichtlich der Rechtsfolgen sollten die beiden letztgenannten Gruppen gleich behandelt werden (beispielhafte Situation: Datenübermittlung des Kraftfahrtbundesamtes an die französische Polizei).

- Es ist zu klären, unter welchen Voraussetzungen ein Mitgliedstaat Daten, die er im Anwendungsbereich der EG-Datenschutzrichtlinie erhalten hat, außerhalb des Anwendungsbereichs der EG-Richtlinie verwenden darf (beispielhafte Situation: Übermittlung personenbezogener Daten, die eine französische Umweltbehörde erhebt, an die deutsche Polizei).

Soweit das Landesrecht von der Umsetzungspflicht betroffen ist, erscheint es sinnvoll, zunächst das Gesetzgebungsverfahren zum Bundesdatenschutzgesetz abzuwarten. Der Hauptgrund für eine solche Vorgehensweise liegt darin, ein begrifflich einheitliches Datenschutzrecht auf Bundes- und Länderebene zu erhalten.

3.3 Weiterentwicklung des Datenschutzes in der Europäischen Union

Ein europäisches Grundrecht auf Datenschutz ist in den Gemeinschaftsverträgen noch nicht verwirklicht. Der Vertrag über die Europäische Union nimmt zwar an zwei Stellen (Art. F Abs. 2 und Art. K.2 Abs. 2) ausdrücklich auf die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten Bezug und garantiert darin die Achtung der in der Konvention festgeschriebenen Grundrechte. Damit ist auch das Gebot der Achtung der Privatsphäre (Art. 8 der EMRK) von der Garantie des Unionsvertrages umfaßt. In den Staaten der Europäischen Union werden mit hochentwickelten Informationstechnologien vermehrt personenbezogene Daten verarbeitet und grenzüberschreitend ausgetauscht. Diese Entwicklung wird gefördert durch den rasanten Ausbau der transeuropäischen Telekommunikationsnetze, wobei das Grundrecht auf informationelle Selbstbestimmung in Gefahr gerät. Insbesondere im Hinblick auf den Ausbau des europäischen Grundrechtsschutzes haben die Datenschutzbeauftragten eine weitergehende Ergänzung der Vertragswerke gefordert (vgl. Anlage 2). Anläßlich der Revision des Europäischen Unionsvertrages hat sich der LfD Ende 1995 in einem Schreiben an den Bevollmächtigten des Landes Rheinland-Pfalz beim Bund und für Europa gewandt und sich u. a. für die Aufnahme des Grundrechts auf Datenschutz in den Vertrag über die Europäische Union eingesetzt. Daraufhin hat Rheinland-Pfalz für die Europaministerkonferenz schriftlich das Auswärtige Amt gebeten, dieses Anliegen in die Regierungskonferenz einzubeziehen. Die ausdrückliche Regelung des Datenschutzes z. B. in einer Verfassung der Europäischen Union (wie sie vom Europäischen Parlament bereits zur Erörterung gestellt wurde) würde zu einer wirksamen – unionsweiten – Absicherung des Rechts auf informationelle Selbstbestimmung beitragen. Bislang konnten diese Vorstellungen allerdings noch nicht realisiert werden. Das Thema bleibt ein Anliegen für die weitere Entwicklung auf europäischer Ebene.

3.4 Datenschutz bei den Organen und Einrichtungen der Gemeinschaft

Ein besonderes Ärgernis liegt darin, daß für die personenbezogene Datenverarbeitung durch die Organe der EG selbst ein verbindliches Datenschutzrecht fehlt. Zwar war in dem von der Europäischen Kommisson am 13. September 1990, also vor mehr als sieben Jahren, vorgelegten Datenschutzpaket eine „Erklärung der Kommisson betreffend die Anwendung der Grund-

sätze der Richtlinie auf die Organe der EG" enthalten. Dieses Vorhaben wurde allerdings nicht weiter verfolgt. Die EG-Datenschutzrichtlinie richtet sich nur an die nationalen Gesetzgeber als Adressaten. Dies ist vor allem deshalb problematisch, weil die Kommission systematisch große Mengen personenbezogener Daten von den Mitgliedstaaten anfordert und bei vielen Gemeinschaftsprojekten Daten in größerem Umfang verarbeitet werden. Daher bedarf es für die Gewährleistung des Datenschutzes durch EG-Organe einer rechtsverbindlichen Regelung. Darauf angesprochen, erklärten die Vertreter der Kommisson regelmäßig, daß man diesen Fragen große Aufmerksamkeit widme. Gleichwohl ist jahrelang nichts geschehen.

Erst am 17. Juni 1997 ist anläßlich der Konferenz des Europäischen Rates in Amsterdam bezüglich des Datenschutzes bei den Organen und Institutionen der Gemeinschaft beschlossen worden, einen neuen Artikel 213 b in den Vertrag über die Europäische Union („Maastricht II") einzufügen. Die Absätze 1 und 2 dieses Textes lauten:

- „(1) Ab 1. Januar 1999 finden die Rechtsakte der Gemeinschaft über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und dem freien Verkehr solcher Daten auf die durch den Vertrag oder auf der Grundlage des Vertrags errichteten Organe und Institutionen der Gemeinschaft Anwendung.
- (2) Vor dem in Absatz 1 genannten Datum beschließt der Rat nach dem Verfahren des Artikels 189 b die Errichtung einer unabhängigen Kontrollinstanz, die für die Überwachung der Anwendung solcher Rechtsakte der Gemeinschaft auf die Organe und Institutionen der Gemeinschaft verantwortlich ist und erläßt erforderlichenfalls andere einschlägige Bestimmungen."

Es ist zu begrüßen, daß hiermit auf politischer Ebene eine Entscheidung getroffen wurde, die vielfach formulierte datenschutzrechtliche Anliegen nunmehr berücksichtigt.

4. Meldewesen

Das Meldewesen bildet nach wie vor einen Schwerpunkt der Datenschutzarbeit. Es ist nie gelungen, das technische Verfahren EWOIS mit den gesetzlichen Vorgaben des Meldegesetzes vollständig in Übereinstimmung zu bringen. Häufig mußten vor dem Hintergrund eines nicht oder nur mit unverhältnismäßig großem Aufwand anpassungsfähigen Automationsverfahrens Lösungen akzeptiert werden, die aus der Sicht des Datenschutzes nicht in vollem Umfange zufriedenstellen. Die neuere Entwicklung ist dadurch gekennzeichnet, daß Städte und Gemeinden versuchen, den Online-Zugriff auf Meldedaten erheblich auszuweiten. Möglichst jede Mitarbeiterin und jeder Mitarbeiter soll auf Einwohnerdaten zugreifen können. Hiergegen ist dann nichts einzuwenden, wenn es zur Aufgabenerfüllung erforderlich ist und der Zugriff auf die wirklich wichtigen Merkmale beschränkt werden könnte. Hier liegt aber das Problem: Oft steht die Zugriffshäufigkeit außer Verhältnis zu den Datenschutzgefahren des Online-Zugangs, und eine Anpassung des Datenzugangs an die Erfordernisse des jeweiligen Arbeitsplatzes ist in EWOIS nur in Ausnahmefällen möglich.

Seit vielen Jahren besteht die Absicht, für das rheinland-pfälzische Einwohnermeldeverfahren eine neue technische Grundlage zu schaffen. Im Blick auf den Umstellungsaufwand im Jahr 2000 gibt es zur Zeit verstärkte Bemühungen, ein neues Verfahren zu installieren, bei dem eine Vielzahl der gegenwärtig noch bestehenden Probleme gelöst werden soll. Der LfD wird die Entwicklung sorgfältig beobachten und darauf achten, daß die notwendigen datenschutzrechtlichen Verbesserungen realisiert werden.

4.1 Datenschutzrechtliche Defizite im Zusammenhang mit der Einrichtung und Nutzung automatisierter Übermittlungsverfahren in EWOIS

Durch Nummer 27 Buchst. d des Ersten Gesetzes zur Änderung des Meldegesetzes wurde § 31 Abs. 7 MG um den Hinweis ergänzt, daß § 7 LDSG unberührt bleibt. Damit ist klargestellt, daß die Datenübermittlung innerhalb der Verwaltungseinheit, der die Meldebehörde angehört, nur dann zulässig ist, wenn die formellen und materiellen Voraussetzungen für die Einrichtung automatisierter Übermittlungsverfahren vorliegen. Zu diesen Voraussetzungen gehört, daß das automatisierte Übermittlungsverfahren unter Berücksichtigung der schutzwürdigen Belange der Betroffenen, des Schutzes besonderer Berufs- oder Amtsgeheimnisse und der Aufgaben der beteiligten öffentlichen Stellen angemessen ist (§ 7 Abs. 1 Satz 1 LDSG). Weiter ist gefordert, daß die Voraussetzungen für die Datenübermittlung im Einzelfall vorliegen (§ 7 Abs. 1 Satz 2), daß die Zulässigkeit der Übermittlung personenbezogener Daten zumindest stichprobenweise überprüft werden kann (§ 7 Abs. 4 Satz 3) und daß der LfD vor der Einrichtung eines automatisierten Übermittlungsverfahrens angehört wird (§ 7 Abs. 3).

Mit der Ergänzung des § 31 Abs. 7 MG ist der frühere Dissens zwischen dem Ministerium des Innern und für Sport und der Datenschutzkommission, die von der Geltung des Verordnungsvorbehalts nach Absatz 5 auch für automatisierte Datenübermittlungen nach Absatz 7 ausging, ausgeräumt.

Im Berichtszeitraum wurde schwerpunktmäßig überprüft, in welchem Umfang und in welcher Weise Online-Zugriffe auf Meldedaten, die unter § 31 Abs. 7 MG i. V. m. § 7 LDSG zu subsumieren sind, praktiziert werden. Hierbei wurde folgendes festgestellt:

4.1.1 Angemessenheit der Einrichtung und Nutzung von Online-Anschlüssen

Bei der Beurteilung der Angemessenheit der automatisierten Datenübermittlung sind die Vorteile, die ein solches Verfahren für die Verwaltung mit sich bringt, den Beeinträchtigungen gegenüberzustellen, die sich hieraus für die Betroffenen ergeben können. Dabei ist bei der Übermittlung von Meldedaten, selbst wenn es sich nur um Basisdaten wie Name und Anschrift handelt, zu berücksichtigen, daß diese durchaus sensitiv sein können. Zu denken ist beispielsweise an die Adressen der Insassen von Vollzugsanstalten oder von Krankenhäusern und von Pflegeheimen. Datenschutzrechtlich noch bedeutsamer ist die Übermittlung von Auskunftssperren – beispielsweise wegen einer Gefahr für Leben, Gesundheit, persönliche Freiheit usw. oder wegen eines bestehenden Adoptionsverhältnisses – sowie die Übermittlung besonders empfindlicher Daten aus dem Katalog des § 3 MG wie rechtliche Zugehörigkeit zu einer Religionsgesellschaft oder steuerrechtliche Daten.

Die örtlichen Feststellungen ergaben ein sehr uneinheitliches Bild. So verfügt beispielsweise eine Stadt mit sehr großer Einwohnerzahl nur über 52 Terminals außerhalb der Meldebehörde mit Zugriff auf EWOIS; in einer anderen, sehr viel kleineren Stadt sind es nicht weniger als 145 Datenstationen. Konkret bedeutet dies, daß hier mindestens 145 Bedienstete – außerhalb des Meldeamtes (Bürgerbüro) – auf Meldedaten zugreifen können. Die Zugriffsmöglichkeiten sind unterschiedlich ausgestaltet; sie umfassen aber in allen Fällen die Adreßdaten und den Hinweis auf das Vorliegen einer Auskunftssperre, in den Zugriffs-Berechtigungsklassen G, P, I/K, L und D außerdem nähere Hinweise zur Sperrung, also beispielsweise GF (Gefahr für Leben, Gesundheit, persönliche Freiheit), AP (Adoptionspflegeverhältnis) oder TS (Geschlechtsumwandlung nach dem Transsexuellengesetz – vgl. Tz. 4.5 –). Der Wert einer Auskunftssperre wegen einer Gefahr für Leben, Gesundheit usw. ist außerordentlich stark herabgesetzt, wenn so viele Bedienstete von der Existenz einer solchen Situation Kenntnis nehmen können. Es ist deshalb ein Anliegen, das immer wieder hervorgehoben werden muß, daß der Zugang zu solchen Daten so weit wie möglich eingeschränkt wird.

Aufschlußreich waren auch Feststellungen zur Zugriffshäufigkeit. Eine Auswertung der Zugriffsstatistik einer Stadtverwaltung für einen Monat des Jahres 1996 ergab, daß an 43 Terminals keine Einwohnerdaten abgerufen wurden. Bei weiteren 35 Terminals waren im gesamten Monat weniger als 20 Online-Übermittlungen erfolgt. Es gab aber auch gegenteilige Feststellungen: Eine im Jugendamt einer Stadtverwaltung beschäftigte Mitarbeiterin hatte einen wesentlichen Teil ihrer Arbeitszeit damit zugebracht, Meldedaten abzurufen. 1 800 Zugriffe wies die Monatsstatistik aus. Nähere Feststellungen ergaben, daß viele Zugriffe die Daten von Kolleginnen, Kollegen und Dienstvorgesetzten betrafen, zu ihrer eigentlichen Arbeit also keinerlei Bezug hatten.

Die Angemessenheit der automatisierten Datenübermittlung muß insbesondere dort in Frage gestellt werden, wo über einen längeren Zeitraum keine oder nur sehr wenige Abrufe erfolgten. Sicherlich kann eine einmalige geringe Zahl von Abrufen darauf zurückzuführen sein, daß ein Arbeitsplatz über längere Zeit nicht besetzt war. Dennoch: Die Zugriffsstatistiken weisen häufig aus, daß an manchen Arbeitsplätzen kein Erfordernis besteht, auf Meldedaten zuzugreifen. Damit stellt sich aber die Frage, ob die Einrichtung eines automatisierten Übermittlungsverfahrens im Sinne des § 7 LDSG angemessen ist. Die Feststellungen des LfD hatten zur Folge, daß die Zugriffsberechtigungen auf Meldedaten erheblich reduziert wurden.

4.1.2 Anpassung der Auskunftsformate an die Erforderlichkeit zur Aufgabenerfüllung

Eine wesentliche Voraussetzung für die Datenübermittlung – und damit für die Zulässigkeit einer automatisierten Übermittlung von Meldedaten – ist die Erforderlichkeit für die rechtmäßige Aufgabenerfüllung (§ 14 LDSG). Jede Stelle, der ein Online-Abruf ermöglicht wird, sollte nur auf die Meldedaten zugreifen können, die sie zur Erfüllung ihrer Aufgaben benötigt. Auch bei der Realisierung dieser gesetzlichen Forderung bestehen erhebliche Probleme. Ein Amt für Statistik und Wahlen verfügte über drei Bildschirme der Berechtigungsklasse S und damit nicht nur über den Zugang zu Meldedaten, die für die Durchführung von Statistiken und Wahlen erforderlich sein können, sondern auch über Daten aus der Lohnsteuerauskunft (Steuerklasse und Religionszugehörigkeit), der Lohnsteuerarchivauskunft und über Schulanfänger. Das Problem besteht darin, daß es technisch kaum möglich ist, den Zugang zu Meldedaten so zu differenzieren, wie dies aufgrund der Aufgabenzuweisung an die Dienststellen geboten wäre.

Andererseits hindert diese Gliederung nach Berechtigungsklassen, daß einzelnen Ämtern stets die für eine wirtschaftliche Aufgabenerfüllung erforderlichen Daten zur Verfügung gestellt werden. Das Steueramt der Stadt, in der eine Ortskirchensteuer nach dem Grundbesitz erhoben wird, muß beim Eigentumsübergang von Grundstücken in rund tausend Fällen jährlich die Religionszugehörigkeit von Grundstückseigentümern beim Meldeamt erfragen. Es ist anzuerkennen, daß hier die gesetzlichen Voraussetzungen für eine automatisierte Datenübermittlung auch bezüglich des Merkmals Religionszugehörigkeit vorliegen. Würde indessen das Auskunftsformat M 202 in die Berechtigungsklasse D, der das Steueramt angehört, einbezogen, so stünde dieses empfindliche Datum auch Steuerämtern, die außerhalb des Bereichs der Landeskirche liegen, sowie allen sonstigen Stellen mit entsprechender EWOIS-Kennung zur Verfügung, also beispielsweise Liegenschaftsämtern, Stadtkassen oder Rechtsämtern. Dies wiederum wäre weder erforderlich noch angemessen.

Anzustreben wäre insoweit eine an den Zugriffserfordernissen der Dienststellen orientierte dynamische Generierung von Auskunftsformaten. Es bestünde dann die Möglichkeit, den jeweiligen Stellen genau die EWOIS-Daten zur Verfügung zu stellen, die sie zur Erfüllung ihrer Aufgaben benötigen. Eine Lösung könnte darin bestehen, daß die bereits jetzt in der EWOIS-

Anwendung vorhandenen Berechtigungsklassen (A,G/V,P,S,I/K,L,O,Z,D) um weitere Klassen erweitert werden. Damit wäre die Möglichkeit geschaffen, einzelnen Stellen EWOIS-Daten differenzierter zur Verfügung zu stellen. Es wäre danach z. B. möglich, mit einer neuen Benutzerkennung den Steuerämtern, die eine Ortskirchensteuer nach dem Grundbesitz erheben, die Auskunftsformate entsprechend der bereits jetzt vorhandenen Benutzerkennung D, erweitert um das Auskunftsformat M 202, zur Verfügung zu stellen. Eine andere Lösung könnte darin gesehen werden, daß mit einer flächendeckenden Einführung der benutzerorientierten Zugangskontrolle im LDKN die Funktionsgruppensystematik so erweitert wird, daß den Dienststellen nur die für die Aufgabenerfüllung erforderlichen EWOIS-Informationen zugänglich sind.

4.1.3 Stichprobenprüfung/Protokollierung

Nach § 7 Abs. 4 Satz 3 LDSG hat die übermittelnde Stelle zu gewährleisten, daß die Zulässigkeit der Übermittlung personenbezogener Daten zumindest stichprobenweise überprüft werden kann. Dieser gesetzlichen Anforderung an automatisierte Übermittlungsverfahren kann nur durch eine benutzerbezogene Protokollierung von Abrufen entsprochen werden. Es muß – stichprobenweise – nachvollziehbar sein, welche personenbezogenen Daten durch wen abgerufen wurden.

Dieser gesetzlichen Anforderung war für eine Übergangszeit nur in der Weise Rechnung getragen, daß alle Maskenaufrufe im „IMS-Log" aufgezeichnet wurden. Die Aufzeichnungen erfolgten jedoch terminalbezogen und in einer Weise, die Auswertungen zum Zwecke der Datenschutzkontrolle erschwerte. Insbesondere war es dem jeweiligen Meldeamt – als der übermittelnden Stelle – nicht möglich, in angemessener Zeit die Zulässigkeit des automatisierten Übermittlungsverfahrens ohne Hilfe von Dritten (DIZ) zu überprüfen.

Diese unbefriedigende Situation ist grundlegend verändert, nachdem das DIZ eine automatisierte Stichprobenprotokollierung auf der Basis von zehn Prozent der automatisierten Online-Abrufe eingeführt hat. Zwar kann zu Kontrollzwecken noch nicht online auf diese Datei zugegriffen werden; auf Anforderung der aufsichtsführenden Stellen oder der Datenschutzkontrolle ist es indessen verhältnismäßig leicht möglich, die benötigten Daten zur Verfügung zu stellen. Gegenüber der früheren Situation – Auswertung des „IMS-Log" – ist dies ein deutlicher Fortschritt.

4.1.4 Anhörung des Landesbeauftragten für den Datenschutz

§ 7 Abs. 3 LDSG fordert, daß der LfD vor der Einrichtung eines automatisierten Übermittlungsverfahrens zu hören ist. Vereinzelt wird diese Vorschrift beachtet, häufiger aber aus Unkenntnis nicht berücksichtigt.

4.1.5 Unterrichtung der Aufsichtsbehörde und der Meldebehörden

Das Ministerium des Innern und für Sport wurde über die Feststellungen unterrichtet. Es hat die wesentlichen Ergebnisse in einem Rundschreiben vom Januar 1997 an die nachgeordneten Behörden zusammengefaßt. Unabhängig hiervon muß die Behebung von Datenschutzdefiziten bei der inhaltlich-technischen Neugestaltung des Einwohnermeldeverfahrens einen besonderen Schwerpunkt bilden.

4.2 Meldefähige Anschrift für wohnungslose Personen

In der Bundesrepublik Deutschland nimmt die Zahl der Menschen zu, die aus eigener Kraft nicht in der Lage sind, ihre Wohnung zu halten oder nach Verlust des eigenen Wohnraums eine neue Wohnung zu finden. Als eine Maßnahme, die geeignet sein könnte, die sozialen Folgen der Obdachlosigkeit zu mildern, schlug der Ausschuß für Raumordnung, Bauwesen und Städtebau des Deutschen Bundestages vor (Drucksache 13/1848), durch Änderung des Melderechts auch wohnungslosen Personen die Möglichkeit einzuräumen, eine meldefähige Anschrift zu haben, die nicht von vornherein den Status der Wohnungslosigkeit erkennen läßt.

Der Bundesminister des Innern stellte sich in der Diskussion um diese Thematik auf den Standpunkt, daß das Melderecht keinen Beitrag für die Zielsetzung der Initiative leisten könne. Es habe rechtssystematisch betrachtet eine stringent ordnungspolitische Funktion, so daß für die Berücksichtigung sozialpolitischer Belange grundsätzlich kein Raum sei. Die Registrierung einer fiktiven Anschrift im Melderegister begegne auch deshalb Bedenken, weil alleiniges Eintragungskriterium der Bezug einer Wohnung sei. Das Melderegister spiegele ausnahmslos die tatsächlichen Lebensverhältnisse der Einwohner wider.

Der LfD, der vom Ministerium des Innern und für Sport um Stellungnahme gebeten wurde, sah in der ordnungspolitischen Funktion des Melderechts keinen Hinderungsgrund, auch sozialpolitische Zielsetzungen zu verfolgen oder die statistische Erfassung von Obdachlosen zu fördern. Von einer stringent ordnungspolitischen Funktion des Meldewesens kann auch jetzt schon nicht mehr gesprochen werden. Bei der Schaffung meldefähiger Anschriften muß freilich verhindert werden, daß das Recht auf informationelle Selbstbestimmung der wohnungslosen Personen beeinträchtigt wird. Solche Beeinträchtigungen wären zu besorgen, wenn als solche erkennbare fiktive Anschriften ohne Zustimmung der Betroffenen in das Melderegister eingetragen würden. Im übrigen müßten Adressen von Wohnungslosen im Melderegister (Erreichbarkeitsadressen) durch angemessene Auskunftssperren geschützt sein.

Problematisch wären Doppelerfassungen, denn es ist ein Kernanliegen des Datenschutzes, daß im Melderegister nur richtige Daten gespeichert werden. Die Einführung und Überwachung der Meldepflicht für Obdachlose würde einen erheblichen Berichtigungsbedarf und einen kaum zu bewältigenden Nachforschungsaufwand erzeugen. Auch dies muß bei einer Melderechtsänderung mit dem Ziel, meldefähige Anschriften für wohnungslose Personen zu schaffen, bedacht werden.

4.3 Nutzung von Meldedaten für den Rundfunkgebühreneinzug

Rundfunkgebühren werden von der GEZ eingezogen, die hierbei jeweils das Datenschutzrecht des Sitzlandes der Rundfunkanstalt anzuwenden hat. Für Rheinland-Pfalz ist insoweit der Südwestfunk zuständig. Da er seinen Sitz in Baden-Baden hat, gilt das baden-württembergische Landesdatenschutzgesetz (LDSG B-W). Entsprechende Regelungen sind in den §§ 31 und 32 enthalten. Die Aufgabe der datenschutzrechtlichen Kontrolle des Südwestfunks obliegt gem. § 32 Abs. 2 LDSG B-W dem Rundfunkbeauftragten für den Datenschutz.

Die Zulässigkeit der Übermittlung von Meldedaten an die Rundfunkanstalten und die GEZ zum Zwecke des Gebühreneinzugs bestimmt sich nach dem Melderecht des Landes, in dem die um Auskunft ersuchte Meldebehörde ihren Sitz hat. Eine Rechtsgrundlage für die regelmäßige Übermittlung von Meldedaten aus Anlaß der An- und Abmeldung von Einwohnern sowie von Sterbefällen zum Zwecke des Rundfunkgebühreneinzugs besteht in Rheinland-Pfalz nicht (vgl. 13. Tb., Tz. 4.4). Seit der Novellierung der Meldedatenübermittlungsverordnung im September 1994 ist es indessen zulässig, dem Südwestfunk oder der von ihm beauftragten Stelle im Wege des automatisierten Datenabgleichs Einwohnerdaten zur Verfügung zu stellen. Dieser Datenabgleich setzt jedoch voraus, daß der Meldebehörde zunächst ein – inaktueller – Datenbestand zum Zwecke der Berichtigung übermittelt wird. Der Melderegisterabgleich ist damit als Grundlage für die Suche nach unbekannten Gebührenschuldnern weniger geeignet als die von den Rundfunkanstalten angestrebte regelmäßige Übermittlung von Meldedaten in Zuzugs-, Wegzugs- und Todesfällen. Immerhin dürfte die schnelle Information über die aktuelle Adresse in Umzugsfällen für den Gebühreneinzug dienlich sein, und über Sterbefälle würde die GEZ schnell informiert, weil im Rahmen des Abgleichs auch solche Informationen übermittelt werden dürfen. Dennoch wird diese Form der Datenübermittlung nicht praktiziert; die GEZ ist in dieser Sache bisher nicht an die zuständigen Behörden herangetreten.

Eine andere Rechtsgrundlage für die Übermittlung von Meldedaten an die GEZ bietet § 31 MG Rheinland-Pfalz, der die Datenübermittlung an andere Behörden oder sonstige öffentliche Stellen regelt. Wenn die GEZ in Schwerpunktbereichen, die geographisch und altersmäßig abgegrenzt werden können, ihrer nach dem Staatsvertrag bestehenden Befugnis zur Ermittlung unbekannter Gebührenpflichtiger nachkommt, so können hierfür Adreßdaten aus dem Melderegister übermittelt werden. Dies hatte die DSK gegenüber dem Ministerium des Innern und für Sport bereits 1986 vertreten. Daß eine Meldedatenübermittlung auf der Grundlage der gesetzlichen Bestimmungen über die Datenübermittlung an öffentliche Stellen grundsätzlich in Betracht kommt, wurde durch den VGH Mannheim in einem Urteil vom 15. November 1994 – I S 310/94 – für Baden-Württemberg ausdrücklich bestätigt.

Nachdem das Ministerium diese Rechtsauffassung gegenüber dem Südwestfunk bekräftigt hat, ist davon auszugehen, daß die Möglichkeiten der Meldedatenübermittlung auf der Grundlage des § 31 MG in der Zukunft stärker genutzt werden und auf die Schaffung einer speziellen Rechtsgrundlage für regelmäßige Datenübermittlungen an die Rundfunkanstalten in der Meldedatenübermittlungsverordnung weiterhin verzichtet werden kann.

4.4 Erteilung von Melderegisterauskünften durch die Wegzugsbehörde

Nach Nr. 28.1 der VV zur Durchführung des Meldegesetzes darf die für eine frühere Wohnung zuständige Meldebehörde aufgrund eines Auskunftsersuchens nach § 34 MG auch die ihr bekanntgewordene aktuelle Anschrift mitteilen. Nur wenn eine Auskunftssperre nach § 34 Abs. 5 wegen einer Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen eingetragen ist, hat sie das Auskunftsersuchen an die zuständige Behörde weiterzuleiten.

Damit ist eine Ausnahme von dem Grundsatz zugelassen, daß Verwaltungshandlungen von der sachlich und örtlich zuständigen Behörde vorzunehmen sind. Für den Anwendungsbereich von EWOIS ist diese Ausnahme unter Datenschutzgesichtspunkten deshalb vertretbar, weil alle Meldebehörden auf den gleichen, zentral gespeicherten Datensatz zugreifen. Der LfD ging allerdings in der Vergangenheit davon aus, daß die Ausnahmeregelung auf den Anwendungsbereich des Meldegesetzes Rheinland-Pfalz beschränkt sei.

Gelegentlich einer Erörterung von Datenschutzfragen zum Melderecht mit Leitern und Sachbearbeitern von Meldebehörden wurde eine andere Praxis bekannt: Viele Meldebehörden sehen sich nicht gehindert, auch dann Melderegisterauskünfte über die aktuelle Wohnung zu erteilen, wenn ein Einwohner in ein anderes Bundesland verzogen ist. Es wird argumentiert, daß nach § 30 Abs. 3 MG die zuständige Meldebehörde die für die vorherige Wohnung zuständige Meldebehörde in den Fällen des § 34 Abs. 5 und 6 MG zu unterrichten habe; das Vorliegen von Auskunftssperren werde der früher zuständigen Meldebehörde also bekannt und könne von dieser berücksichtigt werden. Diese Argumentation überzeugt nicht, denn nicht alle Länder haben in ihren

Meldegesetzen geregelt, daß Auskunftssperren in die Rückmeldung einzubeziehen sind (beispielsweise Baden-Württemberg, Berlin, Sachsen). § 17 MRRG enthält hierzu auch keine Verpflichtung. Im übrigen ist keineswegs sichergestellt, daß eine Auskunftssperre wegen einer Gefahr für Leben, Gesundheit usw. auch dann noch der Wegzugsbehörde mitgeteilt wird, wenn seit dem Umzug längere Zeit vergangen ist.

Es ist also nicht vollständig auszuschließen, daß eine rheinland-pfälzische Meldebehörde beim Umzug eines Einwohners in ein anderes Bundesland oder in der Zeit danach keine Kenntnis von einer Auskunftssperre nach § 34 Abs. 5 MG erhält, eine Anfrage also nicht an die zuständige Meldebehörde weiterleitet, sondern die Auskunft selbst erteilt und damit die schutzwürdigen Interessen von Betroffenen verletzt. Das Ministerium des Innern und für Sport vertritt indessen die Auffassung, daß regelmäßig auch die für die bisherige Wohnung zuständige Meldebehörde in der Lage ist, eine Auskunft über die aktuelle Anschrift unter Berücksichtigung der Eintragung einer etwaigen Auskunftssperre zu erteilen, da sowohl die für frühere Wohnungen zuständigen als auch die für Nebenwohnungen zuständigen Meldebehörden über die Eintragung einer Auskunftssperre zu unterrichten seien. An der eingeführten Praxis solle festgehalten werden, weil im Falle der Erteilung einer Auskunft durch die bisherige Meldebehörde die verwaltungsaufwendige Weiterleitung eines Auskunftsersuchens an eine andere Meldebehörde vermieden werden könne. Das Ministerium hält es jedoch für klärungsbedürftig, inwieweit die Weiterleitung eines Auskunftsersuchens an die für die jeweilige Hauptwohnung zuständige Meldebehörde zumindest in denjenigen Fällen erforderlich werden kann, in denen Einwohner in eines der oben genannten Länder umziehen, in denen keine Pflicht zur Rückmeldung einer Auskunftssperre besteht.

Bei einem Meinungsaustausch im Unterausschuß „Melde-, Paß- und Personalausweiswesen" der Melderechtsreferenten der Länder habe Einvernehmen darüber erzielt werden können, daß bei Auskunftsersuchen bei der früher zuständigen Meldebehörde grundsätzlich die neue Anschrift mitgeteilt werden darf. Es habe auch Einvernehmen darüber bestanden, daß Einwohner bei Beantragung einer Auskunftssperre darauf hingewiesen werden sollen, zur Gewährleistung eines umfassenden Schutzes auch bei der früher zuständigen Meldebehörde eine Auskunftssperre beantragen zu können. Grundsätzlich könne insoweit den Betroffenen zugemutet werden – bei Vorliegen der Voraussetzungen für eine Auskunftssperre –, sich selbst um einen umfassenden Schutz zu kümmern.

Der LfD hält diese Argumentation nicht für stichhaltig. Es geht nicht darum, was den Betroffenen zugemutet werden kann, sondern um die staatliche Verpflichtung, ein für den Bürger kaum zu durchschauendes staatliches Verwaltungsverfahren so zu organisieren, daß schwerwiegende Beeinträchtigungen schutzwürdiger Belange zuverlässig ausgeschlossen sind. Im übrigen wird dem LfD aus der Praxis berichtet, daß eine Mitteilung von Auskunftssperren außerhalb des Rückmeldeverfahrens nicht stattfindet. Er wird den Vorgang deshalb erneut aufgreifen.

4.5 Meldedaten von Transsexuellen

Im Berichtszeitraum erhielt der LfD zwei Eingaben, die sich auf die Behandlung der Meldedaten von Transsexuellen bezogen. Feststellungen beim DIZ ergaben, daß der aufgrund der Geschlechtsanpassung fortgeschriebene Meldedatensatz mit dem Hinweis „Auskunftssperre" und der Ergänzung „ts" für Transsexuelle unter Verwendung des Auskunftsformats M 201 von allen Meldebehörden, Polizeibehörden, Bußgeldstellen, Kreisverwaltungen (Abfallbeseitigung) und Kfz-Zulassungsstellen abgerufen werden kann. Transsexuelle werden von den Übermittlungsempfängern als solche erkannt, obwohl hierfür unter keinem denkbaren Gesichtspunkt ein Erfordernis besteht. Betroffen sind in Rheinland-Pfalz 25 Personen.

Schon im Jahre 1984 fragte die DSK beim Ministerium des Innern und für Sport an, wie die Einwohnerdaten von Transsexuellen im Melderegister behandelt werden. Sie erhielt die Antwort, daß zur Wahrung des Offenbarungsverbots des § 5 TSG ein neuer Datensatz mit einem neuen Ordnungsmerkmal angelegt werde. Bezüglich des alten Datensatzes werde eine Auskunftssperre mit dem gleichen automationstechnischen Sicherheitsgrad wie im Falle der Inkognito-Adoption angeordnet.

Wie die jetzigen Feststellungen ergaben, ist dies nicht geschehen. Der LfD hat das Ministerium um Stellungnahme gebeten. Bei Redaktionsschluß dieses Berichts war der Vorgang noch nicht abgeschlossen.

4.6 Einwohnerverzeichnisse auf CD-ROM

§ 35 Abs. 4 MG läßt zu, daß an Adreßbuchverlage eine einfache Melderegisterauskunft (Name und Anschrift) über sämtliche Einwohner, die das 18. Lebensjahr vollendet haben, erteilt werden darf. Die Betroffenen können widersprechen; hierauf ist einmal jährlich durch öffentliche Bekanntmachung sowie bei der Anmeldung hinzuweisen.

Die auf dieser gesetzlichen Grundlage beruhende Praxis der Meldebehörden hat in der Vergangenheit wiederholt zu schwerwiegenden datenschutzrechtlichen Verstößen geführt. So wurden im Adreßbuch einer größeren Stadt die Anschriften der Insassen einer Justizvollzugsanstalt abgedruckt; in einer anderen Stadt wurde ein Stadtadreßbuch herausgegeben, in dem auch die Adressen solcher Einwohner enthalten waren, die einer Datenweitergabe widersprochen hatten.

Regelmäßig führt die Herausgabe von Stadtadreßbüchern zu Eingaben an den LfD in erheblicher Zahl. Die Betroffenen beschweren sich, daß sie nicht ausdrücklich um die Einwilligung zur Veröffentlichung gebeten wurden und verweisen auf die Gefährdungen, die insbesondere mit den Straßenverzeichnissen in Stadtadreßbüchern einhergehen. Es ist bekannt, daß Stadtadreßbücher zur Vorbereitung von Straftaten genutzt werden können. (Wo wohnen Alleinstehende?)

In die Diskussion geraten ist neuerlich die Absicht verschiedener größerer Städte, die Herausgabe von Stadtadreßbüchern auf CD-ROM zuzulassen. Das Ministerium des Innern und für Sport hat, einer Empfehlung des LfD folgend, in einem Runderlaß angeordnet, Meldedaten für Stadtadreßbücher nur dann herauszugeben, wenn die Verlage sich verpflichten, keine CD-ROM zu erstellen.

Es besteht freilich das weitere Problem, daß auch in den Stadtadreßbüchern abgedruckte Daten von Dritten gescannt und so für die Erstellung von CD-ROM genutzt werden können. Auf diese Weise können – durch Zusammenfassung von Stadtadreßbüchern – Landesadreßbücher oder sogar Bundesadreßbücher (vergleichbar der Telefon-CD) entstehen. Es ist dann durch Abgleich des Inhalts von CD-ROM beispielsweise möglich festzustellen, wo alleinstehende Personen ohne Telefonanschluß wohnen. Auch andere Auswertungen – z. B. wer wohnt im Villenviertel oder wer ist aufgrund seiner Wohnlage zu den sozialen Randgruppen zu rechnen – werden möglich sein.

Der LfD vertritt die Auffassung, daß die technische Entwicklung eine Änderung der gesetzlichen Bestimmungen über die Verwendung von Meldedaten für die Herausgabe von Adreßbüchern fordert: Die Rechte der Betroffenen müssen gestärkt werden. Dies könnte in der Weise geschehen, daß die Vorschrift über die Datenübermittlung an Adreßbuchverlage (§ 35 Abs. 4 MG) gestrichen würde. Wer die aktuelle Anschrift eines Einwohners in Erfahrung bringen wollte, müßte diese, weil Stadtadreßbücher dann nicht mehr zur Verfügung stünden, bei der Meldebehörde unmittelbar erfragen (einfache Melderegisterauskunft nach § 34 Abs. 1 MG). Angemessen könnte aber auch eine Einwilligungslösung sein, die die bisherige Widerspruchslösung ersetzt. Danach dürften nur die Daten solcher Einwohner, die hiermit nach Aufklärung über die denkbaren weiteren Verwendungsmöglichkeiten einverstanden sind, an Adreßbuchverlage weitergegeben werden. In Nordrhein-Westfalen wurde eine solche Einwilligungslösung durch Gesetzesänderung mit Wirkung vom 1. Januar 1999 eingeführt.

4.7 Alters- und Ehejubiläen

4.7.1 Was ist ein Jubiläum?

Ein Mitglied des Deutschen Bundestages erbat von einer Verbandsgemeinde Auskünfte aus dem Melderegister, die ihn in die Lage versetzen sollten, älteren Mitbürgerinnen und Mitbürgern zu ihren Geburtstagen zu gratulieren. Konkret ging es um die Wohnanschriften und Geburtsdaten von Einwohnern, die das 65. Lebensjahr vollendet hatten. Damit entstehe, so meinte er, „auch ein Stück Nähe zwischen den Politikern und den Menschen, die durch sie vertreten werden".

Dies ist sicherlich zutreffend, und § 35 Abs. 3 des MG läßt auch zu, daß für Gratulationszwecke Daten über Alters- und Ehejubiläen (Vor- und Familiennamen, Doktorgrade, Anschriften sowie Tag und Art des Jubiläums) übermittelt werden. Voraussetzung ist allerdings, daß die Betroffenen, also die Jubilare, der Auskunftserteilung nicht widersprochen haben.

Dennoch konnte dem Wunsch des Abgeordneten nicht vollständig entsprochen werden, denn nicht jeder Geburtstag ab der Vollendung des 65. Lebensjahres stellt ein Altersjubiläum im Sinne des Meldegesetzes dar. § 8 Abs. 1 MeldDÜVO ist zu entnehmen, daß erst ab der Vollendung des 70. Lebensjahres von einem Altersjubiläum gesprochen werden kann; allgemein üblich ist, daß danach nur im Zeitabstand von fünf Jahren erneut Jubiläumsdaten übermittelt werden. Die Übermittlung von Daten schon ab dem 65. Lebensjahr ist durch § 35 Abs. 3 MG nicht gedeckt.

Bezüglich der Ehejubiläen besteht Unklarheit: Nummer 29.4 der Verwaltungsvorschrift des Ministeriums des Innern und für Sport zur Durchführung des Meldegesetzes zählt hierzu bereits das Silberne Ehejubiläum; § 8 der MeldDÜVO nennt das Fest der Goldenen Hochzeit. Der LfD erhebt gegen die Übermittlung von Daten zur Silbernen Hochzeit keine Bedenken, empfiehlt aber eine Angleichung der Bestimmungen.

4.7.2 Dürfen Jubiläumsdaten für Werbezwecke übermittelt werden?

Übermittlungsempfänger von Alters- und Ehejubiläumsdaten können nicht nur Bundestagsabgeordnete und andere Repräsentanten von Staat und Gemeinden sein. Das Meldegesetz formuliert in § 35 Abs. 3: „Begehrt jemand eine Auskunft . . ." und meint damit einen weiten Kreis von Auskunftsempfängern, also Privatpersonen, aber auch die Presse oder andere Medien, die über ein Jubiläum berichten wollen.

Anfragen an den LfD zur Zulässigkeit einer Übermittlung von Jubiläumsdaten beziehen sich bisweilen auf deren Nutzung für kommerzielle Zwecke. Insbesondere die Produktwerbung steht hier im Vordergrund.

Im Rahmen der datenschutzrechtlichen Beurteilung ist zu berücksichtigen, daß § 35 Abs. 3 MG keine Verpflichtung zur Übermittlung von Jubiläumsdaten, sondern eine Befugnis begründet. Auch wenn dies aus dem Wortlaut der Vorschrift nicht in der gebotenen Deutlichkeit zu entnehmen ist, so ist doch ergänzend eine Abwägung zwischen dem Übermittlungsinteresse – kommerzielle Nutzung der Daten – und einer möglichen Beeinträchtigung der schutzwürdigen Belange Betroffener vorzunehmen (§ 7 MG). Zu berücksichtigen ist ferner, daß das Meldegesetz auch in anderen Vorschriften kommerzielle Interessen als Übermittlungsgrund nicht gelten läßt (§ 34 Abs. 3).

5. Polizei

5.1 Europol

Nach der im Bundestag zur Zustimmung anstehenden Europol-Konvention („Übereinkommen aufgrund von Artikel K.3 des Vertrags über die Europäische Union über die Errichtung eines Europäischen Polizeiamts – Europol-Übereinkommen") wird Europol zunächst auf den Gebieten des illegalen Drogenhandels, des illegalen Handels mit nuklearen und radioaktiven Substanzen, der Schleuserkriminalität, Menschenhandel und Kraftfahrzeugkriminalität tätig (Art. 2 Abs. 1 und 2). Beabsichtigt ist aufgrund einer Ministervereinbarung auch die Erweiterung auf die Bekämpfung des Mißbrauchs von Kindern sowie der Geldwäsche in den genannten Bereichen. Später werden noch Straftaten terroristischen Charakters bearbeitet (Art. 2 Ziff. 2 Satz 2).

Europol wird die Ermittlung und Fahndung durch die Polizeien der Mitgliedstaaten unterstützen und hierfür zur Erstellung von Lagebildern Informationen auswerten und bewerten („Intelligence"-Arbeit) sowie Präventionsstrategien entwickeln.

Hierfür werden Durchführungsbestimmungen und Dateienrichtlinien erlassen, von denen insbesondere die Durchführungsbestimmungen über Analysedateien aus der Sicht des Datenschutzes von Bedeutung sind (Art. 10 der Europol-Konvention); sie finden ihre Entsprechung in § 4 des Gesetzentwurfs der Bundesregierung zur Ratifizierung der Konvention, demzufolge das BKA zur Analyse Daten übermittelt, die von ihm zu Zwecken der Verhütung oder Verfolgung von Straftaten gespeichert sind.

In den Analysedateien kann Europol im Rahmen seiner Aufgabenstellung die für die jeweils spezifischen Analysezwecke erforderlichen Daten speichern, ändern und nutzen. Dabei geht es um einen erweiterten Kreis von Betroffenen, nämlich um Personen, die bei Ermittlungen der betreffenden Straftaten oder bei einer künftigen Strafverfolgung in Betracht kommen, potentielle Opfer, Kontakt- und Begleitpersonen sowie um Personen, die Informationen über die betreffende Straftat liefern können.

Analysedateien werden nicht auf Dauer, sondern fallweise auf Initiative von Mitgliedstaaten bei Vorliegen verschiedener Voraussetzungen eingerichtet. Das Instrument ist in Deutschland noch nicht sehr bekannt, wird aber in anderen Mitgliedstaaten der EU, z. B. in Großbritannien, bereits verwendet. Aufgrund vorab gebildeter Hypothesen über vorstellbare kriminelle Abläufe werden durch Integration der vorhandenen Informationen Zusammenhänge durch graphische Aufbereitung sichtbar.

Analysen werden nicht auf eigene Initiative von Europol durchgeführt; sie werden jeweils für bestimmte Analyseprojekte erstellt. Die Dateien werden gegenüber anderen Dateien, auch gegenüber anderen Analysedateien, abgeschottet. Die weitere Speicherung der Daten nach Abschluß der Analyse bedarf jeweils einer neuen Projektvereinbarung.

Die aus der Sicht des Datenschutzes in der Diskussion problematisierte Verarbeitung von Daten über die rassische Herkunft, religiöse oder andere Überzeugungen, politische Anschauungen, das Sexualleben oder die Gesundheit in Analysedateien ist nach massiven Interventionen größtenteils entschärft worden; ihre Verwendung muß in jeder einzelnen Errichtungsanordnung für eine Analysedatei als „unbedingt erforderlich" gesondert spezifiziert werden; sie darf nur auf ausdrücklichen Antrag von zwei oder mehr an der Analyse beteiligten Mitgliedstaaten erfolgen. Außerdem bedürfen die einzelnen Errichtungsanordnungen der Zustimmung des Europol-Verwaltungsrates (mit 2/3-Mehrheit), der seinerseits „alle diesbezüglichen Bemerkungen der gemeinsamen Kontrollinstanz berücksichtigt". Dieses Gremium setzt sich aus Vertretern aller Mitgliedstaaten zusammen; für Deutschland sind dies parlamentarisch kontrollierbare Ministerialbeamte. Schließlich liefern die Mitgliedstaaten die Daten nach eigenem Recht an.

Die vielfach, zunächst auch vom LfD angesprochene Gefahr, daß die geplante Analysetätigkeit als selbständiger Verarbeitungszweck für eine Vielzahl von Dateien gesehen wird, der neben die klassischen polizeilichen Aufgabengebiete der Gefahrenabwehr und Strafverfolgung tritt, ist damit jedenfalls deutlich verringert. Die Geeignetheit dieser neuen kriminalistischen Arbeitsmethode kann sich erst in der Praxis erweisen. Auch dann wird sich erst beurteilen lassen, ob die damit verbundenen Eingriffe in Bürgerrechte verhältnismäßig sind.

Aus der Sicht des Datenschutzes bleibt insoweit mindestens zu fordern, daß in der Praxis die Ziele der einzelnen Analyseprojekte in den Projektvereinbarungen und in den entsprechenden Vorgaben in den Errichtungsanordnungen möglichst eindeutig festgelegt werden.

Weitere Durchführungsbestimmungen für die Übermittlung von Informationen durch Europol an Drittstaaten und Drittstellen sowie über die Entgegennahme der von diesen an Europol gelieferten Informationen liegen im Entwurf vor. Der LfD hat gegenüber dem Ministerium des Innern und für Sport gefordert, daß auch hier die Übermittlung und Entgegennahme der besonders sensitiven Daten über rassische Herkunft u. a. nicht nur von der Bindung an den Übermittlungszweck abhängig gemacht wird, sondern daß auch hier geprüft und festgehalten wird, weshalb die Übermittlung auch dieser Daten jeweils für unbedingt erforderlich angesehen wird.

5.2 Gesetz über das Bundeskriminalamt

Am 1. August 1997 ist das „Gesetz über das Bundeskriminalamt und die Zusammenarbeit der Länder in kriminalpolizeilichen Angelegenheiten" (Bundeskriminalamtgesetz) in Kraft getreten. Der LfD hat zu den einzelnen Regelungen des Entwurfs mehrfach Stellung genommen (siehe auch 15. Tb. Tz. 5.2). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte in einer Entschließung vom März 1995 (abgedruckt als Anlage 18 zum 15. Tb.) auf die Defizite aus der Sicht des Datenschutzes hingewiesen.

Insgesamt ist es zu begrüßen, daß die seit langem überfälligen Regelungen zur bundesweiten polizeilichen Datenverarbeitung besonders im polizeilichen Informationssystem INPOL jetzt zur Verfügung stehen. Verglichen mit den Vorentwürfen enthält das Gesetz auch aus der Sicht des Datenschutzes gewisse Verbesserungen. So wurde in § 8 Abs. 4 auch für die Speicherung personenbezogener Daten von Hinweisgebern und Auskunftspersonen das Einwilligungserfordernis eingeführt, gleichzeitig aber auch eine sehr allgemein formulierte Ausnahmemöglichkeit hiervon für die genannten Personengruppen und auch für Zeugen und mögliche Opfer geschaffen.

Ebenso wurde die Kontrollzuständigkeit der Landesbeauftragten für den Datenschutz in § 12 Abs. 3 klargestellt. Allerdings fehlt in der nunmehr gewählten Fassung der Hinweis, daß der BfD und die LfD nach Maßgabe der jeweiligen Datenschutzgesetze des Bundes und der Länder kontrollieren. Gerade dies wäre an dieser Stelle hilfreich gewesen.

Auch wurden in § 16 Abs. 2 bis 5 Anordnungsvorbehalte beim Einsatz technischer Mittel zur Eigensicherung von nicht offen ermittelnden Bediensteten (Aufnahme des innerhalb oder außerhalb einer Wohnung nicht öffentlich gesprochenen Wortes) eingeführt und gleichzeitig an dieser Stelle Löschungs- und Benachrichtigungspflichten geregelt.

Weiterhin wurde hinsichtlich der „Besonderen Mittel der Datenerhebung" in § 23 Abs. 2 Ziff. 2 klargestellt, daß deren Einsatz in einer für den Betroffenen nicht erkennbaren Weise für Bild- und Tonaufnahmen nur außerhalb von Wohnungen gilt.

Schließlich wurde bei der Verarbeitung und Nutzung personenbezogener Daten für die wissenschaftliche Forschung (§ 29) in teilweiser Anlehnung an die Regelung des § 42 Abs. 2 BZRG eine Interessenabwägung vorgeschrieben, die sich am öffentlichen Interesse am einzelnen Forschungsvorhaben im Verhältnis zu den schutzwürdigen Interessen der Betroffenen orientiert und gleichzeitig die Veröffentlichung übermittelter personenbezogener Daten von der Zustimmung des BKA abhängig macht.

Diese Verbesserungen werden ausdrücklich begrüßt.

Kritisch bleibt anzumerken, daß die Befugnisse des BKA als Zentralstelle zur selbständigen Datenerhebung (§ 7) und -übermittlung nach wie vor sehr weit gehen, ohne den Verantwortungsbereich der Länderpolizeien angemessen zu berücksichtigen.

Datenschutzrechtlich defizitär ist es auch, daß z. B. in den §§ 8 und 14 nach wie vor das zu unbestimmte Merkmal „Straftaten von erheblicher Bedeutung" verwendet wird, obwohl man in § 16 Abs. 3 auf die Katalogstraftaten des § 100 a StPO zurückgreift.

5.3 Novellierung des Polizei- und Ordnungsbehördengesetzes

Bereits seit dem 14. Tb. muß wiederholt die Notwendigkeit ergänzender Regelungen im POG angesprochen werden (14. Tb. Tz. 5.13 und 15. Tb. Tz. 5.4). Die schon in den genannten Berichten dargestellten Defizite sind nach wie vor aktuell, wie sich auch bei den örtlichen Feststellungen in der Berichtszeit verstärkt bestätigt hat.

Es stellt sich aber die Frage, ob eine vollkommene Neufassung der Informationsbestimmungen des Polizei- und Ordnungsbehördengesetzes mit einer völlig anderen Systematik tatsächlich geboten ist. Die allgemeine Grundregelung in § 25 a POG hat sich in der Praxis in ihrer Grundanlage als wirksam im Sinne des Datenschutzes gezeigt und bewährt; sie hat auch für sich, daß sie bei den Anwendern innerhalb und außerhalb der Polizei und der allgemeinen Ordnungsbehörden bekannt ist und gut verstanden wird. Die Informationsverarbeitung durch die Polizei des Landes hat sich auf dieser Basis auch im Vergleich zu anderen Polizeien unter Wahrung der Persönlichkeitsrechte der Bürger insgesamt zufriedenstellend entwickelt. Es ist nicht auszuschließen, daß ein im System weitgehend verändertes und damit zwangsläufig wesentlich komplizierteres Geflecht von Vorschriften in der Praxis zumindest in einer längerandauernden Übergangsphase zu Unsicherheiten und damit zu Zeit- und Effizienzverlusten führt, die sich nicht zuletzt zu Lasten der Sicherheitsinteressen der Allgemeinheit auswirken.

Es wäre deshalb durchaus der Überlegung wert, ob es nicht ausreicht, wenn unter Beibehaltung der bestehenden Systematik, insbesondere der Grundnorm des § 25 a, in ihrer Struktur diejenigen Regeln normenklar und möglichst kurz eingefügt werden, die in der Praxis derzeit nur durch Interpretation gewonnen werden können. Dies könnte auch zu einem rascheren Ergebnis führen.

So könnten schon in § 25 a geregelt werden:

- die Datenverarbeitung zur Vorbereitung von Hilfeleistung und des Handelns in Gefahrenfällen,
- der Abgleich von Daten, die die Polizei bei ihrer rechtmäßigen Aufgabenerfüllung erlangt hat, mit dem Fahndungsbestand sowie
- die Übermittlung vorhandener Daten an die allgemeinen Ordnungsbehörden zur konkreten Gefahrenabwehr, soweit es für deren Aufgabenerfüllung erforderlich ist (i. d. R. Erkenntnisanfragen bei Zuverlässigkeitsprüfungen).

5.4 Nutzung von Protokolldaten zur Strafverfolgung

Aufgrund des Beschlusses eines Amtsgerichts aus Baden-Württemberg in einer Vergewaltigungs- und Raubsache wurde es erforderlich, Logbänder über Terminals der hiesigen Polizei dahin zu überprüfen, ob das zur Tat benutzte und dann gewaltsam entwendete Fahrzeug in der fraglichen Zeit abgefragt wurde.

Der Wortlaut des anzuwendenden § 13 Abs. 5 LDSG läßt die Nutzung für andere als Protokollzwecke zu, soweit „dies zur Abwehr erheblicher Gefährdungen der öffentlichen Sicherheit, insbesondere für Leben, Gesundheit oder Freiheit erforderlich ist". § 98 c StPO läßt Datenabgleiche zur Strafverfolgung mit Polizeidaten zwar generell zu, läßt aber ausdrücklich „entgegenstehende landesgesetzliche Verwendungsregelungen" unberührt. Deshalb kommt es trotz kompetenzmäßig bundesgesetzlicher Regelung auf die Anwendbarkeit des § 13 Abs. 5 LDSG an.

Bereits die ehemalige DSK hatte gegen die Verwendung von Protokolldaten in gravierenden Fällen sowohl zur Gefahrenabwehr wie auch zur Strafverfolgung keine Bedenken erhoben. Grundsätzlich wird das auch vom Bundesgesetzgeber für den hier in Frage stehenden Bereich der Strafverfolgung so gesehen. Dies war bei Abfassung des LDSG auch beabsichtigt.

Dementsprechend kamen Vertreter des Ministeriums des Innern und für Sport und des LfD nach Prüfung überein, daß die in § 13 Abs. 5 LDSG zugelassene Auswertung von Logbanddaten für Zwecke der Abwehr erheblicher Gefährdungen der öffentlichen Sicherheit auch den Schutz der Integrität der Rechtsordnung umfaßt und damit Logbandauswertungen zur Aufklärung erheblicher Straftaten ermöglicht.

Entsprechende Anträge zur Logbandauswertung zu primär repressiven Zwecken legen die sachbearbeitenden Polizeidienststellen zunächst unmittelbar den zuständigen sachleitenden Staatsanwaltschaften vor. Diese ersuchen unter Berücksichtigung der entsprechenden strafprozessualen Anordnungskompetenzen unmittelbar das LKA um Auftragsweiterleitung an das DIZ. Auf Wunsch des LfD hat das Justizministerium mitgeteilt, daß in diesen Fällen die zuständigen Staatsanwaltschaften nach Beendigung der Maßnahme ihn hierüber informieren werden.

Die Kommission beim Landesbeauftragten für den Datenschutz hat das Thema beraten und im Grundsatz den entsprechenden Auswertungen zugestimmt.

Soll durch eine Logbandauswertung festgestellt werden, ob aus polizeilichen Systemen von einem bestimmten Beamten unberechtigte Abfragen getätigt wurden, handelt es sich unabhängig von der evtl. damit zusammenhängenden Strafverfolgung in erster Linie um eine Maßnahme der Datenschutzkontrolle. Diese Nutzung ist damit auch nach dem bloßen Wortlaut von § 13 Abs. 5 LDSG zweckgerichtet.

5.5 Personenbezogene Auswertung der polizeilichen Kriminalstatistik

Die Datei „Polizeiliche Kriminalstatistik – echte Tatverdächtigenzählung" (PKS) wurde bereits im Jahre 1982 bei der DSK angemeldet. Nach ihrer Errichtungsanordnung dient sie dem Zweck der Zuordnung von Straftaten zu einer Person und damit der Beobachtung der Kriminalität. Die Personalien selbst sind Bestandteil der KpS und unterliegen den KpS-Richtlinien. Trotz Verwendung des Wortes „Statistik", was im Grundsatz die Beachtung der Geheimhaltungsbestimmungen des Bundesstatistikgesetzes nahelegen würde, ist zumindest fallweise davon auszugehen, daß der eigentliche Zweck der Speicherung personenbezogener Daten in dieser Datei darin besteht, Kriminalität zu beobachten. Dies geschieht wiederum nicht wertfrei, sondern mit dem Ziel, konkrete und wirksame Maßnahmen zu deren Bekämpfung zu ermöglichen. Dabei ist nicht auszuschließen, daß hierzu je nach Lage der Dinge einzelne Strafverfolgungsmaßnahmen gehören. Bei dieser Annahme handelt es sich bei den in der Datei gespeicherten Daten um solche, die zu Zwecken der Strafverfolgung gespeichert sind, so daß je nach Fallgestaltung die Voraussetzungen des § 98 c StPO als erfüllt gelten können.

Im Berichtszeitraum hat der LfD auf zwei Anfragen hin (Aufklärung von Brandstiftungen in Kindergärten und in einem Mordfall) der Nutzung zur konkreten Strafverfolgung zugestimmt.

Unabhängig davon besteht jedoch Änderungsbedarf für die Errichtungsanordnung, weil nach § 7 Abs. 2 des Landesstatistikgesetzes eine gesetzliche Grundlage erforderlich ist, wenn durch Landesstatistiken in Grundrechte eingegriffen wird. Bis zur letzten Novellierung des Polizeiverwaltungsgesetzes bestand diese Ermächtigung in dessen § 89 Abs. 1 Ziff. 3. Es könnte zweifelhaft sein, ob die nunmehr in § 79 Abs. 1 Satz 2 POG enthaltene Befugnis des LKA zur Informationssammlung „für die vorbeugende Bekämpfung und die Verfolgung von Straftaten" nach der Zweckdefinition der Errichtungsanordnung für die PKS-Datei ausreicht. Durch eine Neuformulierung der Zweckdefinition könnten die Zweifel ausgeräumt werden. Die Erörterungen mit dem Ministerium dazu dauern noch an.

5.6 Richtlinien über die Führung von Kriminalakten überarbeitungsbedürftig

Die z. Z. in Kraft befindlichen „Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien)" stammen aus dem Jahre 1982. Sie sind damit älter als die den gleichen Sachverhalt regelnden Bestimmungen der §§ 25 a bis g POG über die Informationsverarbeitung durch die Polizei. Durch diese Normierungen sind die KpS-Richtlinien zu großen Teilen überholt. Außerdem sind in der Zwischenzeit verschiedene einschlägige Regelungen zu den Richtlinien durch Rundschreiben getroffen worden. Schließlich wurden durch Praxis und Rechtsprechung in den vergangenen 15 Jahren verschiedene Sachverhalte geregelt, die mit dem Anwendungsbereich der Richtlinien eng zusammenhängen. Andere Sachverhalte sind teilweise in den Richtlinien und teilweise in anderen schriftlichen Anordnungen mit Allgemeincharakter enthalten.

Werden beispielsweise Kriminalakten von einer Polizeidienststelle angelegt, in deren örtlichem Bereich der Betroffene zwar seinen Wohnsitz hat, aber für eine andere Behörde vernommen wird, die ein Ermittlungsverfahren gegen ihn führt, dann können hier wie dort über ihn Kriminalakten bestehen. Die Richtlinien gehen zwar eindeutig von der Zulässigkeit auch der Aktenführung durch die Wohnsitzbehörde aus, es fehlen aber spezifische Regelungen, die gerade dieser eingriffsintensiveren Situation Rechnung tragen. Zwischenzeitlich liegt ein Rundschreiben vor, das diesen einen Punkt regelt.

Dies alles zeigt, daß eine umfassende und baldige Überarbeitung der Richtlinien dringend geboten ist. Unübersichtlichkeit und Unklarheit über die Rechtslage im Bereich der Informationsverarbeitung geht nämlich häufig zu Lasten des informationellen Selbstbestimmungsrechts der Bürger.

5.7 Kein Täterschutz durch die Aussonderungsregeln für Altkriminalakten

Die für die Aufbewahrung polizeilicher Unterlagen anzuwendenden Polizeigesetze der Länder einschließlich des rheinland-pfälzischen Polizei- und Ordnungsbehördengesetzes sehen nicht vor, daß die Polizei Akten über Personen nach Ablauf bestimmter Aufbewahrungsfristen vernichten muß; sie kann vielmehr die Daten solange speichern, wie es für die Erfüllung ihrer Aufgaben im Einzelfall erforderlich ist. Dies hat sie allerdings jeweils innerhalb bestimmter Fristen zu prüfen. Der Resozialisierungsgedanke gebietet, daß nicht mehr erforderliche Unterlagen vernichtet werden. Gerade bei besonders schweren Delikten kann die Polizei Aussonderungsprüfungen festlegen, die über die Regelfristen hinausgehen. Auch nach deren Ablauf zwingt also der Datenschutz nicht zur Vernichtung der Unterlagen, wenn von der Polizei zu beurteilende fachliche Gesichtspunkte eine weitere Aufbewahrung gebieten. Dies sind beispielsweise die Art und Weise der Tat, die Persönlichkeit des Täters oder generelle kriminalistische Erfahrungen. Jeder Datenschutzbeauftragte ist sich bewußt, daß diese „Kriminalprognose" schwierig ist und daß sie sich nachträglich als falsch herausstellen kann. Dem hat der LfD bei seinen Überprüfungen „vor Ort" jederzeit Rechnung getragen.

Um so mehr verwunderte es, daß gerade der Landesverband Rheinland-Pfalz einer Vereinigung von Kriminalbeamten zwei übrigens ungeeignete Fälle zum Anlaß einer Presseerklärung mit unbegründeter Kritik am Datenschutz nahm. So wie im Ablauf dort dargestellt, ergeben sich in beiden Fällen Anwendungsfehler, die nicht dem Datenschutz angelastet werden können. Der erste Fall, der übrigens keine rheinland-pfälzische Polizeidienststelle betrifft, handelt von den nicht mehr vorhandenen Akten über den späteren Sexualmörder des Kindes Kim Kerkow. Die für die Kriminalaktenführung einschlägigen Richtlinien, die auch in Rheinland-Pfalz gelten, lassen nämlich eine über die zehn Jahre hinausgehende Aufbewahrung von Unterlagen in solchen Fällen zu, in denen dies „wegen Art und Ausführung der Tat erforderlich" ist. Bei einer vergleichbaren Vortat wäre dies – soweit von hier erkennbar – ohne weiteres geboten gewesen.

Zwischenzeitlich hat das Ministerium des Innern und für Sport bei Sexualstraftätern die Prüf- und Regelaussonderungsfrist auf frühestens 15 Jahre nach Entlassung aus der Strafhaft oder nach Beendigung einer mit Freiheitsentziehung verbundenen Maßnahme der Besserung und Sicherung festgelegt.

In dem Fall eines 17jährigen Polizistenmörders war bemängelt worden, daß er nach Verbüßung einer zehnjährigen Haft „im elektronischen Kriminalaktenbestand nicht mehr als Mörder erkennbar" war, allerdings dann weiter als Straftäter in Erscheinung trat.

Die genannten Richtlinien bestimmen, daß kriminalpolizeiliche Unterlagen nicht vor Ablauf von zehn Jahren nach der Entlassung aus der Justizvollzugsanstalt ausgesondert werden dürfen. Die Akten hätten also bei richtiger Anwendung der Bestimmung noch vorhanden sein müssen, insgesamt 20 Jahre oder sogar noch länger, wenn zwischenzeitlich neue Delikte hinzukamen.

Der LfD hatte hierzu erklärt:

„Nicht ein überzogener Datenschutz, sondern unsachgemäße Aktenbehandlung im Einzelfall sabotieren Täterermittlungen. Wer sich offenbar ohne jede Kenntnis der Rechtslage dazu hinreißen läßt, die Reduzierung des Persönlichkeitsschutzes der Bürger zu fordern, tut unserem freiheitlichen Rechtsstaat einen Bärendienst."

5.8 Automatisches Fingerabdruckidentifizierungssystem des BKA (AFIS)

Nach dem Asylverfahrensgesetz sind grundsätzlich alle Asylbewerber erkennungsdienstlich zu behandeln. Dazu gehört auch die Abnahme der Fingerabdrücke als sicheres Mittel zur Identifizierung der Betroffenen; sie werden von der Polizei abgenommen sowie vom BKA gespeichert und unter den gesetzlich bestimmten Voraussetzungen mit anderen Fingerabdrücken verglichen. Die Abfrage im dortigen Bestand erfolgt durch das LKA. Dorthin wenden sich die sachbearbeitenden Polizeidienststellen, wenn eine aufgefundene Spur abzugleichen ist.

Nach § 16 Abs. 5 AsylVfG ist ein Abgleich von Spuren im sog. Asylbestand zur Zuordnung von Beweismitteln nur zulässig, wenn bestimmte Voraussetzungen die Annahme begründen, daß dies zur Aufklärung einer Straftat führen wird oder wenn es zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist.

Wie schon im 15. Tb. (Tz. 5.18) dargestellt, werden auf Anregung des LfD in Rheinland-Pfalz die Untersuchungsanträge der Polizeidienststellen im LKA zu Prüfzwecken befristet aufbewahrt. Gleichzeitig wird der Grund für die Annahme, daß eine bestimmte Spur auch im Asylbestand zu finden sein könnte, vom jeweiligen Sachbearbeiter in Kurzform aktenkundig gemacht.

Bei allen örtlichen Feststellungen bei Stellen der Kriminalpolizei wurde die Einhaltung dieser Regelung überprüft und ggf. angemahnt. Es hat sich jedoch gezeigt, daß ganz überwiegend richtig verfahren wird und daß die festgehaltenen Gründe die Recherche auch im Asylbestand rechtfertigten. Die Anzahl dieser Untersuchungsanträge hält sich in Grenzen und läßt keinen Schluß auf einen unverhältnismäßigen Gebrauch zu.

Zu bemängeln ist, daß nunmehr schon über mehrere Jahre AFIS ohne gültige Errichtungsanordnung vom BKA betrieben wird. Diese müßte zumindest eine klare Regelung über die fallbezogene Protokollierung solcher Anfragen enthalten, die Recherchen nach § 16 Abs. 5 AsylVfG und solche im Bestand nach § 78 Abs. 3 AuslG zum Gegenstand haben. Zu diesem Zweck muß auch die eindeutige Trennung der Aufbewahrung der verschiedenen Bestände, wie sie gesetzlich vorgesehen ist, in der Errichtungsanordnung zum Ausdruck kommen.

5.9 Regelungen über die Zusammenarbeit der Polizei- und Zollbehörden in den Grenzgebieten

Über die Zusammenarbeit mit den französischen Polizeibehörden und die aus der Sicht des LfD hierfür bestehenden datenschutzrechtlichen Grundlagen wurde bereits im 15. Tb. (Tz. 5.3) berichtet. In der Berichtsperiode wurde ein umfangreicher Entwurfstext ausgearbeitet, der die Zusammenarbeit der Behörden und Dienststellen mit polizei-, grenzpolizei-, bahnpolizei- und zollrechtlichen Aufgaben in den Grenzgebieten im Einvernehmen mit den Ländern Baden-Württemberg, Rheinland-Pfalz und dem Saarland regelt. Im Blick auf das Schengener Durchführungsübereinkommen, insbesondere seinen Artikel 39 und hierzu erlassenen Ausführungsregelungen, soll der illegalen Zuwanderung und grenzüberschreitenden Kriminalität entgegengewirkt sowie die öffentliche Sicherheit und Ordnung durch Abwehr grenzüberschreitender Gefahren und Störungen gewährleistet werden.

In Rheinland-Pfalz sind die Polizeibezirke der Polizeipräsidien Rheinpfalz und Westpfalz in die Zusammenarbeit einbezogen sowie das LKA.

Ein Kernstück des Abkommens wird die Zusammenarbeit in gemeinsamen Zentren für den Informationsaustausch sein.

Der LfD wurde in jeder Phase der Vorbereitungen beteiligt und hat auf der Basis der vorhandenen und im 15. Tb. bereits dargestellten Rechtsauffassung verschiedene Anregungen gegeben. Die gefundenen Regelungen halten sich im Rahmen des geltenden Rechts.

Bereits in Kraft befindet sich eine Vereinbarung zwischen dem Bundesminister des Innern und dem Justizminister des Großherzogtums Luxemburg. In Vorbereitung sind ebenfalls entsprechende Vereinbarungen mit dem Königreich Belgien und der Schweizerischen Eidgenossenschaft. Der LfD wird beteiligt.

5.10 Kann die Polizei Daten aus einer Datei des Bundesgrenzschutzes nutzen?

Aufgrund der Anfrage eines Polizeipräsidiums beim Ministerium des Innern und für Sport war auch vom LfD zu prüfen, ob und unter welchen Voraussetzungen Ersuchen um Übermittlung von Daten aus der Datei „Geschützter Grenzfahndungsbestand" des Bundesgrenzschutzes an die Grenzschutzdirektion in Koblenz gerichtet werden dürfen.

Der Grund ist, daß innerhalb der Datenfelder bestimmte Inhalte gespeichert sind, die sich aus den Angaben in INPOL/POLIS nicht ergeben.

§ 32 Abs. 1 BGSG läßt Datenübermittlungen vom BGS an Behörden des Polizeivollzugsdienstes der Länder ausdrücklich zu, soweit dies zur Erfüllung polizeilicher Aufgaben erforderlich ist. Die damit korrespondierende landesrechtliche Erhebungsnorm ist § 25 a POG. Für die Strafverfolgung finden die einschlägigen Bestimmungen der Strafprozeßordnung Anwendung. Von daher bestehen im Grundsatz keine Bedenken aus der Sicht des Datenschutzes gegen Anfragen seitens der Polizei des Landes in konkreten Einzelfällen.

Auf Anregung des LfD wurde abgeklärt, inwieweit die in § 32 Abs. 2 Satz 1 BGSG vorgesehene Protokollierung der Übermittlungen beim BGS auch für die Datenschutzkontrolle durch rheinland-pfälzische Polizeibehörden und den LfD nutzbar ist. Beim BGS werden über jeden Übermittlungsfall alle für eine Nachprüfung erforderlichen Daten einschließlich des Anlasses in einer Nachweisung festgehalten. Nach Mitteilung der Grenzschutzdirektion an das Ministerium sind auf Grundlage konkreter personenbezogener Daten Einsichtnahmen auch durch den LfD natürlich realisierbar.

Für die Kontrollbedürfnisse des LfD erscheint dies als ausreichend. Eine zusätzliche Protokollierung auf der Erhebungsseite (anfragende Polizeibehörde) erscheint damit entbehrlich, zumal dabei größtenteils die gleichen Daten festgehalten werden und damit eine Doppelspeicherung erfolgen würde.

5.11 Ermächtigung zur Abfrage im Ausländerzentralregister

Abfragen durch die Polizei im AZR sind relativ häufig. Bei einem Polizeipräsidium wurden ca. zehn Abfragen täglich festgestellt; die Abrufe erfolgen im automatisierten Verfahren.

Ermächtigungsgrundlage hierfür ist § 22 Abs. 1 Ziff. 4 AZRG. Nach Absatz 3 der genannten Vorschrift trägt die abrufende Stelle die Verantwortung für die Zulässigkeit des einzelnen Abrufs. An gleicher Stelle ist vorgeschrieben, daß die Abrufe nur von Bediensteten vorgenommen werden dürfen, die vom Leiter der Behörde hierzu besonders ermächtigt sind.

Bei örtlichen Prüfungen wurde mitunter festgestellt, daß die Ermächtigungen mehr oder weniger pauschal an dienstliche Funktionen geknüpft waren, ohne daß sie sich auf bestimmte Personen bezogen. Das Gesetz schreibt aber eindeutig die Nennung der Namen der Berechtigten vor. Das Ministerium des Innern und für Sport wurde gebeten, in geeigneter Weise auf die richtige Handhabung hinzuwirken. Soweit bekannt, ist das geschehen.

Bei einer Überprüfung wurde die Frage gestellt, ob nur der Abfrager oder auch der Veranlasser einer Abfrage ermächtigt sein muß. Hier vertrat der LfD die Auffassung, daß die Veranlassung von Abfragen durch Sachbearbeiter sich aus den verschiedensten Gründen ergeben kann, die sich nicht voraussehen und hinsichtlich des handelnden Personenkreises auch nicht abgrenzen lassen. Eine weitere Ermächtigung auch der Veranlasser ist weder praktikabel noch nach der zitierten Rechtsvorschrift geboten.

5.12 Prüfungen bei Polizeidienststellen des Landes

Im Berichtszeitraum wurden das LKA mehrmals sowie 27 Polizeidienststellen überprüft; damit sind seit der Neuorganisation der Polizei des Landes alle Polizeipräsidien, das Wasserschutzpolizeiamt, alle Polizei- und Kriminaldirektionen, die Kriminalinspektionen und ein Teil der Polizeiinspektionen und Wasserschutzpolizeistationen überprüft worden. Es stehen noch aus jeweils etwa zwei Drittel der Polizeiinspektionen und der Wasserschutzpolizeistationen. In Zukunft sollen verstärkt die Verkehrsdirektionen bei den Polizeipräsidien mit ihren nachgeordneten Dienststellen überprüft werden. Die KpS-Haltung bei der Polizei des Landes ist mit Ausnahme der noch ausstehenden Feststellungen bei den Wasserschutzpolizeistationen flächendeckend überprüft.

Regelmäßiger Gegenstand von Prüfungen und Nachfragen sind neben der Kriminalaktenhaltung (KpS) die Rechtmäßigkeit der POLIS-Abfragen einschließlich der vorgeschriebenen Zusatzprotokollierung, die Art der Aktenvernichtung, die Aufbewahrung von Zweitschriften von Verkehrsunfall- und Ordnungswidrigkeitenanzeigen, die Einsichtnahmen in Paß- und Personalausweisregister sowie die Führung der Gewahrsamsunterlagen. Besonderes Augenmerk gilt auch der Beachtung der Verfahrensvorschrift des § 16 Abs. 5 AsylVfG bei Auswertungsanträgen an die beim BKA geführte Fingerabdruckdatei AFIS (vgl. Tz. 5.8) sowie der Aufbewahrungsdauer von Notrufaufzeichnungen.

Bei diesen örtlichen Feststellungen ergab sich insgesamt kein Grund zur Beanstandung. Es wurden aber zu verschiedenen Handhabungen Empfehlungen aus der Sicht des Datenschutzes gegeben. Von den Beamten vor Ort angeschnittene Probleme wurden besprochen und soweit möglich in Zusammenarbeit mit dem Ministerium des Innern und für Sport gelöst.

So wurden in einer Kriminalakte mehrere Unterlagen aus einer Telefonüberwachung (TÜ) aus dem Jahre 1993 festgestellt; und zwar sog. „Dokumentationsanzeigen" mit inhaltlichen Gesprächswiedergaben in Kurzform wie auch wörtliche Wiedergaben. Das Strafverfahren, zu dem die TÜ durchgeführt wurde, war zwischenzeitlich durch rechtskräftige Entscheidung des Gerichts abgeschlossen.

Der Vorgang wurde sofort bereinigt. Es bestand auch Übereinstimmung über ein Verfahren zur Auffindung und Bereinigung evtl. ähnlicher Vorgänge im Aktenbestand.

Bei einer Polizeiautobahnstation wurde es als Problem angesprochen, nach Verkehrsunfällen mit Feuerwehreinsatz das jeweilige Aktenzeichen der Bußgeldstelle oder der Staatsanwaltschaft an den Träger der eingesetzten Feuerwehr weiterzugeben. Nicht selten rückt ein ganzer Löschzug wegen mitunter geringfügigen Verletzungen von Personen aus. Diese zeigen ihren Unmut über die bis zu vierstelligen Rechnungsbeträge gegenüber der Polizei. Aus der Sicht des Datenschutzes bestehen aber gegen die o. g. Übermittlung keine Bedenken. Dies folgt aus dem allgemeinen Rechtsstaatsprinzip, wie es auch in § 25 a Abs. 1 Ziff. 3 POG zum Ausdruck kommt.

Bei einer Polizeiinspektion befanden sich im Wachraum in einem Ordner Unterlagen über ausländerrechtliche Verfügungen, teilweise auch aus Asylverfahren. Die Betroffenen waren im polizeilichen Informationssystem INPOL zur Fahndung ausgeschrieben. Dabei wurde festgestellt, daß der Polizei von der zuständigen Ausländerbehörde neben dem allein zur Ausschreibung erforderlichen Vordruck KP 21 auch die ausländerrechtliche Verfügung in vollem Wortlaut übersandt wurde. Eine Rückmeldung nach erfolgter Ausschreibung durch die Polizei an die Ausländerbehörde war nicht vorgesehen. Die Unterlagen wären solange vorgehalten worden, bis sich die Ausschreibung erledigt hätte (zehn Jahre). Es ist zweifelhaft, ob die Aufbewahrung derartiger ausländerrechtlicher Unterlagen bei der Eingabe von Fahndungsnotierungen durch die Polizei auf Ersuchen der Ausländerbehörden erforderlich ist.

Die Angelegenheit wird zur Zeit in Zusammenarbeit mit dem Ministerium geklärt.

5.13 Aufbewahrung von Zweitschriften bis zur Hauptverhandlung

Unter bestimmten Voraussetzungen legen in Strafsachen ermittelnde Polizeibeamte nach Abgabe des Ermittlungsvorganges an die Staatsanwaltschaft einen Vorgang an, der aus besonders wesentlichen Teilen der Ermittlungsakte, wie z. B. bestimmten Vernehmungsniederschriften, besteht. Da es sich rechtlich um Bestandteile der staatsanwaltschaftlichen Ermittlungsvorgänge handelt, bleiben die Gewährung von Akteneinsicht und die Erteilung von Auskünften aus diesen „Zweitschriften" der Staatsanwaltschaft vorbehalten. Werden im späteren Verlauf des Verfahrens weitere Ermittlungen nötig, können diese Zweitschriften ebenfalls unterstützend herangezogen werden; sie dienen aber auch der Vorbereitung der Beamten auf die Hauptverhandlung, in der sie möglicherweise als Zeugen auftreten müssen. Wegen der oft längeren Dauer bis zur Hauptverhandlung und der Vielzahl der von den betroffenen Beamten zwischenzeitlich bearbeiteten weiteren Vorgänge wäre ansonsten eine klare Erinnerung an Zusammenhänge und Einzelheiten möglicherweise beeinträchtigt. Allerdings dürfen diese Zweitschriften nur bis zum rechtskräftigen Abschluß des Strafverfahrens aufbewahrt werden; sie sind deshalb zu vernichten, wenn die entsprechende Mitteilung der Staatsanwaltschaft (gelber Vordruck nach MiStra Nr. 11) eingeht, jedoch mit Ausnahme derjenigen Teile, die nach den KpS-Richtlinien in die Kriminalakten übernommen werden. Die genannten Vorgänge sind daher strikt zu unterscheiden von den Kriminalakten nach den KpS-Richtlinien, die aufgrund einer Kriminalprognose über den Betroffenen zur vorbeugenden Bekämpfung evtl. zukünftiger Straftaten angelegt und vorgehalten werden. Beide Aktenarten sind deshalb getrennt voneinander aufzubewahren.

Nach Auffassung des LfD ist – in Fortführung der Haltung der damaligen Datenschutzkommission – die Aufbewahrung solcher Zweitschriften zu jedem der genannten Zwecke zulässig, wenn dies nach Lage des Falles erforderlich erscheint, insbesondere wenn Art und Umfang des Verfahrens dies gebieten. Es wäre aus der Sicht des Datenschutzes zu begrüßen, wenn den Beamten vor Ort hierfür geeignete nähere und verständliche Kriterien zur Verfügung gestellt würden.

Die Handhabung in der Praxis muß allerdings in engem Kontakt mit der jeweils verfahrensleitenden Staatsanwaltschaft geschehen sowie unter strikter Wahrung des Grundsatzes der Verhältnismäßigkeit.

In dem Zusammenhang ist es nicht ohne Bedeutung, daß bei Verkehrsunfällen mit Personen- oder Sachschäden die von den Verfahrensakten der Strafverfolgungs- oder Bußgeldbehörden ebenfalls getrennten polizeilichen Akten ein Jahr nach Ablauf des Kalenderjahres aufzubewahren sind, in dem sich der Vorfall ereignet hat (siehe Nr. 11 der Verkehrsunfallaufnahme-Richtlinien vom 22. August 1995, MinBl. 1995, 364).

5.14 Mitteilungen der Straßenverkehrsbehörden an die Polizei

Wie bei örtlichen Überprüfungen festgestellt wurde, teilen Straßenverkehrsbehörden der Polizei des Wohnortes der betreffenden Person die Entziehung der Fahrerlaubnis mit. Bei der überprüften Polizeidienststelle werden diese Mitteilungen an den zuständigen Sachbearbeiter weitergeleitet; es ergab sich die Frage, ob sie auch alphabetisch in einem Ordner abgeheftet werden können.

Aus der Sicht des Datenschutzes ist anzumerken, daß die Kenntnis von der Fahrerlaubnisentziehung sowohl zur künftigen Strafverfolgung wie auch zur Gefahrenabwehr im Grundsatz erforderlich ist. Im Prinzip sind derartige Entscheidungen zwar im bundesweiten Verkehrsinformationssystem ZEVIS abrufbar, es ist aber allgemein bekannt, daß sich die entsprechenden Eingaben dort mitunter über mehrere Wochen verzögern. Es besteht also für die Polizei praktischer Bedarf.

Der LfD hat deshalb das Ministerium des Innern und für Sport verständigt, daß bis zum Ablauf von einem Vierteljahr keine Bedenken gegen die Vorhaltung der Mitteilungen in Papierform bestehen. Von da an wäre allerdings von einer nicht erforderlichen Doppelspeicherung auszugehen. Die Mitteilungen sind von da an nicht mehr aufzubewahren.
In dem genannten Zeitraum bestehen auch keine Bedenken, wenn die Mitteilungen in einem-Ordner aufbewahrt werden.

5.15 Geisterautos und Schrottfrisierungen

Im 15. Tb. (Tz. 5.12) wurde über den kriminellen Mißbrauch der Kfz-Briefe total unfallbeschädigter Kraftfahrzeuge berichtet. Der LfD hatte auf Anfrage des Ministeriums des Innern und für Sport zu prüfen, ob ein Meldeverfahren zulässig sei, in dem die Zulassungsstellen unter bestimmten Voraussetzungen die Wiederzulassung von Kfz mit technischem Totalschaden der Polizei mitteilen. Der LfD hatte vorbehaltlich der Kenntnis der Details der angestrebten Regelung grundsätzlich keine Bedenken aus der Sicht des Datenschutzes.

Voraussetzung für das Tätigwerden der Polizei ist ein Anfangsverdacht im Sinne von § 152 Abs. 2 StPO, der auch bei Vorliegen bestimmter typischer Voraussetzungen angenommen werden kann. Das Ministerium hat in einem Rundschreiben vom September 1995 die Polizeibehörden auf die Situation aufmerksam gemacht und von der mit dem LfD übereinstimmenden Rechtsauffassung unterrichtet. Das Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau hat auf die gemeinsame Anregung hin durch Rundschreiben an die Zulassungsstellen vom Januar 1996 angeordnet, daß wieder zuzulassende Gebrauchtfahrzeuge – entsprechend der Grundregel der StVZO (§ 23 Abs. 4 Satz 5) – grundsätzlich vorgeführt werden müssen, wenn nicht das Vorliegen genau bestimmter Kriterien den Mißbrauch ausschließt. Bei bestimmten technischen Totalschäden ist die Polizei zu verständigen, z. B. dann, wenn Anhaltspunkte für Schrottfrisierungen und Scheinzulassungen vorliegen.

Bei örtlichen Feststellungen in Polizeidienststellen des Landes konnte jedoch bisher keine einzige Meldung der vorgesehenen Art festgestellt werden. Zwischenzeitlich wurde das Thema u. a. im zuständigen Bund-Länder-Fachausschuß „Fahrzeugzulassungen" kontrovers diskutiert. Welche Ursache das Ausbleiben der Meldungen hat, war bisher nicht festzustellen. Es ist jedoch festzuhalten, daß hier die wirksame Bekämpfung der Kraftfahrzeugkriminalität nicht durch den Datenschutz behindert wird.

Der LfD hat das Ministerium auf das magere Ergebnis der örtlichen Feststellungen insoweit aufmerksam gemacht.

5.16 Die Zusatzprotokollierung von POLIS-Abrufen ist stärker zu beachten

Mit Dienstanweisung vom 16. November 1992 wurde neben der schon vorhandenen Protokollierung jedes Abrufs im System POLIS und in Anlehnung an die bayerische Praxis eine Zusatzprotokollierung eingeführt, mit der bei jeder 20. Abfrage automatisch am Bildschirm die Aufforderung zur Eingabe des Anlasses der Abfrage mittels eines fünfteiligen Schlüssels erfolgt. Bis dahin bleibt der Bildschirm blockiert. Erfolgt die Abfrage im Auftrag eines anderen Sachbearbeiters, also eines Dritten (z. B. aus einem Funkstreifenwagen), so ist in jedem Fall der Abfrageanlaß (Schlüssel) sowie die Identifizierung des Auftraggebers einzugeben (siehe 14. Tb. Tz. 5.10).

Die Regelung wurde eingeführt, um bei Kontrollen des Abfrageverhaltens durch Aufsichtsbehörden und durch den LfD auch die Rechtmäßigkeit dieser Drittabfragen lückenlos überprüfen zu können. Frühere Kontrollen hatten ergeben, daß die unmittelbar Abfragenden sich im Zeitpunkt der Überprüfung wegen der Vielzahl der zwischenzeitlichen Vorgänge an den Grund und an die Auftraggeber nicht mehr erinnern konnten. Dies führte zu einer im Sinne des Datenschutzes nicht hinnehmbaren Lücke.

Die Lückenlosigkeit der Kontrolle liegt aber auch im wohlverstandenen Interesse der Polizeibehörden und ihrer Beamten, denn gerade dadurch kann das Aufkommen von Mißtrauen bei Betroffenen von vornherein verhindert werden. Bei Eingaben wie auch bei Diskussionen mit Interessierten und Betroffenen spielt erfahrungsgemäß der Hinweis auf die effektiven Kontrollen regelmäßig eine nicht zu unterschätzende Rolle.

Demgegenüber wird bei örtlichen Feststellungen in Dienststellen der Polizei immer wieder Kritik an der Zusatzprotokollierung geübt; sie wird als Ausdruck unberechtigten Mißtrauens empfunden, insbesondere aber als weitere Belastung im arbeitsmäßigen Ablauf. Hier stellt sich allerdings häufig das Mißverständnis heraus, daß im Grunde die verhältnismäßig lange Dauer des Aufrufens des POLIS-Programmes selbst gemeint ist. Verfügt bei einer kleineren Dienststelle der Beamte in der Zentrale nur über ein Gerät und erledigt er nachts gleichzeitig seine eigenen dienstlichen Arbeiten, so muß er in der Tat bei jedem Abfragewunsch aus einem Funkstreifenwagen sein Programm ausschalten und POLIS aufrufen. Bei einer örtlichen Feststellung hat sich dies durch eine probeweise Abfrage bestätigt. Gleizeitig stellte sich aber heraus, daß der zeitliche Aufwand für die Zusatzprotokollierung von untergeordneter Bedeutung ist. Damit erübrigen sich etwaige Überlegungen, diese Einrichtung zu überprüfen.

Da allerdings bei örtlichen Prüfungen wiederholt festgestellt werden mußte, daß die Zusatzprotokollierung nicht durchgängig, teilweise überhaupt nicht durchgeführt worden ist, hat der LfD das Ministerium des Innern und für Sport gebeten, in geeigneter Weise auf die konsequente Beachtung der genannten Dienstanweisung zu dringen. Das LKA hat zwischenzeitlich durch ein Rundschreiben an die Polizeibehörden des Landes erneut auf die Einhaltung der entsprechenden Dienstanweisung hingewiesen.

5.17 Dokumentation von Ermittlungen für eine andere Polizeidienststelle

Bei der Überprüfung einer Polizeiinspektion wurden im Keller zwei umfangreiche Aktenstücke gefunden, die Ermittlungen über einzelne Spuren für jeweils andere Polizeidienststellen betrafen. Es handelte sich um einen Entführungsfall und einen Raubüberfall. Die jeweils letzten Vorgänge datierten aus 1983 und 1985. Die Akten enthielten u. a. Fernschreiben, Vernehmungsprotokolle und Zeitschriftenausschnitte.

Die Aktenstücke dienten nach Angabe der zuständigen Stellen in erster Linie der Behördendokumentation. Mit dem Ministerium des Innern und für Sport bestand Übereinstimmung, daß unabhängig von der Frage, ob es sich um Behördendokumentation handelte oder nicht, eine eindeutige Klassifizierung derartiger Akten z. B. als KpS, Zweitschrift oder Dokumentationsakte zu erfolgen hat. Ebenso bestand kein Zweifel, daß die Aufbewahrung der Akten für die Erfüllung der Aufgaben der Stelle nicht mehr erforderlich war. Die Unterlagen sind im Zusammenhang mit der Überprüfung durch den LfD vernichtet worden.

Im Grunde handelt es sich auch bei derartigen Vorgängen um Teile der staatsanwaltschaftlichen Ermittlungsakten; ihr weiteres Schicksal richtet sich nach den Regeln über Zweitschriften und KpS, insbesondere soweit sie personenbezogene Daten z. B. in Kopien von Vernehmungsniederschriften enthalten. Ist der eigentliche Ermittlungsvorgang an die sachbearbeitende Polizeidienststelle oder direkt an die ermittlungsführende Staatsanwaltschaft abgegeben, ist auf alle Fälle organisatorisch dafür Sorge zu tragen, daß der Ausgang des Verfahrens rechtzeitig bekannt wird, damit die vorgeschriebenen Konsequenzen gezogen werden können.

5.18 Generalerrichtungsanordnungen

Im 14. Tb. (Tz. 5.22) wurde das in Rheinland-Pfalz eingeführte System der Generalerrichtungsanordnungen (GEA) beschrieben, mit dem jeweils Dateienarten mit im wesentlichen gleichen Inhalt nach § 25 g POG generalisiert für die Polizei des Landes angemeldet werden können, so daß die einzelnen Anmeldungen nach dem LDSG in verkürzter Form erfolgen können. Wie schon damals feststellbar, kann auf diese Weise sehr viel Verwaltungsaufwand bei mindestens gleichem Effekt erspart werden. Auch in der Berichtsperiode hat sich diese Einrichtung bewährt. Bei Redaktionsschluß ist die Zahl dieser GEA auf insgesamt zehn angestiegen.

Dabei handelt es sich neben den bereits bekannten und überwiegend seit längerem angewandten GEA „Medico" für Ärzteverfahren, „Ermittlungsverfahren" für strafrechtliche umfangreiche Ermittlungsverfahren, „Alarmierungsdatei" für Alarmierungen zur Gefahrenabwehr (eigene Bedienstete, Abschleppdienste, Dolmetscher, Ärzte, Handwerker etc.) sowie der TÜ-Dateien „Phone" um folgende neuere Dateienbereiche:

„Automatisierte Vorgangs- und Asservatenverwaltung der Polizei des Landes Rheinland-Pfalz (AVP)": Es handelt sich um die Registrierung, Verwaltung und Dokumentation von Vorgängen und Asservaten bei der Polizei. Betroffen sind Personen, deren Daten zur Registrierung, Verwaltung und Dokumentation von Akten sowie Asservaten benötigt werden.

„Verkehrsüberwachungsanlagen": Gegenstand ist die rechnerische Auswertung von Videoaufnahmen überwiegend auf Bundesautobahnen durchgeführter Geschwindigkeits- und Abstandsmessungen zum Zwecke der Anzeigenbearbeitung. Betroffen sind Beschuldigte, Betroffene i. S. d. Ordnungswidrigkeitenrechts, Halter, Zeugen, Anzeiger und Sachbearbeiter.

„Überörtliche Eigentumskriminalität": Es geht um überörtlich agierende Täter. Zur Deliktsbreite gehören im wesentlichen Serien von Einbruchsdiebstählen in Geschäfte, Post- und Geldinstitute sowie Wohnungen bis hin zu Raubdelikten.

„Jugendgruppenkriminalität": Die Datei dient der Tataufklärung typischer Jugendgruppendelikte insbesondere an Schulen, in deren Umfeld sowie auf öffentlichen Straßen und Plätzen, aber auch der zielgruppenorientierten Prävention u. a. durch das Erkennen wechselnder Gruppenzusammensetzungen bzw. -strukturen sowie der unterschiedlichen Beziehungsgeflechte zwischen Tätern und Opfern.

„Jugenddelinquenz": Es handelt sich um eine Datei zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung, für die die Polizei im Bereich der Jugenddelinquenz z. B. Beauftragte für Jugendsachen einsetzt, deren Aufgabe es ist, Lagebilder zu erstellen sowie Problemanalysen der Jugenddelinquenz zu entwickeln.

Seit kurzem wird die Übersendung der einzelnen Kurzanmeldungen von Telefonüberwachungsdateien im Rahmen der GEA „Phone" durch das Justizministerium in Frage gestellt, nachdem der LfD auf diese Weise Defizite bei der zeitgerechten Löschung einer solchen Datei festgestellt hatte und rügen mußte. Hauptbedenken ist offenbar die Befürchtung, der Erfolg von Ermittlungsverfahren könnte gefährdet werden, weil der Personenkreis, der von einem einzelnen Verfahren Kenntnis erhält, „ohne Not vergrößert wird". Hierzu ist zunächst zu sagen, daß die 1991 mit Kenntnis und unter Beteiligung der Justiz eingeführte und seither eingespielte und bewährte Praxis zu keinem einzigen Fall von Indiskretion geführt hat. Auch die Arbeitsbelastung hält sich in engen Grenzen, denn die einzelne Mitteilung an den LfD besteht jeweils aus einem formatierten Blatt und enthält keine Namen.

Der datenschutzrechtliche Ertrag ist aber beachtlich: Der LfD kann Schwerpunkte der Nutzung dieser sensiblen automatisierten Datenverarbeitungen feststellen und dementsprechend auch Prüfungsschwerpunkte finden; dies setzt ihn in die Lage, im Wege der begleitenden Kontrolle bei überdurchschnittlich langen Speicherzeiten konkret nachzufragen. Die genannte Praxis hat sich somit als ein bewährtes Mittel des auch vom Bundesverfassungsgericht geforderten organisatorischen Datenschutzes erwiesen.

Der LfD müßte bei einem Wegfall dieses Kontrollmittels angesichts der besonderen Eingriffstiefe der in Frage stehenden Maßnahmen in mehr oder weniger regelmäßigen Abständen schriftliche Auskünfte bei den einzelnen Polizeibehörden zur Frage des Einsatzes von Phone-Dateien einholen. Dabei würden jeweils in erheblichem Umfang personenbezogene Daten bekannt, jedenfalls mehr wie bei dem derzeitigen Verfahren.

In diesem hochsensiblen Bereich mit empfindlichen Eingriffen sollte die Arbeit des LfD nicht behindert werden. Die Erörterungen sind noch nicht abgeschlossen.

5.19 Ringalarmfahndungsdaten Unbeteiligter jahrelang im Computer

Um die Aufklärung einer Reihe sachlich im Zusammenhang stehender Banküberfälle zu unterstützen, wurden die bei den jeweilig sofort ausgelösten Ringfahndungen gewonnenen Daten in einer POLDOK-Datei gespeichert und gegeneinander abgeglichen. Gespeichert wurden Fahrzeugkennzeichen, teilweise mit Fahrzeugtyp und Farbe. In Frage kamen sowohl solche Fahrzeuge, die bei der jeweiligen Ringalarmfahndung angehalten wurden, als auch solche, die nicht angehalten, aber notiert wurden (sog. „Durchfahrtskontrolle"). Der LfD stieß bei einer Prüfung dieser Datei auf insgesamt 767 Dokumente. Die Datei selber war vor etwa zweieinhalb Jahren errichtet worden. Ohne Kenntnis der Prüfung durch den LfD hat das zuständige Polizeipräsidium die Datei zum fast gleichen Zeitpunkt gelöscht, offenbar weil sie nicht den Zweck erfüllte, den man sich von der in POLDOK möglichen Datenauswertung erhofft hatte.

Der Inhalt der Datei wirft gleichwohl die Frage auf, ob es im Rahmen der bestehenden Rechtsgrundlage in der Strafprozeßordnung und möglicherweise auch im POG noch verhältnismäßig war, über einen mehrjährigen Zeitraum eine größere Anzahl von personenbeziehbaren Daten Unbeteiligter zu speichern. Hierfür könnten zwar die Schwere des Tatvorwurfes sowie der Umstand sprechen, daß die auf das Fahrzeug bezogenen Daten im Grunde wenig sensibel sind, solange sich nicht aus dem Zusammenhang oder mit anderen – zunächst unbekannten – Fakten doch eine Sensibilität im Einzelfall ergeben könnte.

Die Dauer der Speicherung hat nach Angaben der Polizei zu keinen nennenswerten Erkenntnissen geführt. Gerade darin liegt aber hier der Schwerpunkt des Eingriffs in das Recht der unbeteiligten Betroffenen auf informationelle Selbstbestimmung.

Zum Zeitpunkt der Einrichtung der Datei und eine Zeit danach war diese Maßnahme nach dem Kenntnisstand des LfD möglicherweise geeignet und verhältnismäßig. Es hätte aber zu einem wesentlich früheren Zeitpunkt geprüft werden müssen, ob eine Löschung erfolgen kann, um die nach dem Kfz-Kennzeichen weiterhin auswertbaren personenbezogenen Daten vieler Unbeteiligter zu vermeiden.

Der LfD hat gegenüber dem Ministerium des Innern und für Sport eine grundsätzliche gemeinsame Prüfung der Modalitäten, insbesondere der Speicherungsdauer, angeregt, falls die genannte Praxis auch in Zukunft landesweit als geeignetes Aufklärungsmittel angesehen werden sollte.

5.20 Nutzung der Telefon-Informationssoftware „D-INFO" auf CD-ROM durch die Polizei

In der Berichtszeit wurden über den Handel von verschiedenen Anbietern CD-ROM mit den Telefondaten aller in den offiziellen Telefonbüchern Deutschlands aufgeführten Anschlußinhaber verkauft. Dabei werden verschiedene Such- und Ver-

knüpfungsmöglichkeiten geboten. Zumindest ein Anbieter ermöglicht dabei auch die sog. „Invert-Suche", mit der über die Telefonnummer ein im Telefonbuch aufgeführter Anschlußinhaber feststellbar wird. Darüber hinaus bestehen weitere Selektions- und Suchmöglichkeiten. Allein von einer Version sollen insgesamt 700 000 bis 800 000 Exemplare verkauft worden sein.

Wegen der Zulässigkeit des Vertriebs insbesondere der CD-ROM mit der Invertsuche sind verschiedene zivilrechtliche Streitverfahren anhängig gemacht worden, die zu unterschiedlichen Beurteilungen geführt haben. So hat das OLG Karlsruhe die systematische und vollständige Übernahme der Teilnehmerdaten aus dem Telefonverzeichnis der Deutschen Telekom AG in ein eigenes Datenwerk als unlautere Behinderung und damit als wettbewerbswidrig eingestuft, während das OLG Frankfurt in einer Entscheidung vom Oktober 1996 sich auf den gegenteiligen Standpunkt stellte. In den jeweiligen Urteilsgründen wird schwerpunktmäßig auf wettbewerbsrechtliche Argumente abgestellt, dabei aber inzident auch auf die Frage eingegangen, ob und inwieweit datenschutzrechtliche Bestimmungen (§§ 29 und 33 BDSG) verletzt sind. Während das OLG Karlsruhe dies annimmt, läßt es das OLG Frankfurt dahinstehen.

Zwischenzeitlich wurde in § 89 Abs. 9 TKG ein Widerspruchsrecht der Kunden geregelt. Der Widerspruch ist in den Verzeichnissen des Diensteanbieters unverzüglich zu vermerken und ist auch von anderen Diensteanbietern zu beachten, sobald er in dem öffentlichen Verzeichnis des Diensteanbieters vermerkt ist. In § 10 TDSV werden die Diensteanbieter verpflichtet, auf Verlangen des Kunden die Eintragung in elektronischen oder allgemein in gedruckten öffentlichen Kundenverzeichnissen ganz oder teilweise kostenfrei zu unterlassen. Die Eintragungen sind gesondert zu kennzeichnen.

In der Diskussion wird teilweise gefolgert, daß die mit dem Verkauf der CD-ROM verbundene Übermittlung der Telefonteilnehmerdaten unzulässig sei und demzufolge auch deren Speicherung und Nutzung durch Behörden. Gestützt wird diese Auffassung ohne nähere Ausführungen allgemein auf das Rechtsstaatsprinzip und auf den das Polizeirecht prägenden Verhältnismäßigkeitsgrundsatz, ebenso auf einen „Anspruch auf Folgenbeseitigung".

Aufgrund einer Anfrage des Ministeriums des Innern und für Sport hatte der LfD zu prüfen, ob die Nutzung vorhandener CD-ROM der o. g. Art durch die Polizei zur Gefahrenabwehr und zur Strafverfolgung zulässig ist.

Der LfD ist bei seiner Beurteilung davon ausgegangen, daß Daten auf einer CD-ROM, die in einer Stückzahl von etwa einer Million im Umlauf ist, in einer allgemein zugänglichen Quelle i. S. v. § 2 Abs. 5 LDSG gespeichert sind. Danach ist das LDSG auf diese Daten nicht anzuwenden. Der damit ausgedrückte Rechtsgedanke schließt derlei personenbezogene Daten vom Schutz durch das informationelle Selbstbestimmungsrecht aus, weil der Schutz von Daten, die ohnehin jedermann zugänglich sind, praktisch nicht mehr möglich ist und insoweit die gesetzlichen Schutzmechanismen zur Farce machen würde. Dieser Rechtsgedanke ist auch uneingeschränkt bei der Anwendung des § 25 a Abs. 1 POG zu berücksichtigen, der die Polizei für Zwecke der Gefahrenabwehr zur Erhebung, Nutzung und Speicherung personenbezogener Daten ermächtigt.

Soweit das Vorhalten der CD-ROM zwangsläufig mit Speicherungen von personenbezogen Daten der Anschlußinhaber verbunden ist, entfällt aus der gleichen Überlegung ein relevanter Eingriff in das Recht auf informationelle Selbstbestimmung. Ansonsten wäre für die Polizei der bloße Besitz eines Telefonbuches auch unzulässig.

Auch vom praktischen Ergebnis her wäre es nur schwer vermittelbar, die Polizei da blind zu machen, wo jedermann es sehen kann. Für die Strafverfolgung gelten die o. g. Überlegungen entsprechend für die Anwendung der §§ 161 und 163 StPO. Damit ist die Nutzung der allgemein im Handel erhältlichen o. g. Telefondaten-CD-ROM durch die Polizei aus der Sicht des Datenschutzes nicht zu beanstanden.

Die Kommission beim Landesbeauftragten für den Datenschutz hat sich dieser Beurteilung angeschlossen.

In diesem Zusammenhang kann es auch nicht unberücksichtigt bleiben, daß nach dem Telekommunikationsgesetz die Polizei zur Erfüllung ihrer gesetzlichen Aufgaben jederzeit Auskünfte aus den Kundendateien erhält; insoweit verschafft ihr die genannte CD-ROM im Grunde keine zusätzliche Kenntnis von personenbezogenen Daten, kann aber in gewisser Hinsicht eine Erleichterung der praktischen Arbeit bedeuten.

Die gesetzlichen Regelungen stehen dem nicht entgegen. § 89 Abs. 9 TKG wendet sich nur an die Diensteanbieter. § 10 TDSV regelt nicht die Nutzung bereits erstellter und herausgegebener Kundenverzeichnisse. Aussagen in der Begründung wettbewerbsrechtlicher Urteile können im hier zu beurteilenden Zusammenhang nicht herangezogen werden, weil ihre Rechtskraft grundsätzlich nur zwischen den Parteien („inter partes") gilt und zudem die Urteilsgründe an der Rechtskraft nicht teilnehmen.

5.21 „Wer rast, der spielt mit dem Leben unserer Kinder"

In dem anerkennenswerten Bemühen, die Sicherheit von Kindern im Straßenverkehr noch mehr zu verbessern, unterstützte das Ministerium des Innern und für Sport die Gemeinschaftsaktion eines Fernsehsenders und einer gastronomischen Firma, nach deren Konzeption in Anwesenheit von Kindern im Bereich von Schulen und Kindergärten Verkehrskontrollen mit der Polizei durchgeführt werden.

Bei diesen Kontrollen hat zwar die Aufklärung und das Gespräch mit den „auffällig gewordenen" Kraftfahrern Vorrang vor etwaigen Sanktionen. Es galt aber auch, die Kraftfahrer „in einem klärenden Gespräch unmittelbar im Anschluß an den Verkehrsverstoß auf ihr Fehlverhalten anzusprechen". In die Gespräche waren die Kinder einbezogen. Keinesfalls würden die Kraftfahrer, so das Ministerium des Innern und für Sport, „an den Pranger gestellt". Nach einem Pressebericht, durch den der LfD auf die Praxis aufmerksam wurde, ergoß sich ein Redeschwall über die peinlich berührten Autofahrer. Ohne Maulen und Murren hätten die Kinder den jeweiligen Bremsweg zur aktuellen Geschwindigkeit errechnet.

In seiner ersten Antwort schon stimmte das Ministerium mit dem LfD überein, daß es nicht dazu kommen dürfe, daß einzelne Autofahrer sich gegen ihren Willen gegenüber den Schulkindern für ihr Fehlverhalten rechtfertigen müßten. Hierauf wollte das Ministerium bei vergleichbaren Aktionen in der Zukunft nochmals ausdrücklich hinweisen.

Da es bei entsprechenden Veranstaltungen durchaus denkbar ist, daß in der Praxis – wenn auch ungewollt – personenbeziehbare Daten zur Kenntnis der Schulkinder gelangen, hat der LfD angeregt, durch geeignete Maßnahmen sicherzustellen, daß keine Übermittlungen erfolgen, die der entsprechenden Rechtsgrundlage entbehren. In diesem Zusammenhang ist anzumerken, daß durch die Kenntnis des Kfz-Kennzeichens und ggf. auch der Person des Fahrers (letzteres ist ohnehin ein personenbezogenes Datum) alle Daten über das Vorliegen eines Verstoßes überhaupt, über die gefahrene Geschwindigkeit etc. personenbeziehbar werden.

Es besteht volle Übereinstimmung mit dem Ministerium, daß auch einmal unkonventionelle Wege beschritten werden sollten, wenn es um die Sicherheit und das Leben unserer Kinder geht und daß dabei selbstverständlich die Persönlichkeitsrechte der Betroffenen gewahrt und geachtet werden müssen.

5.22 Privates Sicherheitsgewerbe fahndet im Internet (System „EuSIS")

In früheren Tätigkeitsberichten hat der LfD auf die möglichen Gefahren für den Datenschutz hingewiesen, die durch eine bundesweite Ausdehnung von Dateien privater Sicherheits- und Überwachungsdienste entstehen können (13. Tb. Tz. 21.5 und 14. Tb. Tz. 5.27). Dabei wurde befürchtet, daß der in den vergangenen Jahren bei den Polizeibehörden bundesweit erreichte Standard des Datenschutzes zu Lasten der Rechte der Bürger unterlaufen wird.

Seit dem Frühjahr 1997 bietet eine in Schleswig-Holstein ansässige Firma über das Internet „EuSIS" als ein „modulares Informationssystem" an, „welches für die aktuellen Bedürfnisse von Sicherheitsdienstleistern entwickelt wird. Das private Informationssystem nutzt leistungsfähige Datenbanken auf einem Internet-Server und das Internet als Kommunikationsmedium."

Ein öffentlicher Bereich steht allen Internet-Nutzern offen, ein weiterer nur registrierten Anwendern (Kennwort). Dieser enthält nach der Darstellung der Firma verschiedene Datenbankdienste „wie z. B. Personen-, Sach- und Ereignisfahndungsausschreibungen" sowie eine Ereignissammlung. Dem privaten Ermittler soll die Möglichkeit gegeben werden „unter Einhaltung des Datenschutzes" über verschiedene Datenbanken Personen- und Sachfahndungen auszuschreiben. „EuSIS" (für: Europäisches Sicherheits-Informationssystem) ist als „vernetztes Ermittlungsorgan" nutzbar, „um so Erfolge in der Wiederbeschaffung und Überprüfung von Sachgegenständen zu erzielen". Bei einer Nachschau im Internet durch den LfD im Juli 1997 waren zwölf Sachfahndungen, aber keine Personenfahndung eingestellt.

Unabhängig von dem weiten Komplex der rechtlichen Beurteilung aller Art von Aktivitäten im Internet darf man insbesondere aus der Sicht des Datenschutzes von der Gesetzgebungsseite her die Dinge nicht weiter treiben lassen. Zumindest für das von Umfang und Bedeutung her anwachsende private Sicherheitsgewerbe ist eine gesetzliche Regelung dringend geboten, die die Verantwortlichkeiten und Rechte Dritten gegenüber unter Beachtung des Grundsatzes der Verhältnismäßigkeit und des Rechts auf informationelle Selbstbestimmung klar definiert.

5.23 Großer Lauscheingriff

Die verfassungsrechtliche Regelung des Großen Lauscheingriffes sowie die entsprechenden Detailregelungen in der StPO kommen jetzt in die entscheidende gesetzgeberische Phase. Die dem Bundestag vorliegenden Entwürfe der Fraktionen der CDU/CSU, SPD und F.D.P. lassen unter bestimmten Voraussetzungen und bei Beachtung verschiedener Verfahrenssicherungen aufgrund richterlicher Anordnung die Anwendung technischer Mittel zur akustischen Überwachung von Wohnungen jetzt auch zu Zwecken der Strafverfolgung zu. Gleichzeitig wird der Einsatz dieses Mittels zur Abwehr dringender Gefahren für die öffentliche Sicherheit geregelt. Erstmals werden auch Bestimmungen über derartige Maßnahmen des Verfassungsschutzes vorgeschlagen.

Im Blick auf die grundsätzlich ablehnende Haltung der Datenschutzbeauftragten des Bundes und der Länder (damals bei Gegenstimme Bayerns) vom Oktober 1992 sieht der LfD auch heute in dem geplanten Vorhaben einen besonders schweren

Eingriff in die Persönlichkeitsrechte der Bürger, hier auch in das Recht auf informationelle Selbstbestimmung. Die Zahl derartiger Eingriffe, bisher unter engen Voraussetzungen nur zur Gefahrenabwehr und zu Zwecken des Verfassungsschutzes zulässig, wird sicherlich stark ansteigen.

Andererseits ist derzeit vor dem Hintergrund und in Anbetracht der Entwicklung der kriminalstatistischen Erkenntnisse zum Vordringen organisierter Kriminalität in Deutschland nicht einfach zu übersehen, daß die Kriminalitätsbekämpfung im Vergleich zu den anderen EU-Staaten in ihrer Wirksamkeit nicht wesentlich zurückbleiben darf.

Vor diesem Hintergrund kann der Einsatz elektronischer akustischer Aufklärungsmittel äußerstenfalls auch in Wohnungen aber nur in Betracht kommen, wenn enge materiell-rechtliche Voraussetzungen im Grundgesetz und in der StPO geschaffen werden. Zulässig darf er nur sein, wenn es um die Aufklärung schwerster Verbrechen (z. B. Mord, schwere Verbrechen der organisierten Kriminalität, Rauschgifthandel und vergleichbare Delikte) geht.

Der LfD hat insoweit weitgehend übereinstimmend mit anderen Datenschutzbeauftragten u. a. die Genehmigung des Einsatzes im Einzelfall durch ein Richterkollegium gefordert sowie die jeweilige Genehmigung des Antrages der Staatsanwaltschaft durch den Justizminister, einen jährlichen ausführlichen Bericht an das Parlament, die Unterrichtung der Betroffenen, wenn der Ermittlungszweck nicht mehr gefährdet ist, und die uneingeschränkte Datenschutzkonrolle bei der Durchführung der Einzelmaßnahmen.

Darüber hinaus hat der LfD die rechtsstaatliche Regelung des Einsatzes entsprechender Mittel durch den Verfassungsschutz in Art. 13 GG gefordert, insbesondere auch hier das Erfordernis der Anordnung durch unabhängige Richter (s. hierzu 14 Tb., Tz. 5.5 und 15. Tb., Tz. 6.3).

Einige der Forderungen sind in den o. g. Gesetzentwürfen ganz oder teilweise realisiert, wie der Entscheid durch ein Richterkollegium und die Berichte an das Parlament, was zu begrüßen ist.

Dies gilt auch für die Tatsache, daß entsprechende Maßnahmen des Verfassungsschutzes nun im Grundgesetz für den Bürger erkennbar geregelt werden. Dabei ist nach wie vor zu fordern, daß auch diese Eingriffe wegen ihrer Gleichartigkeit ebenfalls durch unabhängige Richter anzuordnen sind. Der LfD geht davon aus, daß Maßnahmen der in Frage stehenden Art nur „zur Abwehr dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr" ergriffen werden dürfen, wie es sich aus der Systematik des vorgesehenen Absatzes 4 des Art. 13 ergibt und wie es in der Begründung des Gesetzentwurfs bestätigt wird. Dies muß aber im Text deutlicher zum Ausdruck kommen.

Der in dem Entwurf zur Änderung der StPO enthaltene Katalog von Straftaten geht deutlich über den Gesetzeszweck der verbesserten Bekämpfung der organisierten Kriminalität hinaus; er sollte strikt auf die hierfür bestehenden Notwendigkeiten beschränkt werden. Schon jetzt können bei einigen der vorgesehenen Katalogstraftaten Zweifel bestehen, ob es sich, wie in Art. 13 Abs. 3 GG des Entwurfs vorgesehen, um „besonders schwere Straftaten" handelt.

Darüber hinaus darf der Eingriff nicht schon zugelassen werden, wenn „bestimmte Tatsachen den Verdacht begründen". Maßgebende Voraussetzung sollte das Vorliegen eines dringenden Tatverdachtes sein.

Unverzichtbar ist eine ausdrückliche Sicherung der in Art. 4 Abs. 2 GG gewährleisteten ungestörten Religionsausübung. Diese kann, wie gerade die jüngste öffentliche Diskussion zeigt, durch die Anwendung der vorgesehenen Bestimmung empfindlich beeinträchtigt werden. Dem besonderen Rang dieses Grundrechtes wird es nicht gerecht, wenn sein Schutz in dem hier angesprochenen Zusammenhang von der Anwendung des Grundsatzes der Verhältnismäßigkeit im Einzelfall abhinge. Dies würde nämlich bedeuten, daß es in Fällen, die bei der Rechtsanwendung für extrem bedeutend gehalten werden, eben doch möglich wäre, z. B. den Inhalt einer Beichte abzuhören und aufzuzeichnen. Hier ist nur ein absolut wirkender Schutz das allein angemessene gesetzgeberische Mittel. Auch rechtstechnische Schwierigkeiten können nicht entgegenstehen. In Anlehnung an den Text des Grundgesetzes wäre insoweit eine Formulierung ausreichend, die die unmittelbare Religionsausübung ausnimmt.

In gleicher Weise sind die Zeugnisverweigerungsrechte der Berufsgeheimnisträger und der Personen, die aus persönlichen Gründen zur Verweigerung des Zeugnisses berechtigt sind, zu achten.

Im Zusammenhang mit der Zulassung elektronischer akustischer Raumüberwachungsmittel muß gefordert werden, daß der Persönlichkeitsschutz beim Eindringen der Strafverfolgungsorgane in die Privatsphäre auch für die derzeit bereits zulässigen Maßnahmen (insbesondere Telefonabhörmaßnahmen) verbessert wird. Hierfür hat der LfD in den vorhergehenden und in diesem Tb. (s. hier Tz. 7.1.1) Vorschläge zur Verbesserung des Datenschutzes formuliert.

Schließlich wäre es angemessen, wenn der Gesetzgeber sich angesichts der jetzt beabsichtigten Eingriffe in Grundrechte zur Bedeutung des informationellen Selbstbestimmungsrechtes bekennen und wenn er dieses durch seine ausdrückliche Regelung im Grundgesetz betonen würde.

6. Verfassungsschutz

6.1 Dauerbrenner: Neufassung des Verfassungsschutzgesetzes

Auch in der Berichtsperiode ist es nicht zu der erwarteten Neufassung des Landesverfassungsschutzgesetzes gekommen. Die schon im 15. Tb. (Tz. 6.3) gestellte Forderung nach einer normenklaren und transparenten Regelung in Anlehnung an die Systematik anderer Ländergesetze ist daher erneut und verstärkt zu erheben. Zur Vermeidung von Wiederholungen darf an dieser Stelle auf die seinerzeit dargestellten Anforderungen aus der Sicht des Datenschutzes Bezug genommen werden, die nach wie vor aktuell sind. Dies gilt insbesondere auch für die Forderung, das Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes mit technischen Mitteln aus Wohnungen ebenfalls für den Verfassungsschutz von richterlicher Einzelfallentscheidung abhängig zu machen.

Ergänzend wird auf die Notwendigkeit hingewiesen, Maßnahmen gegenüber unorganisierten Einzelpersonen auf Militante zu beschränken, da die isoliert gezielte Beobachtung von Einzelpersonen, die nicht im Tätigkeitszusammenhang mit einer Gruppe stehen, eine weitere Eingriffsdimension in Richtung allgemeiner Überwachung eröffnet. Deshalb müssen die gesetzlichen Voraussetzungen hierfür besonders eng bestimmt sein.

Einer gesetzlichen Regelung bedarf auch die Auskunfterteilung auf Anfrage von Einstellungsbehörden. Diese richtet sich derzeit nach der Verwaltungsvorschrift „Pflicht zur Verfassungstreue im öffentlichen Dienst" des Ministeriums des Innern und für Sport vom 27. Dezember 1990 (MinBl. 1991, 15). Dort ist sinngemäß bestimmt, daß derartige Anfragen nur in bestimmten Fällen zu stellen sind, was praktisch auf das Vorhandensein konkreter Anhaltspunkte für die Anfrage hinausläuft. Dabei handelt es sich jeweils um erhebliche Eingriffe in das Persönlichkeitsrecht der betroffenen Bewerber. Schon von daher sollte unter Berücksichtigung der Wesentlichkeitstheorie des Bundesverfassungsgerichts die Regelung durch Gesetz erfolgen und nicht weiter lediglich auf eine Verwaltungsvorschrift gestützt werden. Nur so könnte wirksam bestimmt werden, daß derartige Anfragen tatsächlich auf das erforderliche Mindestmaß beschränkt bleiben und daß insbesondere die jeweiligen Gründe nachprüfbar sind. Die alte Regelanfrage darf sich unter keinen Umständen wieder einschleichen.

Auf alle Fälle muß die uneingeschränkte Kontrollmöglichkeit des LfD auch gegenüber dem Verfassungsschutz erhalten bleiben. Das Recht des zuständigen Ministers, unter bestimmten Voraussetzungen (Gefährdung der Sicherheit des Bundes oder eines Landes) dem LfD im Einzelfall Auskunft sowie Einsicht in Unterlagen und Akten zu verweigern, ist vom Landtag im neuen Landesdatenschutzgesetz bewußt gestrichen worden. Dies hat sich bewährt, denn das Vertrauen der Bürgerinnen und Bürger in die uneingeschränkte Kontrollfähigkeit des LfD ist Voraussetzung für die Akzeptanz dessen, was ihnen nach einer Überprüfung ihrer Beschwerden und Anfragen mitgeteilt wird.

Rheinland-Pfalz hat insoweit eine vorbildliche Regelung.

6.2 Sicherheitsüberprüfungsgesetz gefordert

Schon im 15. Tb. (Tz. 6.2) wurde auf das verfassungsrechtliche Defizit hingewiesen, das in der Vornahme verschiedener gravierender Eingriffe bei den Sicherheitsüberprüfungen ohne bereichsspezifische gesetzliche Grundlage besteht. Die zur Zeit angewendeten Richtlinien zur Sicherheitsüberprüfung können die vom Bundesverfassungsgericht in seiner Rechtsprechung zur sog. „Wesentlichkeitstheorie" (BVerfGE 20, 150 ff.) für gravierende Eingriffe geforderte gesetzliche Grundlage nicht ersetzen.

Es wird angeregt, bis zur Vorlage und Verabschiedung eines Sicherheitsüberprüfungsgesetzes wenigstens die im Sinne des Rechts der Betroffenen auf informationelle Selbstbestimmung besonders wesentlichen Regelungen wie die Einbeziehung von Ehegatten und Partnern, die Auskunft an Behörden sowie die Benachrichtigung und Zustimmung der Betroffenen in der wahrscheinlich früher erfolgenden Neufassung des Landesverfassungsschutzgesetzes zu regeln.

Gleichwohl muß an der Forderung nach einer möglichst raschen und umfassenden gesetzlichen Regelung – wie auch auf Bundesebene – festgehalten werden.

6.3 Verfassungsschutz beobachtet „Scientology"-Organisation

Im Juni 1997 beschloß die Innenministerkonferenz die Beobachtung der „Scientology"-Organisation (SO) durch die Verfassungsschutzbehörden des Bundes und der Länder. Die Konferenz hatte zuvor eine Arbeitsgruppe aus Vertretern mehrerer Verfassungsschutzbehörden mit der rechtlichen Vorprüfung beauftragt; deren über 200 Seiten umfassender Bericht bildete dann die Grundlage.

Für den Bund ergeben sich die Rechtsvoraussetzungen aus § 3 Abs. 1 Ziff. 1 BVerfSchG, wonach es Aufgabe der Verfassungs-

schutzbehörden des Bundes und der Länder ist, Informationen zu sammeln und auszuwerten u. a. über Bestrebungen, die gegen die freiheitlich-demokratische Grundordnung gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben. Nach § 4 Abs. 1 Buchst. c BVerfSchG sind Bestrebungen gegen die freiheitliche demokratische Grundordnung solche politisch bestimmten ziel- und zweckgerichteten Verhaltensweisen in einem oder für einen Personenzusammenschluß, der darauf gerichtet ist, einen von mehreren aufgezählten Verfassungsgrundsätzen zu beseitigen oder außer Geltung zu setzen. Hierzu zählen nach Absatz 2 u. a. das Recht auf Wahlen, die Gesetzmäßigkeit der Verwaltung, die Bindung der Verwaltung und der Rechtsprechung an Gesetz und Recht, das Recht auf eine parlamentarische Opposition, die Unabhängigkeit der Gerichte und die im Grundgesetz konkretisierten Menschenrechte.

Bei Vorliegen dieser Voraussetzungen darf der Verfassungsschutz des Landes nach § 4 Abs. 1 Ziff. 1 LVSG die nach pflichtgemäßem Ermessen notwendigen Maßnahmen treffen, insbesondere personenbezogene Informationen erheben und verarbeiten, wenn tatsächliche Anhaltspunkte für den Verdacht von Bestrebungen oder Tätigkeiten im o. g. Sinne vorliegen.

Da die Beobachtung der SO durch die Verfassungsschutzbehörde des Landes in erheblichem Umfang Auswirkung auf die Verarbeitung personenbezogener Daten bis hin zur Anwendung nachrichtendienstlicher Mittel haben wird, hat der LfD mit örtlichen Feststellungen beim Verfassungsschutz die tatsächlichen Anhaltspunkte überprüft, die der Beobachtung von SO zugrunde liegen.

Dabei spielte der o. g. Bericht der Arbeitsgruppe eine wesentliche Rolle. Insgesamt wird aufgrund aller vorhandenen Erkenntnisse davon ausgegangen, daß anhand der veröffentlichten Programmatik und der dieser entsprechenden Aktivitäten von SO der Verdacht verfassungsfeindlicher Bestrebungen konkret begründet ist. Die Aktivitäten werden durch die Tatsachenfeststellungen von Gerichtsurteilen, durch Untersuchungsergebnisse in verschiedenen Staaten, durch übereinstimmende und detaillierte Aussagen kompetenter Aussteiger sowie durch verschiedene der SO zuzuordnende Vorkommnisse in Deutschland zurückgeführt, bei denen u. a. in unzulässiger Weise Druck auf Volksvertreter ausgeübt wurde.

Das sich ergebende Bild zeigt die Absicht von SO, auch in Deutschland eine Gesellschaft zu erzwingen, in der die nicht in ihrem Sinne „geklärten" Durchschnittsmenschen von den Scientology-Führern mit einer überlegenen Technologie „gemanagt" werden. Das von der SO angestrebte Verwaltungs-, Technologie- und Gerechtigkeitsverfahren soll keine Rechtsweggarantie, keine Gewährleistung des rechtlichen Gehörs und keinen Anspruch auf einen gesetzlichen und unabhängigen Richter kennen, ebenso keine an Gesetz und Recht gebundene Verwaltung. Bei Erreichung dieser Ziele würden die Grundrechte auf Schutz der Menschenwürde (Art. 1 GG), auf Schutz des allgemeinen Persönlichkeitsrechts (Art. 2 GG), auf Gleichheit vor dem Gesetz (Art. 3 GG) sowie das Demokratieprinzip (Art. 20 GG) außer Geltung gesetzt. Durch die zu erwartende Unterdrückung abweichender Meinungen wäre ebenso das in Art. 5 GG garantierte Grundrecht der freien Meinungsäußerung betroffen.

Belegt ist, daß die SO die Notwendigkeit der Lenkung der Regierungen nicht nur propagiert, sondern gezielt darauf hinarbeitet.

Bereits angesichts der bekannten weltweiten Aktivitäten und der nicht unerheblichen Mitgliederzahlen kann auch kein Zweifel bestehen, daß die beabsichtigte Beobachtung der SO verhältnismäßig im Sinne von § 3 LVSG ist.

Nach alledem ist davon auszugehen, daß insgesamt die gesetzlichen Voraussetzungen für die Maßnahme vorliegen.

6.4 Prüfungen beim Verfassungsschutz

Im Berichtszeitraum fanden mehrere örtliche Feststellungen beim Verfassungsschutz statt. Gegenstand der Prüfungen waren im wesentlichen verschiedene automatisiert geführte Dateien sowie personenbezogene Vorgänge und Sachakten. Alle zur Prüfung vorgesehenen Sachakten und Unterlagen waren für den LfD ungehindert zugänglich. Zu verschiedenen neu eingerichteten Dateien und Anlagen, wie z. B. der Vorgangsverwaltung, wurden Empfehlungen zur Verbesserung des Datenschutzes gegeben, denen weitgehend gefolgt worden ist.

Bei den Sicherheitsüberprüfungsakten galt es festzustellen, ob die bei ihrer letzten Überprüfung (siehe 14. Tb., Tz. 6.2) kritisierten, nicht erforderlichen und z. T. nicht verhältnismäßigen Speicherungen entfallen sind. Sowohl im Altbestand als auch in den inzwischen neu angelegten Akten wurden bei Stichproben keine derartigen Inhalte mehr festgestellt.

Insgesamt werden nach den Prüfungsergebnissen die datenschutzrechtlichen Bestimmungen weitgehend eingehalten.

Verschiedentlich wurden anhand von Eingaben alle entsprechenden Speicherungen sowie die Informationswege von und zu anderen Stellen durchgeprüft und auch unabhängig vom jeweils vorliegenden Fall die allgemeine Praxis untersucht. Auch insoweit ergab sich kein Grund zur Beanstandung.

7. Justiz

Kompetenzkonflikte

Mit dem Ministerium der Justiz besteht ein ungelöster Konflikt bezüglich folgender Fragen:

a) Unterliegen Dateien und automatisierte Verfahren der Bewährungshelfer, der Gerichtsvollzieher, des Schuldnerverzeichnisses und des Schreibdienstes der Gerichte der Kontrolle durch den LfD?

b) Haben Gerichte einen behördlichen Datenschutzbeauftragten zu bestimmen, wenn sie mehr als zehn Bedienstete haben, oder kommt es auf die Zahl der mit Personal- und Haushaltsangelegenheiten befaßten Bediensteten an (mit der Folge, daß nahezu kein Gericht im Lande einen eigenen internen Datenschutzbeauftragten zu bestellen hätte)?

Zu a:

Die datenschutzgesetzliche Regelung in § 24 Abs. 2 LDSG spricht davon, daß sich die Kontrolle des LfD im Bereich der Gerichte und des Rechnungshofs auf Verwaltungsangelegenheiten beschränkt. Auch an anderen Stellen im LDSG wird der Schutz der Unabhängigkeit der Gerichte und des Rechnungshofs durch den Begriff „Verwaltungsangelegenheiten" bezweckt (§§ 10 Abs. 4, 11 Abs. 5, 18 Abs. 6, 27 Abs. 1 und 28 Abs. 2 LDSG).

Diesbezüglich vertritt das Ministerium eine enge Interpretation, wonach nur Haushalts-, Personal- und Ausbildungsangelegenheiten zu den Verwaltungsangelegenheiten gehören. Das hat dazu geführt, daß weite Bereiche gerichtlichen Handelns, die kaum einen Bezug zur richterlichen Tätigkeit und gar keinen Bezug zur richterlichen Unabhängigkeit haben, andererseits aber bedeutsame Eingriffe in das informationelle Selbstbestimmungsrecht begründen, der Kontrolle des LfD entzogen sind. So vertritt das Ministerium die Auffassung, die gesamte Tätigkeit der Gerichtsvollzieher unter Einschluß der von diesen betriebenen automatisierten Datenverarbeitung (mit sensiblen Schuldnerdaten) sowie die gesamte Tätigkeit der Bewährungshelfer ebenfalls unter Einschluß ihrer EDV-Nutzung (mit sensiblen Probandendateien) gehöre nicht zum Bereich der Verwaltungsangelegenheiten und unterläge deshalb nicht der Kontrolltätigkeit des LfD. Diese Auffassung ist inzwischen vom Ministerium in einem Rundschreiben vom 10. September 1997 allen Gerichten und nachgeordneten Behörden mitgeteilt worden. Im Interesse einer effektiven Durchsetzung des informationellen Selbstbestimmungsrechtes ist es demgegenüber aber geboten, alle diejenigen Tätigkeiten auch im Bereich der Justiz der Datenschutzkontrolle zu unterwerfen, für die das Ministerium der Justiz Weisungsbefugnisse besitzt und für die letztlich auch eine politische Verantwortung des zuständigen Ministers besteht.

Eine Einigung konnte bislang mit dem Ministerium nicht erzielt werden. Angesichts der gesetzlichen Formulierung, die beide Interpretationen zuläßt, hat der LfD deshalb vorgeschlagen, das LDSG klarstellend in seinem Sinne zu ergänzen. Sein Vorschlag würde gleichzeitig aber auch gewährleisten, daß der verfassungsrechtlich gebotene Respekt vor der Unabhängigkeit der Rechtsprechung deutlich Ausdruck findet und diese Unabhängigkeit gewahrt bleibt.

Der Rechtsausschuß des Landtags hat angekündigt, sich mit dieser Frage anläßlich der ohnehin anstehenden Novellierung des LDSG (die zum Zweck der Anpassung an die EG-Datenschutzrichtlinie erfolgen muß) zu befassen.

Zu b:

Ein behördlicher Datenschutzbeauftragter muß bei Gerichten dann bestellt werden, wenn sich mindestens zehn Bedienstete nicht nur mit richterlichen, sondern auch mit „Verwaltungsangelegenheiten" befassen (§ 11 Abs. 5 LDSG). Auch hier ist also die Auslegung des Begriffs der „Verwaltungsangelegenheiten" entscheidend. Die Auffassung des Ministeriums führt dazu, daß nahezu in keinem Gericht des Landes ein interner Datenschutzbeauftragter zu bestellen ist. Es liegt auf der Hand, daß dies für den LfD nicht akzeptabel ist; auch hier sollte der Gesetzgeber für Klarheit sorgen.

7.1 Strafrecht

7.1.1 Ergänzung der Strafprozeßordnung um datenschutzrechtliche Grundnormen

Aus datenschutzrechtlicher Sicht ist es grundsätzlich sehr zu begrüßen, daß mit dem nunmehr vorgelegten Entwurf der Bundesregierung die Ergänzung der Strafprozeßordnung um Datenschutzregelungen zügig vorangetrieben werden soll, nachdem entsprechende Länderinitiativen lange Zeit nicht weiter gefördert worden sind.

Angesichts der Bedeutung der Strafprozeßordnung für das informationelle Selbstbestimmungsrecht aller Verfahrensbeteiligten und auch Dritter sollten die Beratungen jedoch sorgfältig und unter Nutzung der Erfahrungen insbesondere auch der Datenschutzbeauftragten des Bundes und der Länder erfolgen. Diese befassen sich seit Jahren mit dem Komplex des Datenschutzes im Strafverfahren sowie der polizeilichen und staatsanwaltschaftlichen Datenverarbeitung.

Zunächst ist zu betonen, daß der LfD das Grundanliegen des vorliegenden Gesetzentwurfs der Bundesregierung unterstützt, datenschutzrechtlich erforderliche Klarstellungen für das Strafverfahren zu formulieren. Dies betrifft insbesondere folgende Vorschriften des Entwurfs:

- die §§ 131 bis 131 c StPO-E, in denen gesetzliche Grundlagen für die öffentliche Fahndung nach Beschuldigten und Zeugen geschaffen werden sollen;
- § 163 f StPO-E, der die Zulässigkeit der längerfristigen Observation betrifft;
- die Ergänzung des § 160 StPO um die Berücksichtigung von gesetzlichen Verwendungsregelungen bei Ermittlungsmaßnahmen;
- die Berücksichtigung spezieller Verwendungsschranken im Rahmen des § 161 StPO;
- die detaillierten Regelungen über die Erteilung von Auskünften aus Akten und die Akteneinsicht in die §§ 474 bis 480 StPO-E;
- die Zweckänderungsregelung des § 481 StPO-E für präventiv-polizeiliche Zwecke;
- die Rückmeldungsregelung des § 482 StPO-E;
- die Dateiregelungen der §§ 493 bis 491 StPO-E einschließlich der Löschungsregelung in § 490 StPO-E;
- den Auskunftsanspruch des Betroffenen in § 492 StPO-E.

Von besonderer Bedeutung ist auch die Klarstellung in § 147 StPO-E, wonach ein Akteneinsichts- und Auskunftsanspruch des Beschuldigten auch nach Abschluß des Strafverfahrens besteht. Zu bedauern ist allerdings, daß eine Reihe von aus datenschutzrechtlicher Sicht regelungsbedürftigen Gegenständen in den vorliegenden Entwurf nicht einbezogen sind. So fehlen

- eine besondere Regelung der Auskunftserteilung bzw. Akteneinsicht, soweit die betroffenen Aktenteile besonders sensible Daten enthalten (etwa in psychiatrischen Gutachten);
- Regelungen für die Aufbewahrung, Aussonderung und Vernichtung der Akten der Strafverfolgungsbehörden;
- Regelungen für die Übermittlung von personenbezogenen Daten an die Medien.

Aus Sicht des LfD ist schließlich bedeutsam, daß datenschutzrechtliche Verbesserungen im Rahmen der Telefonüberwachung nicht aufgenommen worden sind. Es handelt sich hier insbesondere um folgende Forderungen der Datenschutzbeauftragten:

- Verbesserung der Berichtspflichten zur Gewinnung hinreichend aussagekräftiger Erkenntnisse und eine Auswertung der Überwachungsmaßnahmen im Hinblick auf ihren Erfolg, insbesondere Angaben über den Anlaß der Telefonüberwachung, die tatsächliche Dauer der Maßnahme, die Anzahl der überwachten Anschlüsse, den betroffenen Personenkreis sowie die Anzahl der ermittelten Verurteilten, aber auch der entlasteten Personen;
- Verkürzung der Anordnungsfrist des § 100 b StPO von drei Monaten auf einen Monat;
- konkretisierende Anforderungen für die Begründung der Anordnung der Überwachung des Fernmeldeverkehrs;
- Regelungen, die den Schutz besonderer Vertrauensverhältnisse – insbesondere von Verteidigergesprächen – verbessern;
- eine einschränkende Regelung der Aufzeichnung und Nutzung von Verbindungsdaten zu Strafverfolgungszwecken (in Ablösung des § 12 FAG);
- weitere Regelungen, die Eingriffsbefugnisse der Strafverfolgungsbehörden im Bereich der modernen Telekommunikation und der Informationstechnologie konkretisieren bzw. begründen (vgl. dazu die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22. Oktober 1996, „Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich", Anlage 10).

Der LfD hat zu den einzelnen Regelungen des Gesetzentwurfs detailliert Stellung genommen. Seine Vorschläge sind allerdings bislang nur zu einem geringen Teil im weiteren Gesetzgebungsverfahren berücksichtigt worden.

7.1.2 DNS-Analyse im Strafverfahren, DNS-Dateien

In die Strafprozeßordnung wurden Vorschriften eingefügt, die die Voraussetzungen des Einsatzes der Genanalyse im Strafverfahren regeln (§ 81 e StPO). Außerdem wurden Regelungen über den zulässigen Verwendungszweck der gewonnenen Daten geschaffen (§ 81 a Abs. 3 StPO). Es ist allerdings offengeblieben, ob und in welchem Umfang die erhobenen Informationen für die künftige Strafverfolgung gespeichert werden dürfen (etwa in landes- oder bundesweiten Datenbanken mit genetischen Fingerabdrücken).

Nach der einen Auffassung handelt es sich bei Analysedaten (und den daraus abgeleiteten Verformelungen), die allein der Zuordnung von Spuren dienen und die die nicht kodierenden Teile der DNS betreffen, um Daten, die keinerlei Aussage über die Information hinaus, daß die Spur mit Vergleichsmaterial identisch oder nicht identisch ist, zulassen. In diesem Fall wären aus der Sicht des LfD entsprechende Datenbanken wie automatisierte Fingerabdruckdateien (AFIS) zu beurteilen.

Nach anderer Auffassung dokumentieren auch solche Untersuchungsergebnisse zwangsläufig genetische Dispositionen. Angesichts der neuesten wissenschaftlichen Erkenntnisse auf diesem Gebiet müsse davon ausgegangen werden, daß Überschußinformationen in großem Umfang gespeichert würden. Dann aber wäre aus datenschutzrechtlicher Sicht eine restriktive Haltung gegenüber solchen Dateien geboten.

Die Datenschutzbeauftragten des Bundes und der Länder haben hierzu eine Entschließung getroffen („Genetische Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke", Anlage 12), in der die auch naturwissenschaftlich nicht eindeutig geklärte komplizierte derzeitige Situation berücksichtigt wird und angemessene Anforderungen an eine datenschutzgerechte Ausgestaltung einer hier erforderlichen Ergänzung der Strafprozeßordnung formuliert werden. Zu technisch-organisatorischen Fragen in diesem Zusammenhang s. u. Tz. 21.2.1.

Nunmehr sind Bestrebungen erkennbar, europaweit eine zentrale Datenbank mit DNS-Analyseergebnissen, insbesondere bezogen auf die Täter von Sexualdelikten, aufzubauen (Papier des Rates der Europäischen Union vom 17. März 1997, Nr. 6758/97 zum Austausch von DNS-Analyseergebnissen).

Diese Bestrebungen werden vom LfD aufmerksam beobachtet und mit dem Ziel begleitet, dabei die Anforderungen umzusetzen, die in der o. g. Entschließung formuliert worden sind.

7.1.3 Videoaufzeichnungen im Strafverfahren: Schutz der Opferzeugen oder Dokumentationsverbesserung?

Derzeit bestehen starke Bestrebungen, zum Zweck des Zeugenschutzes Videoaufzeichnungen von Zeugenvernehmungen gesetzlich zu gestatten bzw. vorzusehen.

Es existieren auf der Ebene des Bundes drei verschiedene Gesetzentwürfe zu diesem Thema:

- Gesetzentwurf der SPD-Fraktion vom 28. November 1995 zur Verbesserung der Rechtsstellung von Deliktsopfern und zum Einsatz von Videogeräten bei Zeugenvernehmungen in der Hauptverhandlung, Bundestagsdrucksache 13/3128;

- Gesetzentwurf des Bundesrates zur Änderung der Strafprozeßordnung (Gesetz zum Schutz kindlicher Zeugen) vom 19. Juni 1996, Bundestagsdrucksache 13/4983;

- Gesetzentwurf der Fraktionen der CDU/CSU und F.D.P. zur Änderung der Strafprozeßordnung (Gesetz zum Schutz von Zeugen bei Vernehmungen im Strafverfahren; Zeugenschutzgesetz – ZSchG) vom 11. März 1997, Bundesratsdrucksache 13/7165.

Der vorgeschlagene Einsatz von Videoaufzeichnungen der Zeugenaussagen berührt eine große Zahl datenschutzrechtlicher Fragen: Es ist in diesem Zusammenhang zu entscheiden, wer zu dem geschützten Personenkreis zählen soll, ob und in welchem Umfang der Einsatz der Videotechnik von der Einwilligung der Betroffenen bzw. ihrer gesetzlichen Vertreter abhängig sein soll, wer in welchem Stadium des Verfahrens den Einsatz der Videotechnik anordnen können soll, wer bei der Erstellung der Aufzeichnungen ein Anwesenheitsrecht besitzen soll, unter welchen Bedingungen und Voraussetzungen die aufgezeichneten Aufnahmen genutzt und verwertet werden sollen sowie für welche Zeit die Aufzeichnungen aufzubewahren sein sollen.

Die Konferenz der Datenschutzbeauftragten hat hierzu die in der Anlage 16 wiedergegebene Entschließung verabschiedet.

7.1.4 Telekommunikationsüberwachung

7.1.4.1 Defizite bei der Durchführung der Telefonüberwachung gem. § 100 a StPO

Grundsätzliche Defizite auf der Ebene der Gesetzgebung im Bereich der Telefonüberwachung wurden bereits im 15. Tb. (Tz. 7.5.3) erörtert. Bei der obigen Darstellung der datenschutzrechtlichen Defizite der Strafprozeßordnung (Tz. 7.1.1) war ebenfalls auf entsprechende datenschutzrechtliche Forderungen hinzuweisen.

Im Zusammenhang mit örtlichen Feststellungen in zwei Polizeipräsidien wurde ein Aspekt deutlich, der als Vollzugsdefizit bezeichnet werden kann: Die Abstimmung zwischen Polizeidienststellen und Staatsanwaltschaften bei der Löschung von Phone-Dateien funktionierte noch nicht ausreichend.

In beiden Polizeipräsidien wurde festgestellt, daß die Phone-Dateien, in denen Verbindungsdaten sowie Zusammenfassungen der Gesprächsinhalte gespeichert werden, über den Zeitpunkt der Löschung der Tonbänder und sonstigen Unterlagen hinaus weiter gespeichert wurden, weil die beteiligten Stellen über die Verantwortlichkeiten und die jeweilige tatsächliche Situation nicht ausreichend informiert waren. Wichtig ist, daß die Polizeidienststellen die Staatsanwaltschaften über die Existenz von Phone-Dateien unterrichten und daß die Staatsanwaltschaften ihrerseits mit der Anordnung der Vernichtung der sonstigen Unterlagen und der Löschung der Tonbänder auch die Löschung der Phone-Dateien anordnen.

Der LfD hat in diesem Zusammenhang sowohl das Justizministerium wie das Ministerium des Innern und für Sport auf die Unzulänglichkeiten hingewiesen. Das Justizministerium hat erklärt, die Angelegenheit werde auf Dienstbesprechungen erörtert, so daß künftig zu erwarten sei, daß entsprechende Fehler nicht mehr aufträten.

Der LfD hat außerdem ergänzende technisch-organisatorische Maßnahmen gefordert, um die Durchführung der Löschung nachvollziehbar und prüffähig zu machen. Über deren Umsetzung haben die beteiligten Ressorts noch nicht entschieden.

Anzumerken ist noch, daß das Justizministerium die in Rede stehenden Fälle zum Anlaß genommen hat, die seit 1991 bewährte Praxis der Anmeldung von Phone-Dateien beim LfD grundsätzlich in Frage zu stellen. Über die Fortführung der Anmeldepraxis ist derzeit noch nicht abschließend entschieden (vgl. Tz. 5.18).

Weitere Vollzugsdefizite bei der Durchführung von Telefonüberwachungsmaßnahmen ergaben sich anläßlich der Eingabe eines Betroffenen:

In dem zu beurteilenden Fall waren wegen einer sog. „Katalogtat" (einer Straftat, die nach § 100 a StPO die Anordnung einer Telefonüberwachung rechtfertigt) TÜ-Maßnahmen angeordnet und durchgeführt worden. Es ergab sich aus der TÜ aber kein Hinweis auf das tatsächliche Vorliegen eines solchen Straftatbestandes. Dennoch verwandte der zuständige Staatsanwalt die aufgezeichneten Gesprächsinhalte, um Zeugen daraus Vorhalte in ganz anderen strafrechtlichen Zusammenhängen zu machen (die den Vorwurf einer „Nichtkatalogtat" betrafen).

Die Nutzung von Informationen aus den aufgezeichneten Telefongesprächen zu Zeugenvorhalten war in diesem Fall unzulässig. Nach der Intervention des LfD hat der Ltd. Oberstaatsanwalt den zuständigen Dezernenten darauf hingewiesen.

Außerdem waren in diesem Fall Details aus der TÜ im Abschlußbericht der Polizei an die Staatsanwaltschaft wiedergegeben worden. Auch dadurch wurde nach Auffassung des LfD gegen das Gebot verstoßen, Erkenntnisse aus der Telefonüberwachung nur als Ermittlungsansatz, nicht dagegen darüber hinausgehend als Beweismittel und belastendes Material im weiteren Verfahren zu verwenden. Nachdem das wesentliche Ergebnis der Ermittlungen Bestandteil der Ermittlungsakte und damit jedem zugänglich wird, der befugt Akteneinsicht begehrt, im vorliegenden Fall auch dem ehemaligen Arbeitgeber des Beschuldigten, war die Verwertung der Ergebnisse der Telefonüberwachung in einer derart umfassenden und detaillierten (andererseits aber sicher auch aus Sicht des Betroffenen angreifbaren) Zusammenfassung als unzulässiger Eingriff in die Rechte des Beschuldigten zu bezeichnen.

Beide Gesichtspunkte will der Ltd. Oberstaatsanwalt anläßlich einer Dienstbesprechung mit der Polizei erörtern.

Von einer förmlichen Beanstandung konnte Abstand genommen werden, weil sich aus der Stellungnahme des Ltd. Oberstaatsanwalts ergibt, daß dieser Maßnahmen ergriffen hat, die sicherstellen sollen, daß künftig entsprechende Verstöße nicht mehr erfolgen.

7.1.4.2 Entwicklungen im Bereich der Telekommunikationsüberwachung

Die technische Weiterentwicklung der Informationsübermittlung und die als qualitative Änderungen im Bereich der Kommunikation zu bezeichnenden Neuentwicklungen (Internet, globale Vernetzung, Digitalisierung) führen zu stürmischen Entwicklungen im Bereich der technischen Abhörmöglichkeiten wie der diesbezüglichen Gesetzgebung.

Die Datenschutzbeauftragten des Bundes und der Länder haben in diesem Zusammenhang ein ausführliches Thesenpapier (unter Federführung des LfD Rheinland-Pfalz) erstellt (Anlage 17) und eine dazugehörige Entschließung gefaßt (Anlage 10).

7.1.4.3 Überwachung von Telefondaten in digitalen Mobilfunknetzen

Im Bereich des Landes bemüht sich der LfD um rechtzeitige Beteiligung bei der Einführung neuer Abhör- und Speichertechniken zur Überwachung der digitalen und mobilen Kommunikation, die sich derzeit größtenteils noch im Planungsstadium befinden.

Der Schwerpunkt der datenschutzrechtlichen Probleme liegt hier allerdings im technisch-organisatorischen Bereich; insoweit wird auf den Beitrag unter Tz. 21 des vorliegenden Berichts verwiesen.

7.1.4.4 Datenschutzgerechte Ausgestaltung der Fangschaltung

Wenn Menschen durch Telefonanrufe belästigt oder bedroht werden, haben sie die Möglichkeit, mit Hilfe einer Fangschaltung die verursachende Person herauszufinden (vgl. Tz. 19.6.3). Hierfür existiert nunmehr eine gesetzliche Grundlage (§ 8 TDSV). Diese Norm schreibt aber auch vor, daß alle diejenigen Personen und Stellen, die den Belästigten als Anrufende mitgeteilt worden sind, darüber unterrichtet werden (§ 8 Abs. 2 TDSV: regelmäßig sechs Wochen nach Abschluß der Fangschaltungsmaßnahme und nur dann, wenn kein überwiegendes Interesse der antragstellenden Person entgegensteht). Diese Pflicht der Netzbetreiber, den jeweiligen Anrufer oder die jeweilige Anruferin über die Auskunftserteilung an den Antragsteller oder die Antragstellerin zu unterrichten, ist Ausdruck des verfassungsrechtlichen Transparenzgebotes, wonach die Betroffenen grundsätzlich darüber unterrichtet sein bzw. werden müssen, welche Stellen ihre personenbezogenen Daten jeweils zur Kenntnis erhalten oder erhalten haben (zum Erfordernis grundrechtssichernder Maßnahmen für die anrufenden Personen in diesem Zusammenhang s. BVerfG, Fangschaltungsbeschluß, BVerfGE 85, 386).

Das Ministerium der Justiz ist der Auffassung, durch diese gesetzliche Verpflichtung werde die antragstellende Person unverhältnismäßig belastet. Es hat deshalb eine bundesweite Initiative zur Änderung dieses Rechtszustandes ergriffen. Die Datenschutzbeauftragten prüfen derzeit noch, ob nicht die Interessen der antragstellenden Personen i. S. v. § 8 TDSV, also derjenigen, die zur Abwehr bedrohender oder belästigender Anrufe die Auskunft über die Anrufer oder Anruferinnen beantragt haben, durch eine Anpassung bzw. Änderung der Verfahrensweise der Deutschen Telekom AG (und ggf. auch der anderen netzbetreibenden Gesellschaften) gewahrt werden können, ohne daß die oben angesprochenen grundsätzlich auch schutzwürdigen Interessen unbeteiligter Dritter hintanstehen müssen.

7.1.5 Opferdatenschutz in bezug auf psychologische Gutachten in Akten der Staatsanwaltschaften und Gerichte

Im 15. Tb. (Tz. 7.8) hat der LfD darauf hingewiesen, daß solche Informationen, die geeignet sind, das Opfer besonders zu gefährden, gesondert aufbewahrt werden sollten. Insbesondere sollten psychologische Gutachten über Opfer und Zeugen, aber auch über Beschuldigte in einem besonderen Aktenheft aufbewahrt werden. Dies hätte die erwünschte Folge, daß auch nach Abschluß des Strafverfahrens, wenn verschiedene Stellen Interesse an einer Einsichtnahme in die Akten bekunden, jeweils gesondert zu entscheiden wäre, ob auch diese besonders schutzbedürftigen Teile übersandt werden müssen.

Das Ministerium der Justiz hat darauf hingewirkt, daß die bundeseinheitliche Aktenordnung entsprechend geändert wurde. Danach müssen medizinische oder psychologische Gutachten, Berichte der Gerichtshilfe und der Jugendgerichtshilfe, Unterlagen über Telefonüberwachungen sowie andere Unterlagen, die von dem Staatsanwalt oder dem Richter besonders gekennzeichnet worden sind, in einem Sonderheft oder in sonstiger geeigneter Weise besonders aufbewahrt werden. Wenn die Akten an mit dem Strafverfahren nicht unmittelbar befaßte Stellen versandt werden oder wenn diesen Akteneinsicht gewährt wird, so sind diese Teile vorher aus den Akten herauszunehmen, es sei denn, daß der Staatsanwalt oder der Richter die Mitübersendung dieser Teile aus den besonderen Gründen des Einzelfalls ausdrücklich angeordnet hat.

Diese Regelung wird vom LfD ausdrücklich begrüßt. Sie trägt in einem sensiblen Bereich zur Verbesserung der Lage der Betroffenen bei.

7.1.6 Eintragung der Schuldunfähigkeit in das Bundeszentralregister

Die Frage, ob und auf welchem Wege Betroffene über die Eintragung ihrer eigenen Schuldunfähigkeit in das Bundeszentralregister zu informieren seien, wurde in der Vergangenheit bereits wiederholt sowohl auf der Ebene des Bundes wie auf der des Landes erörtert.

Nachdem die seit langem geforderte Reform des § 11 BZRG nach wie vor nicht vorangekommen ist und nachdem zumindest in den Bundesländern Berlin und Schleswig-Holstein auf der Ebene von Verwaltungsvorschriften Regelungen in diesem Zusammenhang getroffen worden sind, die die Rechte der Betroffenen stärker berücksichtigen, als dies bislang auch in Rheinland-Pfalz der Fall gewesen ist, hat der LfD die Problematik erneut aufgegriffen. Er hat das Ministerium der Justiz auf eine entsprechende Verfügung des Generalstaatsanwalts beim Landgericht Berlin, die nunmehr auch gleichlautend vom Generalstaatsanwalt bei dem Schleswig-Holsteinischen Oberlandesgericht übernommen worden ist, hingewiesen. Diese Verfügung berücksichtigt den seinerzeit von der Datenschutzkommission hervorgehobenen Umstand, daß nicht in allen Fällen eine Benachrichtigung der Betroffenen angezeigt ist.

Der LfD hat eine Übernahme der genannten Verfügung für Rheinland-Pfalz empfohlen.

Das Ministerium der Justiz hat daraufhin erklärt, es habe die nachgeordneten Behörden über den Inhalt dieser Verfügung unterrichtet und deren Anwendung empfohlen, halte eine verbindliche Übernahme aber für entbehrlich. Aus der Sicht des LfD sind normenklare Vorgaben zwar – auch im Blick auf die Personalfluktuation bei den betroffenen Stellen – vorzuziehen, er begrüßt aber die inhaltliche Übereinstimmung mit dem Ministerium.

7.1.7 Zustellung von Strafbefehlen und sonstigen gerichtlichen Schriftstücken an Wohnungslose

Ein Amtsgericht des Landes stand vor der Schwierigkeit, einem Wohnungslosen einen Strafbefehl zu übersenden. Dem Amtsgericht war als Kontaktadresse nur eine Beratungsstelle eines Diakonischen Werkes bekannt, bei der der Wohnungslose häufiger vorsprach. Es übersandte also das entsprechende Schriftstück mit einem Empfangsbekenntnis an die Diakonische Beratungsstelle. Diese Stelle beschwerte sich beim LfD und erklärte, es sei überflüssig, daß ihr der Inhalt des Strafbefehls zur Kenntnis gegeben würde.

Es ergab sich, daß hier ein Versäumnis der Geschäftsstelle des Amtsgerichts vorlag. Üblicherweise wird in solchen Fällen für das zuzustellende Schriftstück selbst ein zweiter Umschlag verwendet. Dies wurde vorliegend versäumt. Der LfD wies die Geschäftsstelle des Amtsgerichts darauf hin, hier künftig sorgfältiger zu verfahren. Dies wurde zugesagt. Von einer Beanstandung konnte deshalb abgesehen werden.

Der grundsätzlich nicht sehr bedeutsame Vorgang wird deshalb berichtet, um deutlich zu machen, daß gerade auch im Bereich der gerichtlichen Geschäftsstellen datenschutzrechtliche Schwachpunkte auftreten können und daß hier die Tätigkeit des LfD keinesfalls mit der richterlichen Unabhängigkeit kollidiert.

7.2 Zivilrecht

7.2.1 Übermittlung eines zivilgerichtlichen Urteils an die Ordnungsbehörde

Ein Beschwerdeführer war vom Amtsgericht zu Schadensersatz verurteilt worden, weil sein Hund einen Passanten angefallen hatte. Daraufhin erhielt er Post vom Ordnungsamt der Verbandsgemeinde, das überprüfen wollte, ob Auflagen wegen der Hundehaltung auszusprechen waren.

Der Beschwerdeführer war der Meinung, das Amtsgericht hätte hier unzulässigerweise das Urteil übermittelt. Der LfD hat die Situation wie folgt beurteilt:

Das Amtsgericht war nach dem vorgetragenen Sachverhalt unter verschiedenen rechtlichen Gesichtspunkten befugt, Unterlagen aus dem Zivilverfahren an die Ordnungsbehörde der Verbandsgemeinde zu übermitteln.

Wenn eine Anforderung der Ordnungsbehörde vorgelegen haben sollte, wäre Rechtsgrundlage für die Übermittlung entsprechender Unterlagen aus dem zivilgerichtlichen Verfahren § 299 Abs. 2 ZPO gewesen. Danach dürfen Abschriften aus Verfahrensakten der Zivilgerichte dann erteilt werden, wenn der Empfänger ein rechtliches Interesse geltend macht. Rechtliche Interessen sind solche, deren Durchsetzung von der Rechtsordnung vorgesehen ist. Die Durchführung eines ordnungsbehördlichen Verfahrens gegen Hundehalter zum Zweck der Gefahrenabwehr ist gesetzlich geregelt (§§ 1 ff. POG sowie Landesverordnung zur Abwehr von Gefahren durch gefährliche Hunde, GVBl. 92, 374). Die Durchführung eines solchen Verfahrens begründet ein rechtliches Interesse im Sinne der genannten gesetzlichen Regelung.

Möglich ist auch, daß entsprechende Unterlagen von Amts wegen durch das Amtsgericht an das Ordnungsamt übermittelt worden sind. Dies ist gem. Nr. 2 der Anordnung über Mitteilungen in Zivilsachen dann zulässig, wenn der Richter der Auffassung ist, daß diese Mitteilung wegen eines besonderen öffentlichen Interesses unerläßlich ist und wenn er keine dagegenstehenden erheblichen Bedenken erkennt.

Im vorliegenden Zusammenhang waren für den LfD keine Gesichtspunkte ersichtlich, die diese Entscheidung hätten unzulässig erscheinen lassen. Diese Beurteilung liegt deshalb in seiner Zuständigkeit, weil es sich bei der Informationsübermittlung durch das Gericht – nach Abschluß des gerichtlichen Verfahrens – um eine Maßnahme der Gerichtsverwaltung gehandelt hat.

Schließlich ist es denkbar, daß der Kläger in dem Zivilrechtsstreit die Unterlagen an die Ordnungsbehörde weitergeleitet hat. Auch dies wäre datenschutzrechtlich zulässig gewesen.

Damit steht fest, daß unabhängig davon, welche der vorstehend genannten Übermittlungsalternativen tatsächlich vorgelegen hat, die Urteilsweitergabe datenschutzrechtlich zulässig war.

Es blieb zu prüfen, ob die Ordnungsbehörde auch erhebungsbefugt gewesen wäre, d. h. ob sie das zivilgerichtliche Urteil beim Amtsgericht hätte anfordern dürfen. Die maßgeblichen Voraussetzungen hierfür ergeben sich aus § 25 a Abs. 1 Nr. 1 und 4 i. V. m. Abs. 1 a POG. Danach darf die Ordnungsbehörde auch ohne Mitwirkung des Betroffenen selbst Daten bei Dritten erheben, wenn dies zur Abwehr einer im Einzelfall bestehenden Gefahr oder zur Erfüllung der Aufgaben nach der oben zitierten Rechtsverordnung über gefährliche Hunde erforderlich ist. Die in Rede stehenden Unterlagen waren zur Entscheidungsfindung in diesem Zusammenhang erforderlich.

Unter den gleichen genannten Voraussetzungen des § 25 a POG, die hier vorlagen, darf die Ordnungsbehörde die in Rede stehenden Unterlagen auch in ihren Akten aufbewahren („speichern"). Unerheblich ist dabei, ob sich die Ordnungsbehörde für ihre Entscheidungen ausschließlich auf diese Unterlagen stützen darf oder ob sie auch andere Erkenntnisquellen heranziehen muß. Jedenfalls sind zivilgerichtliche Unterlagen in diesem Zusammenhang grundsätzlich verwertbar.

Vor diesem Hintergrund hat der LfD keinen Anlaß gesehen, das Verhalten der beteiligten öffentlichen Stellen zu beanstanden.

7.2.2 Datenschutzfragen im Zusammenhang mit dem Schuldnerverzeichnis

Im Berichtszeitraum ist es erneut vorgekommen, daß sich Bürger an den LfD gewandt haben, die im Schuldnerverzeichnis wegen Ablegung der eidesstattlichen Versicherung eingetragen waren und die in der Folge Werbematerial von sog. „Kredithaien" erhalten haben (s. auch 12. Tb., Tz. 7.8.2; 13. Tb., Tz. 7.5).

Es stellt sich in diesen Fällen die Frage, woher diese Kreditvermittler – die nicht selten unseriös arbeiten – die Daten erhalten haben.

Bemühungen der zuständigen Datenschutzaufsichtsbehörden für den privaten Bereich ergaben kein konkretes Ergebnis: Die Kreditvermittler beriefen sich zum Teil darauf, daß sie die Daten von einem Adressenhändler erhalten und nur zur einmaligen Verwendung genutzt hätten. Diese Daten seien bei ihnen nicht gespeichert worden, so daß es nicht nachvollziehbar sei, woher sie die Daten im konkreten Fall bezogen hätten. Die Adressenhändler, die als Lieferanten genannt wurden, hatten sämtlich ihren Sitz im Ausland (Florida, Kleinwalsertal/Österreich, Schweiz).

Zum Teil hatten die Kreditvermittler selbst ihren Sitz im Ausland (z. B. in Minsk, Weißrußland).

Es wird deutlich, daß sich der Weg der Daten vom Schuldnerverzeichnis zu den nutzenden Kreditvermittlern grundsätzlich nicht aufklären läßt. Daß hierzu die Ausdrucke aus dem Schuldnerverzeichnis genutzt werden, die von den Industrie- und Handelskammern für ihre Mitgliedsbetriebe herausgegeben werden, läßt sich nicht mit Sicherheit belegen.

Es scheint so zu sein, daß in diesem Fall mißbräuchliche Verwendungen nur dadurch verhindert werden könnten, daß eine besondere Straf- bzw. Bußgelddrohung gegen die Letztnutzer gesetzlich verankert wird. Hierfür wäre der Bundesgesetzgeber zuständig. Aus der Sicht des LfD sollten entsprechende Überlegungen vertieft geprüft werden.

7.2.3 Regelmitteilungen der Grundbuchämter an die Nachlaßgerichte

Aufgrund einer Eingabe ist dem LfD zur Kenntnis gelangt, daß jedenfalls im Bezirk des Oberlandesgerichts Zweibrücken zum Zweck der nachträglichen Erhöhung eines nach § 19 Abs. 2 Kostenordnung festgestellten Geschäftswertes anläßlich einer Grundbuchumschreibung (aus Anlaß eines Erbfalles) wie folgt verfahren wird:

- Das Nachlaßgericht teilt bei Übersendung der Unterlagen zur Grundbuchberichtigung dem Grundbuchamt mit, welcher Wert des Grundstücks der Kostenberechnung zugrunde gelegt wurde.

- Das Grundbuchamt gibt dem Nachlaßgericht in den Fällen Mitteilung, in denen aus den Grundakten bereits zum Zeitpunkt des Erbfalls oder innerhalb eines Kalenderjahres nach Abschluß des Nachlaßverfahrens ein Grundstückswert ersichtlich ist, der wesentlich über dem vom Nachlaßgericht angenommenen Wert liegt.

Nur das Land Rheinland-Pfalz verfährt in dieser Weise; andere Bundesländer verzichten auf diese Datenübermittlungen.

Die datenschutzrechtliche Prüfung ergab, daß für diese Verfahrensweise eine ausreichende gesetzliche Grundlage im LDSG vorhanden ist:

Zunächst war zu prüfen, ob das Nachlaßgericht dem Grundbuchamt bei der Übersendung der Unterlagen zur Grundbuchberichtigung den dort bekannten Wert des Grundbesitzes mitteilen darf.

Dies ist der Fall, weil die Nutzung der Information über den Wert des Grundbesitzes durch das Grundbuchamt zum Zweck der Gebührenberechnung erforderlich ist, um die Aufgaben des Grundbuchamtes im Zusammenhang mit der Umschreibung zu erfüllen und weil diese Datenweitergabe offensichtlich im Interesse der Betroffenen liegt und kein Grund zur Annahme besteht, daß sie in Kenntnis des Zwecks ihre Einwilligung verweigern würden (§ 12 Abs. 4 Nr. 6 i. V. m. § 13 Abs. 2 Nr. 1 LDSG).

Wenn sich aus den Grundakten ein wesentlich höherer Wert ergibt, teilt das Grundbuchamt dies dem Nachlaßgericht mit. Die Weitergabe dieser Daten ist also auf die Fälle beschränkt, in denen aufgrund der erkannten Wertabweichungen ein Tätigwerden des Nachlaßgerichts zu erwarten ist. Überflüssige Datenweitergaben erfolgen damit nicht. Die praktizierten Übermittlungen sind gem. § 13 Abs. 2 Nr. 1 i. V. m. § 12 Abs. 4 Nr. 3 LDSG zulässig.

7.2.4 Vollzugsdefizite bei Mitteilungen in Zivilsachen

In einem Amtsgericht des Landes wurden örtliche Feststellungen durchgeführt, die in erster Linie die Umsetzung der Anordnung über Mitteilungen in Zivilsachen zum Gegenstand hatten. Folgendes hat sich ergeben:

a) Bei Mitteilungen an andere öffentliche Stellen nach der Anordnung über Mitteilungen in Zivilsachen wurde vom Amtsgericht ein Formularanschreiben verwandt. Dieses enthielt folgende Angaben:

„– Absenderangabe (Bezeichnung des Amtsgerichts) mit Geschäftsnummer;

– Betreff;
– Text:
Sehr geehrte
Beigefügte Abschrift erhalten Sie mit der Bitte um Kenntnisnahme und evtl. Stellungnahme. Alle Eingaben an das Gericht sind in dreifacher Ausfertigung einzureichen.
Mit freundlichen Grüßen
Auf Anordnung"

Dieses Anschreiben entspricht nicht der Vorgabe der Nr. 3 Abs. 2 erster Teil, allgemeine Vorschriften der Anordnungen über Mitteilungen in Zivilsachen. Danach ist die jeweilige Vorschrift im Anschreiben zu zitieren, die Grundlage der Mitteilung ist. Dies ist keine bloße Formalie. Damit wird nämlich für den Empfänger der Mitteilung die Erfüllung seiner Pflicht, die Zweckbindung der Mitteilung zu beachten, erleichtert (diese Pflicht besteht gem. § 14 Abs. 3 Satz 1 LDSG).

Das Amtsgericht sicherte zu, das Anschreiben künftig um diese Information zu ergänzen.

b) Bezüglich des Vollzuges der Mitteilung gem. der Anordnungen über Mitteilungen in Zivilsachen IV/1 (Unterrichtung der Sozialämter über Räumungsklagen wegen Mietzinsverzuges) war festzustellen, daß durch das Amtsgericht jeweils die gesamte Klageschrift an das in Betracht kommende Sozialamt übersandt wurde. Dies führte in erheblichem Umfang zu überflüssigen Datenübermittlungen. Diese Verfahrensweise widerspricht auch dem ausdrücklichen Wortlaut der genannten Regelung. Danach sind nur wenige Informationen aus der Klageschrift in ein vorgegebenes Formblatt zu übernehmen. Dieses Formblatt wurde vom Amtsgericht bislang nicht eingesetzt.

Das Amtsgericht erklärte, künftig die Übermittlungen entsprechend zu beschränken.

7.3 Datenschutzfragen beim Vollzug des Betreuungsrechts

Eine Kreisverwaltung fragte an, ob sie dem Betreuer eines Grundeigentümers, der im größeren Umfang Ländereien verpachtet hatte, Auskünfte aus der landwirtschaftlichen Betriebsdatenbank darüber geben müßte, wer jeweils Pächter war. Bei dem Betreuten waren die Unterlagen nicht mehr vorhanden. Der LfD beurteilte dies wie folgt:

Zunächst war festzustellen, daß es sich bei der vom Betreuer begehrten Datenweitergabe im vorliegenden Zusammenhang nicht um eine Datenübermittlung i. S. v. § 3 Abs. 2 Nr. 4 LDSG handelte. Danach ist Übermitteln das Bekanntgeben oder sonstige Offenbaren personenbezogener Daten an Dritte. Der Betreuer ist jedoch nicht Dritter im Sinne des Gesetzes, er ist vielmehr in seinem Aufgabenkreis der Vertreter des Betreuten (§ 1902 BGB). Der Vertreter wiederum handelt im Namen des Vertretenen mit Wirkung unmittelbar für und gegen den Vertretenen (§ 164 Abs. 1 BGB).

Damit war der dargestellte Sachverhalt genauso zu beurteilen, wie wenn anstelle des Betreuers die betreute Person selbst nach den Pächtern ihrer Parzellen gefragt hätte.

Die Information, wer als Pächter einer bestimmten Person in der landwirtschaftlichen Betriebsdatenbank gespeichert ist, ist eine Information nicht nur über den Pächter, sondern ebenso eine Information über den Verpächter. Insoweit kann also der Verpächter im Rahmen seines allgemeinen Auskunftsanspruchs gem. § 18 Abs. 1 LDSG verlangen, daß ihm mitgeteilt wird, wer als Pächter seiner Parzellen in der Datenbank gespeichert ist.

Die Tatsache, daß diese Informationen auch solche sind, die den Pächter betreffen, steht dieser Überlegung nicht entgegen. Insoweit regelt § 18 Abs. 3 Nr. 3 LDSG abschließend, wann ein Drittbezug die Auskunftserteilung an den Betroffenen selbst hindert: Dies ist nur dann der Fall, wenn die schutzwürdigen Interessen der betroffenen Dritten überwiegen.

Im vorliegenden Fall war kein Gesichtspunkt ersichtlich, nach dem es ein schutzwürdiges Interesse der Pächter wäre, ihrem Verpächter gegenüber die Pächterstellung zu verheimlichen. Der Betreuer hatte also einen Anspruch auf die begehrten Auskünfte.

Der LfD hat außerdem auf die Anfrage eines Landrats hin ausführlich zu der Frage Stellung genommen, welche Datenerhebungen durch die Kreisverwaltung bei den Betreuungsvereinen zulässig sind, um die Fördermittel gerecht zu verteilen.

7.4 Organisatorisch-technischer Datenschutz in der Justiz

7.4.1 EDV-Einsatz im Bereich der Justiz

Die Landesregierung hat den Landtag über die „Straffung der Justizstrukturen", Landtagsdrucksache 13/885 vom 11. Dezember 1996, ausführlich unterrichtet.

Der Abschnitt „EDV" war und ist naturgemäß für den LfD von besonderem Interesse. Die Zielvorstellungen des EDV-Einsatzes werden dort in wünschenswerter Klarheit dargestellt. Ein vergleichbarer Überblick über den Ist-Zustand der EDV-Ausstattung sowie die geplante Entwicklung im gesamten Zuständigkeitsbereich des Ministeriums der Justiz stand dem LfD in dieser Form bislang noch nicht zur Verfügung.

Bei dieser Gelegenheit ist deutlich geworden, daß der Informationsstand des LfD über den EDV-Einsatz in der Justiz in einigen aus datenschutzrechtlicher Sicht durchaus bedeutsamen Bereichen nicht ausreichend sein dürfte.

So ist er über die Organisation und die technische Ausstattung bei der Textverarbeitung im Bereich der Gerichte wie auch bei den zehn staatsanwaltschaftlichen Behörden derzeit wohl nur unzureichend unterrichtet. Ihm liegen – nach einer entsprechenden Auswertung des Verfahrensregisters – insofern aus dem Bereich der Gerichte nur elf Anmeldungen vor.

Aus dem Bereich der Staatsanwaltschaften sind – außer der Textverarbeitungskomponente des angemeldeten CUST-Systems – keinerlei gesonderte Anmeldungen von Textverarbeitungsverfahren im Datenschutzregister vorhanden.

Nach der eingangs genannten Drucksache wird an 38 Gerichten (28 Amts-, acht Land- und zwei Oberlandesgerichten) sowie bei allen zehn staatsanwaltschaftlichen Behörden die Textverarbeitung eingesetzt.

Wenn moderne automatisierte Textverarbeitungssysteme mit Dokumentationsfunktion (längerfristigen Speicherungen) und textübergreifenden Recherchemöglichkeiten eingesetzt werden, ergeben sich auch in diesem Bereich durchaus datenschutzrechtliche Anforderungen (aus dem LDSG insbesondere die Pflichten aus § 9), deren Einhaltung nicht nur aus formalen Gründen erforderlich ist, sondern die realen Gefahren für das Persönlichkeitsrecht der Betroffenen entgegenwirken.

Der LfD hat deshalb mit Schreiben vom Januar 1997 das Ministerium der Justiz gebeten, ggf. zu veranlassen, daß die entsprechenden Anmeldungen gem. § 27 LDSG nachgeholt werden. Nach sechs Monaten antwortete das Ministerium (mit Schreiben vom 7. Oktober 1997) und erklärte hierzu, auch bei den neuesten Verfahren würden personenbezogene Daten nicht längerfristig zu Dokumentationszwecken gespeichert, sondern direkt nach Beendigung des Verfahrens vom System gelöscht.

Damit besteht auch nach Auffassung des LfD für diese Verfahren derzeit keine Anmeldepflicht.

Bedeutsamer für das informationelle Selbstbestimmungsrecht der Betroffenen ist selbstverständlich die Automation der bisher manuell gespeicherten Bürgerdaten in den Registern. In diesem Zusammenhang ist die offensichtlich geplante Automatisierung der Schuldnerverzeichnisse von besonderer Bedeutung, da es in diesen Bereichen in der Vergangenheit wiederholt Unzuträglichkeiten (bei Verwechslungsfällen) gegeben hat. Insofern hat der LfD um zeitnahe und umfassende Beteiligung an der weiteren Entwicklung gebeten. Das Ministerium hat in seinem o. g. Schreiben (vom 7. Oktober 1997) hierzu mitgeteilt, zwischenzeitlich seien die Programmierarbeiten für das automatisierte Schuldnerverzeichnis im Rahmen des Gesamtprojekts „MAJA" abgeschlossen. Derzeit würden umfangreiche Anwendungstests durchgeführt. Ergänzend hat das Ministerium hierzu das umfangreiche Fachkonzept übersandt, das nunmehr aus Datenschutzsicht beurteilt werden muß.

Ein Bereich, in dem die Informationen des LfD ebenfalls unzureichend sein dürften, ist der PC-Einsatz an Richter- und Staatsanwaltsarbeitsplätzen. Nach dem Bericht wird zwischenzeitlich an mehr als 100 derartigen Arbeitsplätzen ein PC eingesetzt. Welche technischen und organisatorischen Datenschutzmaßnahmen dort jeweils zum Einsatz kommen und welche Daten von welchem Sensibilitätsgrad dort automatisiert verarbeitet werden, ist dem LfD konkret nicht bekannt. Bezüglich der Einsatzbedingungen und Einsatzfelder des PC-Einsatzes bei Richtern hat er das Ministerium um aktuelle allgemeine Informationen gebeten. Bezüglich des PC-Einsatzes bei Staatsanwälten hat er gebeten, die Anmeldung der eingesetzten Verfahren nach § 27 LDSG zu veranlassen, soweit dies noch nicht erfolgt ist.

Hierzu hat das Ministerium mitgeteilt, seiner Auffassung nach seien lediglich Verfahren, in denen personenbezogene Daten automatisiert verarbeitet werden, generell anmeldepflichtig. Daraus folge, daß nicht relevant sei, welche technischen und organisatorischen Datenschutzmaßnahmen am einzelnen Arbeitsplatz zum Einsatz kämen oder welche Daten von welchem Sensibilitätsgrad dort automatisiert verarbeitet werden könnten.

Im übrigen sei die Anmeldung dieser Verfahren Sache der jeweiligen datenverarbeitenden Stelle. Aus Anlaß der Anfrage des LfD habe das Ministerium jedoch alle nachgeordneten Behörden aufgefordert, etwaige nicht angemeldete Verfahren, bei denen die Voraussetzungen des LDSG vorlägen, auf dem Dienstweg anzumelden.

Nähere Auskünfte auch allgemeiner Art zum PC-Einsatz bei Richtern hat das Ministerium unter Hinweis darauf, daß alle hier eingesetzten PC zur Unterstützung der Richter in ihrer rechtsprechenden unabhängigen Tätigkeit dienen würden, abgelehnt.

Der LfD wird das Ministerium der Justiz darauf hinweisen, daß es selbstverständlich Teil der Verfahrensbeschreibung ist, die Art der jeweils gespeicherten Daten mitzuteilen. Auch die jeweiligen Maßnahmen des technischen und organisatorischen Datenschutzes sind bezogen auf den einzelnen Arbeitsplatz als Teil der Verfahrensbeschreibung anzumelden.

Die richterliche Unabhängigkeit hindert zudem nicht, den LfD über die Einsatzbedingungen und Einsatzzwecke der Automation an Richterarbeitsplätzen in allgemeiner Form zu unterrichten.

Zum Projekt „MAJA" (Mainzer automatisierte Justiz-Automation), dessen Einführung dem Bericht zufolge mit großem Nachdruck fortgeführt werden soll, hat der LfD um zeitnahe Information über den Verfahrensfortschritt und insbesondere auch um Mitteilung gebeten, ob und in welchem Umfang sowie wann seine diesbezüglichen Empfehlungen aus seinem Schreiben vom 24. November 1995 umgesetzt worden sind bzw. umgesetzt werden. Mit Schreiben vom 7. Oktober 1997 hat das Mininsterium der Justiz im einzelnen zu den Empfehlungen des LfD Stellung genommen. Eine datenschutzrechtliche Bewertung wird derzeit durchgeführt.

In bezug auf die längerfristig geplanten Projekte ist die zentrale Datei aller staatsanwaltschaftlichen Ermittlungsverfahren von erheblicher datenschutzrechtlicher Bedeutung. Hier hat der LfD um zeitnahe Beteiligung an der Entwicklung gebeten.

Die Bedeutung datenschutzrechtlicher Überlegungen auch für die Justiz von Rheinland-Pfalz wird durch die Aussage des Berichts deutlich, daß derzeit mit EDV-Systemen insgesamt mehr als 2 800 Bedienstete arbeiten.

Insgesamt betont der LfD, daß er seine Aufgabe keinesfalls darin sieht, automationshemmend auf die dringend erforderlichen Rationalisierungsbestrebungen der Justiz einzuwirken. Im Gegenteil: Aus seiner Sicht ist eine datenschutzverträgliche Gestaltung automatisierter Systeme Voraussetzung dafür, daß diese reibungslos, effektiv und von Bürgern wie Bediensteten akzeptiert den Arbeitsablauf der Justiz in allen Bereichen unterstützen können.

7.4.2 Zustellungsreformgesetz

Das Justizministerium übersandte dem LfD auf dessen Bitte hin den vom Bundesministerium der Justiz erstellten Diskussionsentwurf eines Gesetzes zur Reform des Verfahrens bei Zustellung im gerichtlichen Verfahren (Zustellungsreformgesetz).

Der LfD hat aus datenschutzrechtlicher Sicht begrüßt, daß eines der wesentlichen Ziele, die mit dem Gesetzentwurf verfolgt werden sollen, die stärkere Berücksichtigung datenschutzrechtlicher Gesichtspunkte insbesondere bei der Ersatzzustellung und der öffentlichen Zustellung ist. Bereits im derzeitigen frühen Stadium der Gesetzgebung hat er auf eine Reihe von datenschutzrechtlich relevanten Gesichtspunkten hingewiesen, die aus seiner Sicht im Gesetzgebungsverfahren berücksichtigt werden sollten.

Der Fortgang des Gesetzgebungsverfahrens ist zur Zeit nicht absehbar.

7.4.3 Zugang von Mitarbeitern privater Unternehmen zu Archivräumen eines Gerichtsgebäudes

Aufsehen erregten Fernseh- und Presseberichte, wonach Handwerker – zu denen auch Freigänger aus einer JVA des Landes gehörten – während der Renovierung eines Gerichtsgebäudes nicht nur auf Strafverfahrensakten, sondern auch auf Tonbänder aus TÜ-Maßnahmen Zugriff hatten.

Hierzu hat der LfD örtliche Feststellungen in den betroffenen gemeinsamen Räumlichkeiten des Landgerichts und der Staatsanwaltschaft durchgeführt.

Maßstab seiner Prüfung war die Regelung des § 9 Abs. 4 i. V. m. Abs. 1 LDSG. Danach sind bei der Aufbewahrung von Akten Maßnahmen zu treffen, die verhindern, daß Unbefugte auf diese Daten zugreifen können. Erforderlich sind entsprechende Maßnahmen, wenn ihr Aufwand unter Berücksichtigung der Art der zu schützenden personenbezogenen Daten und ihrer Verwendung in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Der LfD hat die Auffassung vertreten, daß die vom Landgericht als hausverwaltender Stelle und vom zuständigen Staatsbauamt als Auftraggeber der privaten Unternehmen getroffenen Maßnahmen nicht ausreichend waren.

Zum einen hätte der Aktenbestand nach Möglichkeit vor der Durchführung der Bauarbeiten reduziert werden müssen. Dazu hätte es gehört, die Akten, deren Vernichtungszeitpunkt erreicht war, auszusondern und zu vernichten. Außerdem hätte das Staatsbauamt die Justizstellen darüber unterrichten müssen, daß die beauftragten Unternehmen Freigänger einsetzen. Schließlich hätte auch angesichts der Größe, Unübersichtlichkeit und Zahl der eingesetzten Mitarbeiter privater Unternehmen ein Justizbediensteter (u. U. auch eine ad hoc eingestellte Zusatzkraft) Bewachungsaufgaben wahrnehmen müssen.

Diese Gesichtspunkte hat der LfD sowohl dem Ministerium der Justiz als auch dem Ministerium der Finanzen als dem für die Staatsbauverwaltung zuständigen Ressort mitgeteilt. Das Finanzministerium hat sich der Auffassung des LfD angeschlossen, während das Justizministerium die Auffassung vertritt, das Resozialisierungsinteresse sei vorrangig und verbiete die Unterrichtung über den Freigängereinsatz; Fälle wie der vorliegende seien letztlich nicht verhinderbar.

Anläßlich örtlicher Feststellungen ergab sich bei einem anderen Amtsgericht, daß die einzelnen Kellerräume, in denen Akten lagerten, bis auf eine Ausnahme verschlossen waren. In dem unverschlossenen Kellerraum allerdings lagerten sämtliche Nachlaßakten des Amtsgerichts. Es war Besuchern möglich, unbeobachtet in diesen Raum zu gelangen.

Unter diesen Voraussetzungen war das Nichtverschließen dieses Archivraumes im Keller des Amtsgerichts in der Zeit, in der dort kein Bediensteter tätig war, als Verstoß gegen § 9 Abs. 4 LDSG zu werten. Der Amtsgerichtsdirektor wies die zuständigen Bediensteten auf ihre insoweit bestehenden Sorgfaltspflichten hin.

7.5 Neufassung der Presserichtlinien

Die Frage, unter welchen Voraussetzungen und in welchem Umfang die Justiz (insbesondere Gerichte und Staatsanwaltschaften) die Presse und andere Medien über Einzelfälle informieren darf, berührt den Datenschutz und macht ein gesetzliches Defizit deutlich:

Nach dem LDSG wäre die Übermittlung personenbezogener Daten an die Presse grundsätzlich nicht zulässig (§ 16 LDSG, anzuwenden nach dem Wortlaut des § 4 Abs. 2 Nr. 2 Landespressegesetz; vgl. den Sächsischen LfD, NJW 96, 977).

Aber auch bei der Zugrundelegung des Landespressegesetzes (§ 4) bleibt die Rechtslage unbefriedigend: Danach nämlich ist im Einzelfall das Informationsinteresse der Öffentlichkeit mit den schutzwürdigen Interessen der Betroffenen abzuwägen. Diese Regelung ist für die Praxis stark ausfüllungsbedürftig und läßt aus der Sicht des LfD zu viele Fragen offen. Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb gefordert, für die Unterrichtung der Öffentlichkeit über Strafverfahren eine normenklare bereichsspezifische Rechtsgrundlage zu schaffen (vgl. die Entschließung vom 9. November 1995 zu „Forderungen an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien", Anlage 6).

Aus der Sicht des LfD sollte zumindest bis zum Erlaß einer entsprechenden gesetzlichen Regelung die Verwaltungsvorschrift des Landes über die Unterrichtung der Presse durch Justizbehörden aus dem Jahr 1985 um folgende Punkte ergänzt werden:

- Es sollte klargestellt werden, daß die Übermittlung personenbezogener Daten an die Medien nur ausnahmsweise gerechtfertigt ist, wenn das Verfahren gerade im Hinblick auf die Person des Betroffenen oder die besonderen Umstände für die Öffentlichkeit von überwiegendem Interesse ist.

- Bei Personen, die keine Veranlassung gegeben haben, daß ihre persönlichen Lebensumstände in der Öffentlichkeit bekanntgemacht werden, kommt die Übermittlung personenbezogener Daten an die Medien grundsätzlich nicht in Betracht.

- Bei der Entscheidung, ob und in welchem Umfang personenbezogene Daten an die Medien übermittelt werden, sind die schutzwürdigen Belange der Betroffenen zu berücksichtigen. Dazu zählen insbesondere die privaten und beruflichen Folgen für die Beteiligten.

- Grundsätzlich sind in Auskünfte und Erklärungen über das Verfahren keine Namen und sonstige personenbezogene Angaben, die einzelne Personen bestimmbar machen, aufzunehmen. Vor allem bei Hinweisen auf den Wohnort, das Alter, den Beruf und die familiären Verhältnisse oder sonstigen sozialen Bindungen (z. B. Partei- oder Vereinsmitgliedschaft) ist zu prüfen, inwieweit dadurch eine Identifizierung des Betroffenen möglich wird.

- Personenbezogene Daten dürfen nicht übermittelt werden, wenn besondere bundes- oder landesgesetzliche Verwendungsregelungen entgegenstehen.

- Wegen des überragenden Schutzes von Minderjährigen und Heranwachsenden ist bei Auskünften und Erklärungen über Verfahren, die diesen Personenkreis betreffen, besondere Zurückhaltung hinsichtlich der Bekanntgabe personenbezogener Daten zu wahren. Auch bei Kapitalverbrechen müssen zusätzliche Gesichtspunkte im Einzelfall für eine Bekanntgabe des Namens sprechen.

Das Ministerium der Justiz hat zwischenzeitlich den Entwurf einer entsprechenden Verwaltungsvorschrift vorgelegt, die diesen Anforderungen weitgehend entspricht.

7.6 Strafvollzug/Untersuchungshaft

7.6.1 Strafvollzugsgesetz

Die in den letzten Tätigkeitsberichten des LfD konstatierte Untätigkeit des Bundesgesetzgebers in bezug auf die datenschutzrechtliche Ergänzung des Strafvollzugsgesetzes ist nach wie vor festzustellen:

Zwar liegt nunmehr ein überarbeiteter Referentenentwurf eines 4. Gesetzes zur Änderung des Strafvollzugsgesetzes vor, der in erster Linie das Ziel verfolgt, im Strafvollzugsgesetz bereichsspezifische Rechtsgrundlagen für die Verarbeitung personenbezogener Daten zu schaffen.

Das Gesetzgebungsvorhaben scheint jedoch ins Stocken geraten zu sein, ein Fortgang oder dessen Abschluß sind derzeit nicht absehbar.

Zum Inhalt des Entwurfes ist festzustellen, daß er im Vergleich zu dem aus dem Jahr 1991 stammenden Vorentwurf datenschutzrechtliche Verbesserungen aufweist, die aber in einzelnen Punkten noch nicht ausreichend sind. Hierauf hat der LfD das Justizministerium hingewiesen.

7.6.2 Untersuchungshaftvollzugsgesetz

Nunmehr haben die bereits lange währenden Bemühungen nicht nur der Datenschutzbeauftragten Erfolg gehabt, für das Recht der Untersuchungshaft ein besonderes Gesetz auf den Weg zu bringen. Derzeit liegt ein vorläufiger Referentenentwurf des Bundesministeriums der Justiz vor (Stand: 19. August 1996).

Hierzu hat der LfD gegenüber dem Justizministerium Stellung genommen. Grundsätzlich hat er begrüßt, daß in der vorgesehenen gesetzlichen Regelung auch datenschutzrechtlich relevante Vorgänge normiert werden sollen. Aus seiner Sicht bestehen allerdings noch Defizite bei den Regelungen hinsichtlich der Überwachung des Schriftwechsels bez. der Überwachung von Telefongesprächen, über die Aufbewahrungsfristen von Akten sowie über die Unterrichtung solcher Personen, die über den Antritt der Untersuchungshaft unterrichtet worden sind, wenn der Untersuchungsgefangene freigesprochen oder wenn das Verfahren gegen ihn nicht nur vorläufig eingestellt wurde.

Auch bei diesem Gesetzgebungsverfahren ist derzeit allerdings ein Abschluß nicht absehbar.

7.6.3 Rückfalluntersuchung nach Vollzug der Jugendstrafe

Der Landtag hatte folgenden Beschluß gefaßt (Drucksache 12/5331 vom 29. Juni 1995):

„Die Landesregierung wird aufgefordert, Untersuchungen über die Rückfallquote nach Vollzug der Jugendstrafe durchzuführen und dem Landtag nach Vorliegen der Ergebnisse darüber zu berichten."

Zu diesem Zweck beabsichtigte das Ministerium der Justiz, folgendes Verfahren einzuführen:

Zunächst war ein Probelauf unter Beteiligung der beiden Jugendstrafanstalten des Landes vorgesehen. Die Anstalten sollten stichprobenweise bei den Gefangenen Daten erheben und in einen Fragebogen höchst sensible Angaben eintragen. Sie betreffen die Persönlichkeitsentwicklung und persönliche Umstände in einem relativ hohen Durchdringungsgrad und sind als außergewöhnlich sensibel anzusehen (regelmäßiger Alkoholgebrauch, regelmäßiger Drogengebrauch, regelmäßiger Medikamentengebrauch, Spielsucht, Krankheiten, psychische Störungen etc.).

Außerdem sind Daten Dritter betroffen (Scheidung der Eltern, Beruf der Eltern, Krankheiten in der Herkunftsfamilie des Gefangenen).

Die erhobenen Daten sollten dann automatisiert gespeichert werden. Sie sollten zunächst bis zur Entlassung der betroffenen Gefangenen in der Anstalt aufbewahrt werden. Nach Beendigung des Vollzugs sollten die Daten durch das Ministerium der Justiz aufbewahrt werden. Nach Ablauf von fünf bis zehn Jahren nach der Entlassung der Betroffenen sollte ein Bundeszentralregisterauszug eingeholt und dieser mit den jeweils gespeicherten Daten dem kriminologischen Dienst des Landes zur Auswertung übermittelt werden.

Nach Auffassung des Ministeriums waren die erhobenen Daten zu Behandlungszwecken bzw. zum Zweck der Durchführung des Jugendstrafvollzugs nötig, auch wenn sie bislang systematisch nicht erhoben und gespeichert worden sind. Der LfD wies demgegenüber darauf hin, daß eine automatisierte langdauernde Speicherung solch sensibler Daten nur vertretbar wäre, wenn sie wirklich unabdingbar zur Erfüllung des beabsichtigten Zweckes sei.

Dem zitierten Landtagsbeschluß konnte er weder entnehmen, daß der Landtag als Teil der Rückfallquotenuntersuchung auch die Erfassung und Erhebung von Daten fordert, die kriminologische Hypothesen über Ursachen von Rückfällen ermöglichen, noch daß er eine auf Dauer angelegte umfassende Datensammlung initiieren wollte. Nach seinem Eindruck könnte eine Rückfallquotenuntersuchung bereits jetzt – retrospektiv – auf der Basis vorhandener Daten durchgeführt werden: Zu diesem Zweck könnte es ausreichen, eine Abfrage beim Bundeszentralregister (gem. § 42 Abs. 2 BZRG) unter Nutzung der Namen der in der Vergangenheit in Rheinland-Pfalz inhaftierten jugendlichen Straftäter durchzuführen. In diesem Zusammenhang könnte u. U. sogar auf die Einholung der Einwilligung der Betroffenen verzichtet werden.

Das Ministerium beharrte jedoch auf seinem Vorhaben der umfassenden Untersuchung unter Einbeziehung von Daten, die zur Klärung möglicher Rückfallursachen beitragen. Es verzichtete jedoch zunächst auf die automatisierte Speicherung der erhobenen Daten; diese sollen vielmehr in der jeweiligen Gefangenenpersonalakte verbleiben. Dies ist gem. §§ 12, 13 LDSG zulässig.

Die eigentliche Rückfalluntersuchung wird nach Ablauf von fünf oder sechs Jahren nach der Entlassung erfolgen. Insoweit soll eine Totalerhebung erfolgen, die auf etwa fünf Jahre angelegt sein wird. Derzeit ist aber noch nicht deutlich geworden, durch welche Stelle unter Verwendung welcher Informationen diese eigentliche Rückfalluntersuchung in etwa fünf Jahren durchgeführt werden soll. Insoweit kann der LfD derzeit noch keine datenschutzrechtliche Bewertung abgeben.

7.6.4 Mithören bei Telefongesprächen Gefangener

In einer JVA des Landes wurde ein Kartentelefon eingeführt, dessen Benutzung nur zulässig ist, wenn jeweils ein Bediensteter mithört. Strafgefangene wandten sich mit folgenden Fragen an den LfD:

1. Ist es zulässig, die Benutzung des Kartentelefons in der JVA durch Gefangene von der Beschränkung abhängig zu machen, daß die Telefongespräche überwacht werden und daß der Gesprächspartner vor dem Gespräch von der Anstalt über die Überwachung informiert wird?
2. Ist es zulässig, diese Beschränkung auch auf Anwaltsgespräche zu erstrecken?
3. Ist es zulässig, die Genehmigung generell nicht für Behörden, Gerichte, Konsulate, Geschäfte, Versandhäuser usw. zu erteilen?
4. Ist es zulässig, daß der Beamte die Telefonnummer des genehmigten Gesprächspartners selbst anwählt?
5. Ist es zulässig, daß in einer Telefonliste Datum, Uhrzeit, Gesprächspartner, Telefonnummer und ggf. eine zusätzliche Überwachungsinformation vermerkt werden?

Zu diesen Fragen hat der LfD wie folgt Stellung genommen:

Das OLG Koblenz hat mit Beschluß vom 29. Januar 1993, Az. 3 Ws 141/93, festgestellt, daß in der betroffenen JVA ein besonderes Sicherungsbedürfnis besteht. Dies resultiere u. a. daraus, daß dort in erster Linie Langzeitgefangene untergebracht seien, die wegen erheblicher Straftaten einsäßen.

Vor diesem Hintergrund hat es das OLG Koblenz für zulässig erachtet, ein generelles Telefonierverbot durch die Anstalt zu erlassen. Damit seien alle Regelungen, die ein Telefonieren der Gefangenen unter einschränkenden Bedingungen zuließen, als gegenüber dem absoluten Verbot des Telefonierens geringerer Eingriff in die Rechte der Gefangenen anzusehen und dementsprechend grundsätzlich zulässig.

Diese Rechtsauffassung ist aus Datenschutzsicht zu akzeptieren: Wenn das generelle Verbot von Telefonaten zulässig ist, kann die Gestattung von Telefonaten unter Auflagen nicht grundsätzlich unzulässig sein.

Diese Auflagen müssen jedoch ihrerseits dem Verhältnismäßigkeitsgrundsatz entsprechen. Sie müssen insbesondere auch Rechte Dritter angemessen berücksichtigen. Der LfD hat anläßlich der vorbereitenden Erörterungen der entsprechenden Verfügung deshalb in der Vergangenheit bereits gefordert, daß eine Überwachung nur dann erfolgt, wenn beide Gesprächspartner, auch der angerufene Teilnehmer außerhalb der JVA, darüber informiert worden sind.

Diesem Anliegen wird die derzeitige Anstaltsleiterverfügung gerecht. Vor diesem Hintergrund sind aber auch die anderen oben unter 2. bis 4. als datenschutzrelevant bezeichneten Modalitäten der hier in Rede stehenden Anstaltsleiterverfügung nicht zu beanstanden.

Soweit die Regelung der Telefonlistenaufzeichnung betroffen ist (oben Punkt 5), stellen sich insbesondere Fragen nach dem Zweck und der Aufbewahrungsdauer dieser Aufzeichnungen. Diesbezüglich sind die Erörterungen mit der JVA noch nicht abgeschlossen.

Zwischenzeitlich hat die JVA allerdings auch die Unterrichtung des angerufenen Teilnehmers über das Abhören problematisiert; sie möchte insbesondere aus praktischen Gründen davon absehen. Die vorgetragenen Argumente haben den LfD jedoch nicht überzeugt. Auch diese Frage ist noch nicht abschließend geklärt.

7.6.5 Haftraumbeschilderung

Die Frage, welche Informationen außen auf dem Haftraum erkennbar sein dürfen, war Gegenstand mehrerer Eingaben. Nach Anfrage des LfD führte das Ministerium der Justiz folgende Klärung, einheitlich für alle Justizvollzugsanstalten des Landes, herbei:

Hinweise auf der Haftraumtür sind zulässig, wenn sie folgenden Inhalt haben:

- Name, Vorname des Gefangenen,
- Status (Strafgefangener/Abschiebungsgefangener),
- Notwendigkeit der Trennung von Tatgenossen in der U-Haft,
- Hinweis auf Disziplinar- oder Sicherungsmaßnahmen ohne Nennung von Einzelheiten (diese werden nur auf der Standtafel bzw. der Liste des Stationsbeamten festgehalten),
- Austauschkost oder Zusatzkost,
- Vegetarierkost,
- Kost ohne Schweinefleisch,
- Arbeitsbetrieb, Status als Vollzeitschüler, Tätigkeit als Hausarbeiter,
- Zulassung zu einem bestimmten Gottesdienst.

Aus organisatorischen Gründen seien nach der Einzelentscheidung der Anstalt möglicherweise auch folgende Hinweise erforderlich:

- Wäschenummer,
- Nichtbeschäftigung, ohne Differenzierung „Arbeitsverweigerer" oder „verschuldet ohne Arbeit",
- vorübergehende Abwesenheit des Gefangenen.

Die Hinweise könnten durch Symbole (farbige Zeichen) oder durch Buchstaben-Abkürzung erfolgen, Volltexthinweise sollen aber nicht erfolgen.

Bei einer entsprechenden Kennzeichnung von Haftraumzellen wird aus der Sicht des LfD der Erforderlichkeitsgrundsatz prinzipiell beachtet. Aus datenschutzrechtlicher Sicht ist eine solche Verfahrensweise nicht zu beanstanden.

7.6.6 Sonstige Eingaben

Weitere Eingaben aus dem Bereich des Strafvollzugs befaßten sich etwa mit folgenden Fragen:

Datenschutz beim Umgang mit Gefangenenlisten;
Speicherung und Nutzung von Rechtsbehelfsdaten Gefangener;
Weitergabe eines ärztlichen Befundberichts;
Anfertigung eines Lichtbildes für einen internen Ausweis;
Zulässige Übermittlung des sog. „A-Bogens" an die Strafvollstreckungskammer;
Kennzeichnung von Paketmarken.

Auf eine nähere Darstellung an dieser Stelle kann verzichtet werden.

8. Schulen, Hochschulen, Wissenschaft

8.1 Schulen

8.1.1 Technisch-organisatorischer Datenschutz in Schulen

Das Ministerium für Bildung, Wissenschaft und Weiterbildung hat eine Musterdienstanweisung über den Datenschutz und die Datensicherheit in Schulen, Studienseminaren, Kollegs und im Staatlichen Studienkolleg – inhaltlich abgestimmt mit dem LfD – erlassen (ABl. 1997, S. 526). Der Mustertext wird für die schulische Praxis sehr bedeutsam werden, der LfD hat sein Erscheinen ausdrücklich begrüßt.

Zusammen mit den Empfehlungen des Ministeriums für Bildung, Wissenschaft und Weiterbildung vom 15. Juli 1996, zum Datenschutz und zur Datensicherheit in der Verwaltung der Schulen bei der Verarbeitung personenbezogener Daten mit Arbeitsplatzrechnern (PC) oder in Akten (Abl. 1996, S. 349, Az. 15312 – Tgb.Nr. 132/96) liegen damit umfassende Materialien für die Schulen vor, die ihnen die Umsetzung des LDSG erleichtern.

8.1.2 Besetzung der Schulleiterstelle einer Grundschule; Fragerecht von Mitgliedern eines Verbandsgemeinderats

Bereits im 14. Tb., Tz. 8.1.5 (Der gläserne Bewerber um eine Schulleiterstelle), und im 15. Tb., Tz. 8.5 (Die Berufung eines neuen Schulleiters unter Beteiligung der Presse), hat der LfD Datenschutzfragen geschildert, mit denen er sich im Zusammenhang mit dem Schulleiterbesetzungsverfahren auseinanderzusetzen hatte.

Im Berichtszeitraum wurden erneut Fragen in diesem Zusammenhang an ihn herangetragen. So war das Fragerecht von Mitgliedern eines Verbandsgemeinderates an Bewerber um eine Schulleiterstelle Gegenstand einer Eingabe. Nach Auffassung des LfD bedarf das bislang praktizierte Verfahren, in dessen Verlauf dem Gemeinderat oder einem seiner Ausschüsse personenbezogene Informationen auch über andere als den von der Schulbehörde ausgewählten Bewerber übermittelt werden, einer ausdrücklichen Regelung im Schulgesetz bzw. in einer Rechtsverordnung. Solange diese Rechtsänderung nicht erfolgt ist, hält er bereits die Information gemeindlicher Entscheidungsorgane über alle Bewerber um eine Schulleiterstelle für unzulässig. Detaillierte persönliche Fragen über den Werdegang oder politische und pädagogische Auffassungen der Bewerber scheiden demnach auf der Basis des geltenden Rechts erst recht aus. Anders verhält es sich bei dem von der Schulbehörde vorgeschlagenen Bewerber:

Informationen über diesen dürfen dem Gemeinderat übermittelt werden. Der Gemeinderat hat die Befugnis, alle ihn sachlich interessierenden Fragen, die nicht die Privatsphäre des Bewerbers betreffen, zu stellen. Fragen zur politischen Überzeugung und zur religiösen Orientierung sind sachfremd und scheiden aus. Der Bewerber entscheidet natürlich selbst, ob und in welchem Umfang er die ihm gestellten Fragen beantwortet.

8.1.3 Datenerhebungen und -übermittlungen durch eine Schule für das Sozialamt

Die Tagesmutter eines Schulkindes beschwerte sich darüber, daß der Schulleiter ihr Pflegekind aus dem Unterricht heraus zu sich gebeten und dieses über seinen tatsächlichen Aufenthalt befragt habe. Außerdem habe er die Adresse dann an das Ordnungsamt weitergegeben.

Nach Einholung einer Stellungnahme des Schulleiters bewertete der LfD diesen Vorgang wie folgt:

Zur Erfüllung ihrer Aufgaben ist es erforderlich, daß die Schule davon Kenntnis hat, wo ein Kind während der Zeit des Schulbesuchs wohnt bzw. sich ständig aufhält und wer dieses Kind tatsächlich betreut. Eine dahin gehende Befragung des Schulkindes war demnach grundsätzlich zulässig. Ob diese Befragung ausreichend kindgerecht und schonend erfolgt ist, ist eine primär pädagogische Frage, es besteht kein unmittelbar datenschutzrechtlicher Bezug. Soweit das Verhalten des Rektors insofern nach Auffassung der Eltern zu beanstanden war, mußten sie auf den Weg der Dienstaufsichtsbeschwerde verwiesen werden. Aus datenschutzrechtlicher Sicht jedenfalls war die Erhebung der entsprechenden Daten zulässig (§ 54 a Abs. 1 Schulgesetz).

Die Übermittlung der Information über den Aufenthaltsort des Kindes an das Ordnungsamt war nach § 54 a Abs. 2 Schulgesetz zu beurteilen. Danach ist eine Übermittlung an eine öffentliche Stelle zulässig, wenn der Empfänger aufgrund einer Rechtsvorschrift berechtigt ist, die Daten zu erhalten. Außerdem muß die Kenntnis der Daten zur Erfüllung der dem Empfänger obliegenden Aufgaben erforderlich sein. Das Ordnungsamt war gem. § 25 a Abs. 1 POG berechtigt, Daten zu erheben, die zur Erfüllung seiner Aufgabe der Bekämpfung der Obdachlosigkeit erforderlich sind.

In diesem Zusammenhang war die tatsächliche Wohnanschrift des Kindes erheblich. Vor diesem Hintergrund war die Schule berechtigt, diese Information dem Ordnungsamt weiterzugeben. Aus datenschutzrechtlicher Sicht bestand folglich keine Veranlassung, das Verhalten des Schulleiters zu beanstanden.

8.1.4 Lehrerdaten im Schulbericht

Eine Schule des Landes veröffentlicht jedes Jahr einen Schulbericht, der in 90 Exemplaren erstellt wird und an alle Lehrer des Kollegiums und an die Pensionäre ausgehändigt bzw. übersandt wird.

In diesem Schulbericht war die Rede des Schulleiters anläßlich der Verabschiedung eines Lehrers in den Ruhestand aufgenommen worden. Dabei wurden auch Informationen aus seinem Lebenslauf verwandt, die wohl nicht allgemein bekannt waren, wie etwa, daß der Lehrer als Maschinenbaumeister und Techniker in Handwerk und Industrie tätig war und daß er in seiner Heimatgemeinde Mitglied des Gemeinderates war und derzeit als Fachübungsleiter einer Behindertensportgruppe tätig sei.

Außerdem war ein Gedicht in den Bericht aufgenommen worden, das von Schülerinnen des betreffenden Abiturjahrganges veröffentlicht worden war und in dem auch einzelne Lehrer mit besonderen Eigenheiten und tatsächlichen oder vermeintlichen Schwächen dargestellt wurden.

Der Personalrat der Schule hielt diese Veröffentlichungen ohne Einwilligung der Betroffenen für nicht zulässig. Maßstab der Prüfung für den LfD war § 54 a Abs. 1 Schulgesetz. Danach dürfen solche Lehrerdaten übermittelt und genutzt werden, deren Verarbeitung und Nutzung für die Aufgabenerfüllung der Schule erforderlich ist.

Daraus folgt für die Informationsverwendung anläßlich der Ruhestandsversetzung, daß jeder Beamte akzeptieren muß, wenn sein beruflicher Werdegang geschildert wird und diese Daten auch einem weiteren Kreis von Interessierten zugänglich gemacht werden. Entsprechende Informationen könnten ggf. auch veröffentlicht werden. Konkrete Informationen insbesondere über außerdienstliche Tätigkeiten allerdings dürften nur mit Einwilligung des Betroffenen in dieser Form verwendet werden.

Ähnliches gilt für die Veröffentlichung eines von Schülern verfaßten Gedichtes über Lehrer:

Soweit personenbezogene Informationen, die den privaten Bereich der Lehrer betreffen, dargestellt werden, ist die Einwilligung Voraussetzung. Es kommt hinzu, daß eine Datennutzung im Jahresbericht der Schule den situationsbedingt erstellten Texten ein weiteres Forum eröffnet hat und daß die Texte durch die amtliche Autorität des Herausgebers des Schulberichts eine besondere Bedeutung gewonnen haben. Für einen Teil des veröffentlichten Gedichtes war deshalb eine Erforderlichkeit der Übermittlung und Nutzung in diesem Zusammenhang zu verneinen.

Der Schulleiter wurde darauf hingewiesen.

8.1.5 Anfertigung von Klassen- und Schülerfotografien

Von Eltern wurde die Frage an den LfD herangetragen, ob es zulässig sei, daß ein Schulfotograf ohne ausdrückliche Einwilligung der Eltern von jedem Kind auch Einzelfotos herstelle.

Der LfD hat zur Frage des Datenschutzes bei der Tätigkeit eines Schulfotografen folgende Beurteilung formuliert:

Es bestehen keine Bedenken dagegen, daß auf der Basis der Information in einer Klassenelternversammlung oder eines Rundschreibens an die Eltern Gruppen- bzw. Klassenfotos durch einen privaten Fotografen erstellt werden. Der Eingriff in die informationelle Selbstbestimmung der betroffenen Schüler und ihrer Eltern ist bei diesem Verfahren nur als gering anzusehen.

Es steht den Eltern frei, ihr Kind von der Teilnahme am Gruppen- bzw. Klassenfoto fernzuhalten und den Lehrer entsprechend zu informieren.

Eine ausdrückliche Einwilligung ist in diesem Zusammenhang nicht erforderlich, weil insoweit an der Erstellung von Gemeinschaftsfotos auch ein schulisches Interesse besteht. Solche Unternehmungen fördern das Gemeinschafts- und Zusammengehörigkeitsgefühl der Schüler, Eltern und Lehrer. Dementsprechend reicht es aus, den Betroffenen eine Widerspruchsmöglichkeit einzuräumen (§ 16 Abs. 1 Nr. 4 LDSG).

Anders verhält es sich allerdings mit der Fertigung von Einzelfotos. An der Erstellung solcher Einzelfotos kann kein überwiegendes schulisches oder sonstiges öffentliches Interesse bejaht werden. Für die entsprechende Handlung bedarf es daher der vorherigen Einholung der konkreten Einwilligung der Eltern.

Im konkreten Einzelfall hat der LfD die Schule über diese datenschutzrechtliche Bewertung unterrichtet und sie gebeten, auf den Schulfotografen einzuwirken, daß dieser die Negative aller derjenigen Einzelfotos vernichtet, in deren Fertigung keine Einwilligung (oder nachträgliche Genehmigung, die konkludent durch den Erwerb eines entsprechenden Fotos erteilt würde) vorliegt.

8.1.6 Personaldatenübermittlung durch den Schulleiter an die Elternvertretungen

Der Gemeinde- und Städtebund wandte sich mit der Frage an den LfD, ob es zulässig sei, wenn ein Schulleiter Informationen über Fehlzeiten von Lehrern, die aus der Wahrnehmung eines Ehrenamtes (etwa als Gemeinderatsmitglied) entstanden sind, an die Elternvertreter weitergebe.

Diese Frage beurteilte der LfD wie folgt:

Informationsweitergaben durch Schulleiter über die Freistellung von Lehrern zur Wahrnehmung von Terminen, die aus dem Ehrenamt resultieren, könnten an den Schulausschuß, an die Schulelternvertretung, an einzelne Klassenelternvertreter oder an sonstige Organe der Schüler- oder Elternmitwirkung im Schulbereich erfolgt sein; es könnte sich jedoch auch um öffentliche Kundgaben gehandelt haben.

Soweit in diesem Zusammenhang Offenbarungen an im Schulgesetz vorgesehene Organe der Eltern- und Schülermitwirkung betroffen sind, ist von folgender Rechtslage auszugehen:

Nach § 1 a Abs. 3 Satz 2 SchulG verpflichtet die gemeinsame Erziehungsaufgabe die Schule und die Eltern zu vertrauensvollem und partnerschaftlichem Zusammenwirken, zu gegenseitiger Unterrichtung und Hilfe in allen für das Schulverhältnis bedeutsamen Fragen sowie zu Aufgeschlossenheit und Offenheit im Umgang miteinander.

Nach § 1 a Abs. 4 SchulG haben die Eltern ein Recht auf Beratung und Unterrichtung in fachlichen, pädagogischen und schulischen Fragen. Nach § 1 a Abs. 7 SchulG informieren Schulleiter und Lehrer die Eltern über alle wesentlichen Fragen des Unterrichts und der Erziehung.

Durch die Elternvertretungen werden die Eltern an der Gestaltung der Erziehungs- und Unterrichtsarbeit der Schule beteiligt. Die Elternvertretungen sollen die Interessen der Eltern im Rahmen der Erziehung ihrer Kinder wahren und das Vertrauensverhältnis zwischen der Schule und dem Elternhaus festigen und vertiefen (§ 33 Abs. 1 SchulG). Zu den Elternvertretungen gehören die Klassenelternversammlung, der Schulelternbeirat, der Bezirkselternbeirat und der Landeselternbeirat. Die gewählten Elternvertreter üben ein öffentliches Ehrenamt aus (§ 33 Abs. 2 SchulG). Der Schulelternbeirat nimmt die Mitwirkungsrechte der Eltern wahr (§ 35 Abs. 2 Satz 2 SchulG). Der Schulleiter unterrichtet den Schulelternbeirat über alle Angelegenheiten, die für das Schulleben von wesentlicher Bedeutung sind (§ 35 Abs. 3 SchulG).

Im Schulausschuß sind Lehrer, Schüler und Eltern vertreten.

Dieser hat die Aufgabe, das Zusammenwirken der Gruppen zu fördern. Er soll vor allen wesentlichen Beschlüssen und Maßnahmen der Schule gehört werden (§ 38 SchulG).

Die Mitglieder der Elternvertretungen sowie des Schulausschusses haben über Angelegenheiten, die ihnen in dieser Eigenschaft bekannt geworden sind, insbesondere über personenbezogene Daten und Vorgänge, Verschwiegenheit zu wahren (§ 39 Abs. 6 SchulG).

Aus datenschutzrechtlicher Sicht handelt es sich dann, wenn die angesprochenen Elternvertretungen bzw. der Schulausschuß Empfänger der genannten Informationen sind, nicht um Datenübermittlungen, sondern um Datennutzungen innerhalb der datenverarbeitenden Stelle Schule. Solche Nutzungen von Lehrerdaten sind zulässig, wenn sie für Zwecke erfolgen, für die die Daten erhoben worden sind, oder soweit dies zur Erfüllung der der Schule durch Rechtsvorschrift zugewiesenen Aufgaben erforderlich ist (§ 54 a Abs. 1 Satz 1 SchulG).

Die genannten schulgesetzlichen Vorschriften, insbesondere die Informationsgebote in den §§ 1 a, 35 Abs. 3 und 38 Abs. 1 SchulG, sind als entsprechende Rechtsvorschriften anzusehen, zu deren Erfüllung die angesprochene Datennutzung erforderlich ist. Der Unterrichtsausfall an Schulen ist eines der wichtigsten Konfliktfelder im Verhältnis zwischen Eltern und Schule. Hier ist der Schulleiter in besonderem Maße gefordert, Verständnis bei den Eltern für die ursächlichen Zwänge und die jeweiligen konkreten schulischen Verhältnisse zu schaffen. Dies setzt eine umfassende Information voraus.

Dieses Beurteilungsergebnis ist auch unter Berücksichtigung der folgenden Gesichtspunkte angemessen:

Die Mitglieder der Elternvertretungen, soweit sie ein Ehrenamt ausüben, sind gem. § 84 VwVfG und gem. § 39 Abs. 6 SchulG zur Verschwiegenheit verpflichtet (eine Verpflichtung, die gem. § 203 Abs. 2 StGB strafbewehrt ist). Es kommt hinzu, daß das Fehlen der entsprechenden Lehrer im Unterricht ohnehin jedenfalls in den jeweiligen Klassen allgemein und damit öffentlich bekannt ist. Daß der Grund die Inanspruchnahme durch ein Ehrenamt und nicht etwa Krankheit oder schuldhafte Versäumnisse des Lehrers ist, ist eine Zusatzinformation, die grundsätzlich im Interesse der betroffenen Lehrer liegen dürfte.

8.1.7 Darf der Schulträger kontrollieren, ob Lehrer dienstlich telefoniert haben?

Aufgrund der Anfrage eines Schulleiters hatte der LfD zu beurteilen, ob der Schulträger die Telefondaten der Lehrer, die durch seine Telefondatenerfassungsanlage erhoben und gespeichert werden, unter dem Gesichtspunkt der Erforderlichkeit überprüfen darf. Im Rahmen der Erörterung dieser Problematik mit dem Ministerium für Bildung, Wissenschaft und Weiterbildung hat der LfD die Auffassung vertreten, daß die vom Schulleiter sachlich und tatsächlich richtig gezeichneten Telefonkosten vom Schulträger zu übernehmen sind. Eine eigene Prüfungskompetenz bezüglich der Erforderlichkeit von Telefonaten kann dem Schulträger nicht zugesprochen werden. Dies hat zur Folge, daß Einzelverbindungsnachweise, die bei dem Schulträger eingehen, ungeprüft an den Schulleiter der jeweiligen Schule weiterzuleiten sind. Sofern der Schulleiter bestätigt, daß die geführten Telefonate dienstlich notwendig waren, muß dies für den Schulträger ausreichend sein. Das Ministerium hat dieser Auffassung zugestimmt.

Wenn der Schulträger den an der Schule Beschäftigten gestattet, über Dienstleitungen Privatgespräche zu führen und diese die entstehenden Kosten erstatten müssen, darf er allerdings die kostenrelevanten Telefongesprächsdaten erfassen, um daraus eine Kostenrechnung zu erstellen. Die angerufene Nummer muß dann allerdings um die letzten drei Ziffern verkürzt werden, so daß nicht die vollständige Anschlußnummer erkennbar ist.

Weiterhin hat der LfD die Auffassung vertreten, daß der Schulträger die Telefondaten der Lehrer dann automatisiert erfassen darf, wenn dies im Rahmen eines datenschutzrechtlichen Auftragsverhältnisses für die Schulleitung erfolgt (Auftragsdatenverarbeitung gem. § 4 LDSG). Auch dann steht dem Schulträger aber keine eigene Prüfungsbefugnis zu. Er ist in diesem Fall zu verpflichten, die entstehenden Daten auf möglichst unmittelbarem Weg transportgesichert (§ 9 Abs. 2 Nr. 9 LDSG, z. B. in einem verschlossenen Umschlag) an die Schulleitung zu übermitteln.

8.1.8 Klassenbuchverwaltung durch Schüler

Ein schulischer Datenschutzbeauftragter hat um Mitteilung gebeten, ob es zulässig sei, Schüler mit der Beaufsichtigung des Klassenbuchs zu beauftragen.

Gemäß den Regelungen der Schulordnungen (z. B. § 22 der Schulordnung für Berufsbildende Schulen) können im Rahmen der Aufsicht u. a. Schüler mit der Wahrnehmung besonderer Aufgaben betraut werden. Die Beaufsichtigung des Klassenbuchs kann als besondere Aufgabe i. S. der o. g. Vorschriften angesehen werden. Der LfD sieht daher aus datenschutzrechtlicher Sicht gegen eine derartige Beauftragung keine grundsätzlichen Bedenken.

Bei der Auswahl des jeweiligen Schülers ist jedoch auf die notwendige Zuverlässigkeit zu achten; außerdem sollte dieser besonders auf das Datengeheimnis und darauf hingewiesen werden, daß ein Verstoß gegen diese Verpflichtung schulische Sanktionen (z. B. Tadel, Ordnungsmaßnahmen) zur Folge haben kann (bei strafmündigen Schülern – die älter als 14 Jahre sind – käme bei Vorliegen der Voraussetzungen des § 35 LDSG sogar Freiheitsstrafe bis zu einem Jahr oder Geldstrafe in Betracht).

8.2 Hochschulen

8.2.1 Datenerhebung bei ausländischen Studenten für das Akademische Auslandsamt

An einer Universität des Landes befragte das Akademische Auslandsamt ausländische Studenten, um Informationen über deren Integration, ihre Studiensituation und mögliche Verbesserungsansätze zu erhalten.

Eine Eingabe Betroffener führte hier zu einer Beanstandung:

In dem Anschreiben an die betroffenen ausländischen Studenten wurden diese aufgefordert, einen Fragebogen auszufüllen. Dieser sollte bis spätestens zu einem bestimmten, kalendermäßig bezeichneten Tag an das Akademische Auslandsamt zurückgesandt werden. Die Fragebögen waren numeriert, damit der Eingang überprüft werden konnte.

In den Befragungsunterlagen fehlte ein Hinweis auf die Freiwilligkeit der Teilnahme und darauf, daß bei Nichtteilnahme keine Nachteile entstehen (§ 5 Abs. 2 LDSG). Es wurde im Gegenteil eher der Eindruck erweckt, daß eine Teilnahmepflicht bestand. Vor dem Hintergrund, daß in dem Fragebogen äußerst sensitive Daten erhoben wurden, die zu politischen Diskriminierungen der betroffenen Studenten in ihrem Heimatland mißbraucht werden konnten, hielt der LfD den Verstoß gegen das Freiwilligkeitsprinzip im vorliegenden Fall für gewichtig. Deshalb wurde die bereits durchgeführte Umfrage ausdrücklich beanstandet. Hierüber hat der LfD das Präsidialamt der Universität sowie das Ministerium für Bildung, Wissenschaft und Weiterbildung unterrichtet.

Das betroffene Akademische Auslandsamt erklärte, künftig die datenschutzrechtlichen Vorgaben beachten zu wollen; es wurde auch Einvernehmen über die weitere Aufbewahrung der zurückgesandten Fragebögen erzielt, die unverzüglich vollständig zu anonymisieren waren.

8.2.2 Datenübermittlungen an andere Universitäten über abgelehnte Dissertationen

Die jeweiligen Promotionsordnungen der Hochschulen, die als Satzungsrecht Rechtsnormqualität haben, sehen sämtlich übereinstimmend vor, daß eine Dissertation nur dann angenommen werden kann, wenn sie noch von keiner anderen Hochschule abgelehnt worden ist.

Vor diesem Hintergrund unterrichten sich die jeweiligen Fachbereiche/Fakultäten der Universitäten untereinander über die jeweils endgültig abgelehnten Dissertationen. Aus datenschutzrechtlicher Sicht stellt sich hier die Frage, ob das geltende Recht die gegenseitige Unterrichtung der betroffenen öffentlichen Stellen (Hochschulen) gestattet.

Der LfD hält dies nur dann für zulässig, wenn eine ausdrückliche rechtliche Grundlage hierfür besteht, die in den Promotionsordnungen derzeit nicht vorhanden ist. Allerdings ist er der Auffassung, daß im Bereich der Dissertationen ebenfalls eine Einwilligungslösung in Betracht kommt. Insofern dürfte die Situation von Promotionswilligen nur ausnahmsweise mit der von Studienbewerbern oder sonstigen Personen vergleichbar sein, die auf bestimmte staatliche Leistungen angewiesen sind. Hier könnte die Gewährung einer universitären Leistung durchaus von der Zustimmung zu dem grundsätzlich erforderlichen Datenaustausch abhängig gemacht werden. Aus der Sicht des LfD käme auch eine Zentralstellenlösung in Betracht, die im vorliegenden Zusammenhang datenschutzrechtliche Vorteile hätte (bessere datenschutzrechtliche Kontrollmöglichkeiten, verbesserte Vorkehrungen gegen Verwechslungen u. ä.). Eine zentrale Lösung dieses Problems steht bislang noch aus.

8.2.3 Adressenweitergaben zur Einladung ehemaliger Studenten

An einer Fachhochschule wollte der Fachschaftsvorstand eines Fachbereichs Daten ehemaliger Studenten beim Studentensekretariat erheben, um ein Ehemaligentreffen durchzuführen. Der LfD hat die Zulässigkeit dieser Datenverarbeitung wie folgt beurteilt:

Der Fachschaftsvorstand ist als Teil der datenverarbeitenden Stelle „Fachhochschule" anzusehen. Dementsprechend hat es sich bei der hier in Rede stehenden Datenweitergabe nicht um eine Übermittlung, sondern um die Nutzung von Daten gehandelt.

Nach § 55 Abs. 3 FachhochschulG ist in der Einschreibeordnung im einzelnen festzulegen, welche für Zwecke des Studiums erforderlichen Daten zur Person sowie zum Studienverlauf erhoben werden, sowie an wen, zu welchen Zwecken und unter welchen Voraussetzungen diese Daten übermittelt werden können. Auch zur zulässigen Nutzung könnten hier Regelungen getroffen werden.

Wenn keine vorrangigen bereichsspezifischen Rechtsvorschriften – etwa in der Einschreibeordnung – vorhanden sind, ist die Nutzung personenbezogener Daten zulässig, wenn dies zur Aufgabenerfüllung der speichernden Stelle erforderlich ist und keine Zweckänderung vorliegt (§ 13 Abs. 1 LDSG). Die Nutzung der Adreßdaten von ehemaligen Studenten zum Zweck der Veranstaltung von Ehemaligentreffen dient nicht mehr der Durchführung des Studiums. Dieser Zweck hängt allerdings eng mit dem ursprünglichen Erhebungszweck zusammen, so daß noch von einer Zweckidentität ausgegangen werden kann. Jedenfalls wäre aber eine Einladung zu einem Ehemaligentreffen durch die Fachschaft ein Vorgang, der im Interesse der Betroffenen liegt und für den kein Grund zur Annahme besteht, daß die Betroffenen in Kenntnis des Zwecks ihre Einwilligung verweigern würden (§ 12 Abs. 4 Nr. 6 LDSG).

Unter diesen Voraussetzungen bestanden aus datenschutzrechtlicher Sicht keine Bedenken gegen die beabsichtigte Datennutzung.

Anders war der Fall zu beurteilen, daß ein Fachbereich die zu Dokumentationszwecken beim Studentensekretariat gespeicherten Daten ehemaliger Studenten zum Zweck der Kontaktpflege mit den Ehemaligen nutzen wollte. Zu diesem Zweck wollte er einen eigenen Datenbestand mit Namen und Anschriften der ehemaligen Studenten aufbauen.

Der Unterschied zwischen dem oben beurteilten zu dem hier dargestellten Fall liegt in der konkreten Datennutzung: Die Einladung zu einem Ehemaligentreffen ist nicht identisch mit der langfristigen Pflege von Beziehungen und der dauerhaften Kontaktnahme (Geldwerbung) zwischen der Fachhochschule und den ehemaligen Studenten.

Bezüglich des Ehemaligentreffens konnte – wie dargelegt – davon ausgegangen werden, daß die Einladung im Interesse der Betroffenen liegt. Bei der Nutzung zur ständigen Kontaktnahme ist dies nicht mehr so deutlich. Es kommt also darauf an, ob die Kontaktpflege zu ehemaligen Studenten als zur Aufgabenerfüllung des Fachbereichs erforderlich angesehen werden kann.

Es wäre zu begrüßen, wenn insoweit eine verbindliche Willensbildung in der Fachhochschule durch die jeweils zuständigen Gremien herbeigeführt würde, um die Frage eindeutig zu beantworten, ob eine solche Kontaktpflege zu ehemaligen Studenten als Teil der Aufgaben der Fachhochschule angesehen wird.

Falls diese Voraussetzung erfüllt wird, bleibt allerdings aus der Sicht des technisch-organisatorischen Datenschutzes zu fragen, ob dann nicht die Adressenverwaltung beim Studentensekretariat zentral beibehalten werden kann, bzw. aus welchen Gründen eine Verdoppelung des Datenbestandes bei den Fachbereichen erfolgen muß. Die Verdoppelung von Datenbeständen erschwert die Einhaltung der technischen und organisatorischen Datenschutzanforderungen gem. § 9 LDSG.

Falls insoweit keine verbindliche Klarstellung durch den Fachbereichsrat erfolgt, bleibt nur die Einholung der Einwilligung der betroffenen ehemaligen Studenten in die Nutzungsänderung ihrer Daten.

8.2.4 Veröffentlichung von studentischen Meinungsumfragen zum Lehrverhalten

Der LfD hat sich grundsätzlich zu der Frage der Veröffentlichung von studentischen Meinungsumfragen zum Lehrverhalten bereits in seinem 14. Tb. (Tz. 8.2.2) geäußert. Dennoch erreichten ihn erneut mehrere Anfragen zu diesem Punkt.

Der LfD verwies zunächst auf seine Überlegungen im 14. Tb.; ergänzend machte er deutlich, daß aufgrund der Neufassung des Fachhochschulgesetzes und des Universitätsgesetzes die Rechtslage in diesem Zusammenhang noch klarer geworden ist. Gemäß § 15 Abs. 3 FachhochschulG und § 20 Abs. 3 Universitätsgesetz dürfen die Hochschulen 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. Die Ergebnisse dürfen, auch soweit sie Namen von Lehrenden enthalten, hochschulöffentlich mitgeteilt werden.

Im Rahmen des ihr gesetzlich zugewiesenen Aufgabenkreises werden auch die Organe der verfaßten Studentenschaft als „Hochschule" tätig. Auch diese selbständigen Teilkörperschaften der Hochschulen dürfen aus der Sicht des LfD entsprechende Aufgaben wahrnehmen.

8.2.5 Multifunktionskarte der Universität Trier (TUNIKA)

Als weitgehend einhellige Auffassung der Datenschutzbeauftragten des Bundes und der Länder zeichnet sich ab, daß der Einsatz von Chipkarten durch öffentliche Stellen als besonders regelungsbedürftige Form der automatisierten Datenverarbeitung angesehen wird. Dies ist vergleichbar der Situation bei Direktabrufverfahren (also bei Online-Zugriffen auf Bestände personenbezogener Daten), deren Einrichtung und Ausgestaltung sowohl im Bundesdatenschutzgesetz wie nunmehr auch in allen Landesdatenschutzgesetzen besonders geregelt ist (vgl. § 10 BDSG, § 7 LDSG R-P).

Der LfD vertritt allerdings die Auffassung, daß bei dem Einsatz der Chipkarte der Universität Trier keine zusätzlichen datenschutzrechtlichen Eingriffe in die Rechte der Betroffenen erfolgen, die den Rechts- oder Sachstand gegenüber der bisherigen Nutzung von Studentenausweisen verändern. Diese Bedingungen sind dadurch gekennzeichnet, daß auf dem Speicherchip der Karte selbst keine über den Datenumfang des traditionellen Studentenausweises hinausgehenden personenbezogenen Daten gespeichert werden und daß keine Datenerfassungen und Datenänderungen im Zuge der laufenden Nutzung erfolgen, womit eine Erfassung des Verhaltens der Betroffenen ausgeschlossen ist.

Die technischen Bedingungen des Einsatzes von Chipkarten erlauben jedoch grundsätzlich, ohne größere technische Aufwendungen vom Nutzer unbemerkt Speicherungen auf der Chipkarte vorzunehmen. Unter anderem dürfte auch daraus eine gewisse Unsicherheit der Betroffenen (hier insbesondere der Studenten) resultieren. Vor diesem Hintergrund hält es der LfD für angemessen, wenn der Einsatz der im Rahmen des Projekts TUNIKA geplanten Chipkarte durch universitäre Rechtsgrundlagen (hier käme eine besondere Satzung der Universität über den Chipkarteneinsatz in Betracht) geregelt wird.

Der Vorteil einer solchen Regelung liegt auf der Hand: Die Rechtspositionen der Betroffenen werden deutlich und lassen sich leichter durchsetzen. Das Verfahren erhält eine demokratische Legitimation, die dem Einsatz eines solchen qualitativ neuen und potentiell eingriffsintensiven Instruments wie der Chipkarte angemessen ist. Die Einsatzbedingungen werden transparent; mögliche wesentliche Verfahrensänderungen müßten ebenfalls in einem transparenten, kontrollierten Verfahren erfolgen. Die damit festgeschriebenen Nutzungsbedingungen der Chipkarte begründen letztlich für alle Beteiligten eine Rechtssicherheit und Rechtsklarheit, die der Akzeptanz des geplanten Verfahrens nur dienlich sein kann. Eine solche universitäre Rechtsgrundlage sollte insbesondere folgende Regelungen enthalten:

a) Die auf dem Kartenchip zu speichernden Daten sollten enumerativ und abschließend bestimmt werden.

b) Es sollte festgeschrieben werden, ob bzw. welche Informationen über Aktivitäten des Nutzers im Bereich des hoheitlichen Einsatzes der Chipkarte (also in dem Bereich, in dem die Chipkarte als Studentenausweis durch universitäre Stellen akzeptiert wird) auf der Chipkarte gespeichert werden.

c) Es sollte weiterhin festgeschrieben werden, daß diejenigen Stellen, die die Möglichkeit der Datenerfassung auf der Chipkarte zu weitergehenden Speicherungen beim Einsatz der Karte tatsächlich nutzen, dies nur aufgrund der informierten umfassenden Einwilligung der Betroffenen tun dürfen.

d) Schließlich sollte in dieser Rechtsgrundlage festgeschrieben werden, daß alle universitären und außeruniversitären Stellen, die die Studentenkarte nutzen und akzeptieren, dabei entstehende Datenspeicherungen im infrastrukturellen Umfeld (also bei den Akzeptanzstellen selbst) den betroffenen Studenten gegenüber deutlich zu machen haben. Die Universität Trier sollte sich verpflichten, eine entsprechende Übersicht zu führen, die im Verhältnis zu den Betroffenen (Studenten) öffentlich ist und für Auskunftszwecke zur Verfügung steht.

Ohne eine entsprechende rechtssatzmäßige Absicherung dieses Vorhabens, die allerdings bislang noch nicht erfolgt ist, kann nicht von einer datenschutzgerechten Ausgestaltung des Verfahrens gesprochen werden. Der LfD hat die Universität hierauf hingewiesen.

8.3 Wissenschaftliche Forschung

Aufgrund von Anmeldungen gem. § 27 LDSG waren im Berichtszeitraum ca. 50 Forschungsvorhaben datenschutzrechtlich zu beurteilen. Daneben sind aufgrund von Eingaben Umfragen oder andere Datenerhebungen zu Forschungszwecken bekannt geworden, die ebenfalls zu prüfen waren. Im folgenden werden Schwerpunkte der Tätigkeit des LfD im Bereich der datenschutzrechtlichen Begleitung der Forschung, aber auch Beispiele aus der ständigen laufenden Arbeit in diesem Zusammenhang dargestellt.

8.3.1 Vorwurf der Wissenschaftsbehinderung durch Datenschutz

Die Deutsche Forschungsgemeinschaft hat in ihrer Denkschrift zu Forschungshindernissen in Deutschland auch den Datenschutz genannt. Zur Klärung der vorhandenen Schwierigkeiten fand beim LfD Hessen ein Gespräch mit Vertretern der Deutschen Forschungsgemeinschaft statt.

Die Hauptkritikpunkte der Deutschen Forschungsgemeinschaft sind:

a) Es existieren unübersichtliche unterschiedliche Regelungen zum Datenschutz auf den Ebenen der EG, des Bundes und der Länder.

b) Diese Regelungen enthalten zudem eine Reihe unbestimmter Rechtsbegriffe, die zu einem zu großen Entscheidungsspielraum der ausführenden Behörden führen und unterschiedlich ausgelegt werden.

Die Datenschutzbeauftragten betonten die Bedeutung des Föderalismus und die Vorteile einer Gesetzgebung, die flexibel und auch im Wettbewerb untereinander unterschiedlich auf vorhandene gesellschaftliche Anliegen reagiere.

Zur konkreten Verbesserung der Abstimmung innerhalb der Datenschutzbeauftragten wurde den Forschern allerdings empfohlen, sich bei länderübergreifenden Forschungsvorhaben unmittelbar an den LfD Hessen als Vorsitzenden des Arbeitskreises Wissenschaft zu wenden, um dort auf eine Vereinheitlichung hinzuwirken.

Nach einer Erörterung einer Reihe von Einzelfragen wurde zum Ende des Gesprächs vereinbart, daß die Deutsche Forschungsgemeinschaft einen Formulierungsvorschlag für ein möglichst gemeinsames Papier von Datenschützern und Forschern vorlegen werde, das die Anliegen zur Verbesserung der derzeitigen Situation zusammenfassen sollte.

Seitens der Datenschutzbeauftragten wurde darauf hingewiesen, daß es wünschenswert wäre, für die Position der Wissenschaftler einen repräsentativen Ansprechpartner zu haben. Die Vertreter der Deutschen Forschungsgemeinschaft räumten ein, daß außer ihrer eigenen Institution insbesondere die Max-Planck-Gesellschaften, die Helmholtz-Institute, der Wissenschaftsrat, die Blauen-Liste-Institute, die Hochschulrektorenkonferenz und die Arbeitsgemeinschaft für wissenschaftlich-medizinische Forschung ebenfalls wichtige Repräsentanten des Interesses der Forscher seien. Das Gespräch soll allerdings zunächst mit der Deutschen Forschungsgemeinschaft vorangetrieben werden.

8.3.2 Krebsregistergesetz

Das Landeskrebsregistergesetz wurde am 17. Juni 1997 verabschiedet (GVBl. 1997 S. 167). Es trat zum 1. Juli 1997 in Kraft. Regelungstechnisch ergänzt es das Bundeskrebsregistergesetz nur um die unabdingbaren Ausführungsbestimmungen; an wenigen Punkten vereinfacht es das bundesgesetzlich vorgegebene Verfahren. Dies ist Anlaß, kurz auf die Bedeutung rheinland-pfälzischer Aktivitäten für die bundesweite epidemiololgische Krebsforschung und auf die Rolle des LfD einzugehen.

Im Jahre 1982 ist in Hessen eine Initiative zur Errichtung eines Krebsregisters an den Vorbehalten des dortigen Datenschutzbeauftragten gescheitert. Datenschutz und Forschung standen sich scheinbar unvereinbar gegenüber, und deshalb wurde nur wenig erreicht, bis Professor Michaelis vom Institut für Medizinische Statistik und Dokumentation der Universität Mainz seinen Kompromißvorschlag der personenbezogenen Meldung bei anonymisierter (aber reidentifizierbarer) Speicherung bei bloßem Widerspruchsrecht der Patienten vortrug. Durch diesen Vorschlag wurden die Fronten zwischen Datenschutz und Epidemiologen aufgelockert, denn die Datenschutzbeauftragten hatten bislang keine Alternative zur Einwilligung der Patienten oder der völlig anonymen Meldung und Speicherung im Krebsregister gesehen. Der LfD hat dieses „Michaelis-Modell" von Beginn an unterstützt und an seiner Entwicklung mitgewirkt. Nunmehr ist es weitgehend unumstritten, daß dieses Modell datenschutzverträglich ist. Es wurde zur Grundlage des Bundeskrebsregistergesetzes.

Das rheinland-pfälzische Gesetz orientiert sich folglich eng an dem Modell, das das Bundeskrebsregistergesetz vorgibt. Das Bundesgesetz läßt allerdings eine Reihe von Alternativlösungen zu. Andere Bundesländer werden zum Teil weitgehend Gebrauch von der Möglichkeit machen, eigene Wege zu gehen. Dies betrifft sowohl die Frage, ob flächendeckende Krebsregister eingerichtet werden, wie die Frage, welches Meldemodell gewählt wird.

Der LfD hält das Landeskrebsregistergesetz für datenschutzverträglich (wenn auch in Details für verbesserungsfähig; dies bezieht sich aber mehr auf regelungstechnische als auf inhaltliche Fragen. Beispiel: § 5 Abs. 3, wo von „Computern" und „Computerprogrammen" statt von „Schlüsseln" und „Entschlüsselungsverfahren" die Rede ist).

Die Ausgestaltung des Entschlüsselungsverfahrens wird im Gesetz nicht im Detail geregelt. Dies wird in verwaltungsinternen Regelungen erfolgen, an deren Zustandekommen und Inhalt der LfD weiterhin intensiv Anteil nehmen wird.

8.3.3 Eine Untersuchung über Zwangssterilisation in der NS-Zeit

Ein Professor an einer Fachhochschule des Landes wandte sich mit dem Anliegen an den LfD, ihn gegenüber dem Landeshauptarchiv zu unterstützen. Dieses lehne es ab, ihm und seinen Diplomanden Zugriff auf dort vorhandene Akten über Zwangssterilisationen in der NS-Zeit zu gewähren. Der LfD beschied ihn wie folgt:

Die Nutzung von Materialien des Landeshauptarchivs richtet sich ausschließlich nach den Regelungen des Landesarchivgesetzes. Das LDSG wird durch diese Nutzungsregelungen bezüglich der Fragen der Übermittlung von Daten auch zu wissenschaftlichen Zwecken verdrängt.

Nach § 3 Abs. 2 Nr. 4 LArchG ist die Benutzung von Archivalien einzuschränken oder zu versagen, soweit die Geheimhaltungspflicht nach § 203 Abs. 1 StGB verletzt würde.

Die allein in Betracht kommenden Akten der Gesundheitsämter enthalten in größerem Umfang – wenn nicht ausschließlich – Daten, die der Geheimhaltungspflicht des § 203 Abs. 1 Nr. 1 StGB unterliegen. Ihre Nutzung ist nur dann zulässig, wenn sich hierfür eine gesetzliche Befugnis ergeben würde. Eine solche Befugnis könnte sich aus § 3 Abs. 3 Satz 2 LArchG ergeben. Danach dürfen Unterlagen, die aufgrund von Rechtsvorschriften geheimzuhalten sind, erst 80 Jahre nach ihrer Entstehung benutzt werden. Im Umkehrschluß könnte man daraus aber auch die Befugnis ableiten, 80 Jahre nach ihrer Entstehung auch solche Unterlagen nutzen zu dürfen, die aufgrund von Rechtsvorschriften geheimzuhalten sind. Diese Frist ist noch nicht abgelaufen. Eine Verkürzung auch dieser Sperrfrist kommt dann in Betracht, wenn die Benutzung der Archivalien für ein wissenschaftliches Forschungsvorhaben erforderlich ist und eine Gefährdung des Archivguts sowie eine Beeinträchtigung wichtiger öffentlicher Belange oder schutzwürdiger Belange Betroffener und Dritter durch geeignete Maßnahmen ausgeschlossen werden kann.

Im Zusammenhang mit dem beschriebenen Forschungsvorhaben war zweifelhaft, ob die Benutzung von Akten der Gesundheitsämter für das wissenschaftliche Forschungsvorhaben erforderlich war. Nach dem nachvollziehbaren Vortrag des Landeshauptarchivs enthalten die Akten der Gesundheitsämter zur Frage der Zwangssterilisationen und zu sonstigen Verbrechen an Behinderten und psychisch kranken Menschen in der Zeit des Nationalsozialismus nur in geringem Umfang relevante Informationen. Die eigentlich bedeutsamen Unterlagen in diesem Zusammenhang werden bei den Landesnervenkliniken aufbewahrt.

Es kommt hinzu, daß bei einer Einsichtnahme in entsprechende Archivalien nicht nur Daten solcher Personen den Einsicht Nehmenden zur Kenntnis gelangen würden, die Opfer der Verbrechen waren. Es wären eine ganze Reihe höchst sensibler sonstiger Angaben, z. B. über Adoptionen, Entmündigungen und Geschlechtskrankheiten von einer Einsichtnahme umfaßt.

Insoweit waren die folgenden Forderungen des Landeshauptarchivs aus datenschutzrechtlicher Sicht nicht nur nachvollziehbar, sondern nachdrücklich zu unterstützen:

- genaue Bezeichnung des Forschungsvorhabens unter genauer Bezeichnung der Archivalien, die anhand der Inventarbücher des Landeshauptarchivs zu benennen wären;
- Durchführung konkreter Maßnahmen zur Anonymisierung bzw. zur Unterbindung der Einsicht in solche Teile der Archivalien, die für das Forschungsvorhaben offensichtlich unbedeutend sind.

Unter diesen Bedingungen können die Sperrfristen verkürzt werden. Dies bedeutet, daß das Landeshauptarchiv eine Ermessensentscheidung hierüber zu treffen hat. Bei dieser Ermessensentscheidung kann der Aufwand berücksichtigt werden, den die erforderliche Anonymisierung verursachen würde.

Vor diesem Hintergrund hat der LfD keine Möglichkeit gesehen, das Anliegen des Fachhochschulprofessors weitergehend zu unterstützen.

8.3.4 Datenschutzanforderungen an wissenschaftliche Untersuchungen in der Schule

Das Thema „Aggressionen unter Schülern" war Thema mehrerer Befragungen, die von Psychologen an Schulen des Landes durchgeführt wurden. In diesem Kontext werden regelmäßig Informationen über die aggressiven Handlungen der befragten Schüler selbst erhoben, etwa „Wie oft hast Du einen Mitschüler so verletzt, daß er geblutet hat" oder auch „Wie oft hast Du einen Lehrer bedroht, angeschrien, geschlagen?", „Wie oft hast Du irgendwo eingebrochen?". Da die ausgefüllten Fragebögen dann, wenn sie vom Lehrer eingesammelt werden, von diesem häufig schon aufgrund der Handschrift dem Urheber zugeordnet werden können, war darauf hinzuwirken, daß entweder diese Möglichkeit ausgeschlossen oder erheblich erschwert wurde oder daß im Text der Einverständniserklärung der Eltern auf diese Reidentifikationsmöglichkeit hingewiesen wurde. Außerdem war regelmäßig darauf hinzuweisen, daß die Eltern bei der Einholung ihrer Einwilligung angemessen über die Fragen des Erhebungsbogens unterrichtet werden. Der LfD hat es für ausreichend gehalten, wenn die Eltern neben einer allgemeinen Information darauf hingewiesen wurden, daß sie den Fragebogen im Schulsekretariat einsehen können.

8.3.5 Ärztliche Untersuchungen zu wissenschaftlichen Zwecken an einer Schule

Folgender Sachverhalt gelangte dem LfD zur Kenntnis:

Ein Allgemeinmediziner führte mit Unterstützung eines Gymnasiums eine Haltungsuntersuchung an Schülern der 5. Klasse durch. Gegenstand der Untersuchung waren Körperbau, Entwicklungsstand, Haltung und Bewegung der Kinder. Die Unter-

suchungen waren Einzeluntersuchungen von je 30 Minuten Dauer. Bei der Untersuchung sollten die Kinder vollständig unbekleidet sein. Am Ende der Untersuchung wurden das Kind und die Eltern befragt, ob sie eine Fotodokumentation erlaubten. Diese Fotodokumentation bestand aus sechs standardisierten Aufnahmen.

Zur Vorbereitung der Untersuchung erbat der Arzt die Angabe des Geburtsdatums, der Anschrift und der Telefonnummer.

Diese Untersuchung wurde über fünf Jahre hinweg durchgeführt, ohne daß die gem. § 54 a Abs. 3 SchulG erforderliche Genehmigung des zuständigen Ministeriums vorgelegen hätte.

Außerdem ergab sich, daß an den Arzt zumindest die Namen, möglicherweise auch die Anschriften derjenigen Kinder übermittelt worden sind, deren Eltern keine Einwilligung in die Untersuchung erteilt hatten. Für eine solche Datenübermittlung war keine Rechtsgrundlage vorhanden, sie war unzulässig.

Unter beiden Gesichtspunkten beanstandete der LfD das bisherige Verfahren.

Einige Zeit später verstarb der die Untersuchung durchführende Arzt, und es stellte sich die Frage, wie mit den entstandenen etwa 400 Kinder betreffenden Unterlagen, die bislang wissenschaftlich nicht ausgewertet waren, unter Wahrung des Arztgeheimnisses angemessen umzugehen ist. Konkret war zu entscheiden, ob sämtliche Unterlagen dieser Studie mit den personenbezogenen Daten der Untersuchten und ihrer Eltern zum Zweck der weiteren Auswertung an einen auswärtigen Wissenschaftler übermittelt werden dürfen.

Dagegen bestehen deshalb Bedenken, weil entsprechende Einwilligungen der Betroffenen fehlen und weil angesichts der gefertigten Lichtbilder eine vollständige Anonymisierung kaum möglich ist. Der LfD ist letztlich für die Beurteilung dieser Fragen aber nicht zuständig, weil es sich insoweit um die Übermittlung von Daten durch eine private Person (den Erben des verstorbenen Arztes) handelt, auf die er keinen unmittelbaren Einfluß ausüben darf.

8.3.6 Nutzung einer Liste ehemaliger Häftlinge des KZ Osthofen

Die Landeszentrale für politische Bildung stellte folgende Frage: Sie habe eine Liste von ehemaligen Häftlingen des KZ Osthofen gefertigt und wolle nunmehr klären, wer diese Informationen zu welchem Zweck nutzen dürfe.

Die Namen und Anschriften der betroffenen Personen wurden durch Auswertung von öffentlich zugänglichen Quellen (Zeitungen, Zeitschriften), durch die Befragung von Zeitzeugen und insbesondere auch durch die Nutzung von Archivbeständen des Hessischen Staatsarchivs in Darmstadt sowie des Hauptstaatsarchivs in Wiesbaden erhoben. Dabei wurden hauptsächlich Unterlagen der ehemaligen Kreisämter benutzt. Die üblichen Nutzungsbeschränkungen, die als Auflagen gegenüber Forschern auch bei den hessischen Staatsarchiven üblich sind, wurden akzeptiert.

Bei den Interessenten an personenbezogenen Informationen aus dieser Liste handelt es sich zum einen um Angehörige, zum anderen aber auch um Regionalforscher und Schulen, die Interesse an ortsbezogener Forschung über die Zeit des Dritten Reiches haben und zu diesem Zweck konkrete Informationen über ortsnahe ehemalige KZ-Insassen nutzen wollen.

Der LfD beantwortete die Frage nach der Zulässigkeit von Übermittlungen und sonstigen Nutzungen dieser Informationen wie folgt:

Zunächst sind bei der Nutzung der aus den Archiven stammenden Daten die Nutzungsbeschränkungen zu beachten, die durch die Archive selbst als Auflage der Benutzung formuliert worden sind. Möglicherweise ergibt sich daraus schon, daß Auskünfte über persönliche Verhältnisse Betroffener an Dritte grundsätzlich auf der Basis der aus den Archivalien erhobenen Informationen nicht zulässig sind, sondern daß diese vielmehr unmittelbar über das jeweilige Archiv erfolgen müssen.

Unabhängig davon ist von der Landeszentrale für politische Bildung bezüglich der Nutzung der bei ihr vorhandenen personenbezogenen Daten ergänzend das (rheinland-pfälzische) LDSG zu beachten.

Eine seiner Anwendungsvoraussetzungen ist, daß die Daten lebende natürliche Personen betreffen. Bei einem Großteil der ehemaligen KZ-Häftlinge wird dies nicht der Fall sein, zu einem hohen Prozentsatz wird es sich um inzwischen verstorbene Personen handeln. Soweit dies der Fall ist, findet das LDSG keine Anwendung. Wenn allerdings unbekannt ist, ob die betroffene Person verstorben ist, ist das LDSG im Zweifel anzuwenden. Dann kommt für die hier in Rede stehenden Auskünfte als Übermittlungsgrundlage allein § 16 LDSG in Frage. Die Übermittlungsalternativen des § 16 Abs. 1 Nr. 1 und Nr. 2 kommen nicht in Betracht, da der Katalog des § 12 Abs. 4, der hierin in Bezug genommen wird, keinen Fall enthält, der im vorliegenden Zusammenhang relevant sein kann.

Nach § 16 Abs. 1 Nr. 3 LDSG ist die Übermittlung an eine private Stelle auch zulässig, wenn der Empfänger ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zur Annahme besteht, daß über-

wiegende schutzwürdige Interessen der Betroffenen entgegenstehen. Diese Alternative kann eine Rolle spielen, wenn Angehörige die Information haben wollen, ob ein Verwandter Insasse des KZ Osthofen gewesen ist. In diesen Fällen kann die Information im Einzelfall Voraussetzung dafür sein, Rechtsansprüche geltend zu machen. Hier wäre die Übermittlung zulässig.

Für die Übermittlung an Regionalforscher zur Erstellung von Ortschroniken oder an Schüler und Lehrer zur ortsnahen Erforschung der NS-Zeit gibt § 16 Abs. 1 Nr. 3 LDSG jedoch keine Rechtsgrundlage, da die hier in Rede stehenden Interessen nicht als rechtliche Interessen angesehen werden können. Auch § 16 Abs. 1 Nr. 4 kommt wohl kaum in Betracht, da danach Voraussetzung der Übermittlung ist, daß die Betroffenen vor der Übermittlung unterrichtet werden und der Übermittlung nicht widersprochen haben. Diese Regelung käme nur dann zum Tragen, wenn die derzeitige Anschrift der ehemaligen KZ-Häftlinge bekannt wäre und sie vor der Übermittlung entsprechend befragt werden könnten.

Zusammenfassend gilt also folgende Rechtslage:

Soweit die betroffenen Personen verstorben sind, ist das LDSG nicht anwendbar. Dann gilt für die aus öffentlich zugänglichen Quellen entnommenen Daten keine datenschutzrechtliche Nutzungsbeschränkung, für die Archivdaten gelten allerdings die von den Ursprungsarchiven auferlegten Schranken. Soweit es sich um Daten Lebender oder möglicherweise noch Lebender handelt, kommt – unabhängig davon, aus welchen Quellen die Daten stammen – eine Übermittlung an Private nur in Betracht, wenn der Datenempfänger ein rechtliches Interesse geltend macht (Fall der Angehörigen) oder wenn der Betroffene der Übermittlung nach Unterrichtung nicht widersprochen hat (Fälle des § 16 Abs. 1 Nr. 3 und 4 LDSG).

In anonymisierter Form dürfen die Daten aus datenschutzrechtlicher Sicht ohne Einschränkungen genutzt werden.

8.4 Einsichtsrecht in das Denkmalbuch gem. § 10 Abs. 3 DSchPflG

§ 10 Abs. 3 DSchPflG bestimmt, daß die Einsicht in das Denkmalbuch jedermann gestattet ist. Nach § 10 Abs. 2 DSchPflG werden in das Denkmalbuch die geschützten Kulturdenkmäler (gem. § 8 Abs. 1) eingetragen. Nach § 8 Abs. 1 DSchPflG werden Kulturdenkmäler durch Verwaltungsakt unter Schutz gestellt, soweit sie nicht Denkmalzonen sind. Der Begriff des Kulturdenkmals wird in § 3 DSchPflG definiert. Danach sind Kulturdenkmäler entweder unbewegliche oder bewegliche Gegenstände, die unter bestimmten Aspekten besonders bedeutsam sind.

Das Eigentum an Kulturdenkmälern ist damit nicht angesprochen; die Information darüber gehört nicht zur Definition oder zur unabdingbaren näheren Bezeichnung eines Kulturdenkmals.

Aus der Sicht des LfD geht der Gesetzgeber davon aus, daß das Denkmalbuch die Gegenstände bezeichnet, die als Kulturdenkmal festgestellt worden sind. Daß Name und Anschrift des jeweiligen Eigentümers hierzu gehören sollten, ergibt sich aus dem Gesetz nicht.

Demnach ist auch die öffentliche Zugänglichkeit des Denkmalpflegebuchs auf die Merkmale beschränkt, die nach dem Gesetz in das Denkmalbuch einzutragen sind. Eine Verwaltungsvorschrift kann die Reichweite des Einsichtstatbestandes nicht über die gesetzliche Regelung hinaus erweitern. Wenn die Verwaltung aus Gründen der Erleichterung der eigenen Arbeit die Namen und Anschriften der Eigentümer mit in das Denkmalbuch aufnimmt, so folgt daraus also noch nicht, daß sich auch die Zugänglichkeitsvorschrift des § 10 Abs. 3 DSchPflG auf diese Zusatzinformationen bezieht.

Bei der Einsichtnahme sind also die Namen und Anschriften der Eigentümer grundsätzlich verdeckt zu halten. Eine Übermittlung dieser Informationen an Dritte wäre nur zulässig, wenn im jeweiligen Einzelfall die Übermittlungsvoraussetzungen des LDSG (§§ 14 oder 16 LDSG) vorlägen. Das Ministerium für Kultur, Jugend, Familie und Frauen hat dieser Auffassung zugestimmt und die Denkmalschutzämter des Landes entsprechend unterrichtet.

8.5 Bibliotheksdaten

8.5.1 Übermittlungen von Ausleihdaten durch eine Universitätsbibliothek an andere Nutzer

Eine Universitätsbibliothek wollte dann, wenn Buchtitel aus dem sog. „Präsenzbestand" (der grundsätzlich von der Ausleihe ausgeschlossen ist) ausnahmsweise doch ausgeliehen wurden (insbesondere an Professoren oder andere Mitglieder des Lehrkörpers), andere Interessenten an einem ausgeliehenen Titel jeweils informieren, wer der jeweilige Entleiher war.

Auf der Basis der geltenden Bibliotheksordnung der betroffenen Universität (die als universitäre Satzung anzusehen ist) konnte der LfD akzeptieren, daß die Ausleihe bestimmter Buchtitel mit der Auflage verbunden wurde hinzunehmen, daß Interessenten über den Entleiher von Präsenzbeständen informiert werden. Diese Auflage war verbindlich und deutlich gegenüber den Ausleihern anzuordnen.

Die Bibliothek wollte diese Information über die Entleiher allerdings jedem Bibliotheksnutzer im Wege des Direktzugriffs (Online-Zugriff) im automatisierten Katalog zur Verfügung stellen. Dies ist aus datenschutzrechtlicher Sicht problematisch:

Hierfür fehlte eine ausdrückliche Rechtsgrundlage in der Bibliotheksordnung, und § 7 LDSG mit seiner Regelung über Direktabrufverfahren ist grundsätzlich nicht auf Verfahren anwendbar, die Privaten den Datenzugriff ermöglichen. Eine Regelung auf der Grundlage der Einwilligung schied ebenfalls aus: Das Einverständnis ist nur dann eine wirksame rechtliche Grundlage für den Eingriff in Rechte, wenn die Einwilligung völlig freiwillig erteilt wird. In den Fällen, in denen auch faktische Nachteile bei der Verweigerung der Einwilligung entstehen, kann die Einwilligung nicht legitimierend wirken.

Dies war vorliegend aber der Fall: Entleiher von Präsenzbeständen, die mit der Aufnahme in das automatisierte Abrufsystem nicht einverstanden waren, sollten nicht am Ausleihsystem für Präsenzbestände teilnehmen dürfen. Dies ist nach Auffassung des LfD wirksam nur in einer Rechtsgrundlage (vorliegend der Benutzungsordnung der Bibliothek) regelbar.

Der konkret zu beurteilende Fall war allerdings von Besonderheiten gekennzeichnet, die es aus der Sicht des LfD rechtfertigten, übergangsweise (bis zu einer entsprechenden geplanten Änderung der Bibliotheksordnung) auch eine Verfahrensweise auf der Basis einer „Einwilligung" (die aus den genannten Gründen eher als qualifizierte Information der Betroffenen anzusehen war) zu tolerieren. Der Einsatz eines Online-Abrufsystems begründete zwar gegenüber anderen Verfahren, die geeignet sind, die Nutzer zu informieren (etwa gegenüber dem Einsatz von Stellvertretern in den Regalen oder den Auskünften auf gezielte Anfrage), eine erhöhte Wahrscheinlichkeit, daß überflüssige Offenbarungen erfolgen. Dadurch wurden die Entleiher aber nicht wesentlich oder schwerwiegend zusätzlich belastet. Vor diesem Hintergrund hat der LfD eine entsprechende Verfahrensweise nicht beanstandet, die im Vorgriff auf eine konkret geplante Änderung der Bibliotheksordnung erfolgt ist.

8.5.2 Löschung der Ausleihdaten

Im Zusammenhang mit der Anmeldung von Verfahren zur Bibliotheksautomatisierung hat der LfD sich immer wieder mit der Frage zu befassen, nach welchem Zeitraum die Ausleihdaten, d. h. die Information darüber, welcher Benutzer welches Medium ausgeliehen hat, zu löschen sind (zur mangelhaften technischen Absicherung von Ausleihdaten bei einer Universitätsbibliothek s. Tz. 21.2.7).

Gemäß § 19 Abs. 2 LDSG sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die datenverarbeitende Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

Aus dem Benutzerverhalten können Rückschlüsse auf höchstpersönliche Interessen, Neigungen, Vorlieben und Charaktereigenschaften gezogen werden. Außerdem können auch buchbezogene Auswertungen, wer ein bestimmtes Buch ausgeliehen hatte (z. B. zu Themen wie AIDS, Sprengstoffherstellung, nationalistisches Gedankengut o. ä.), gemacht werden, die sensible personenbezogene Informationen zum Ergebnis haben können.

Auch unter Berücksichtigung des Arguments, bei Beschädigungen eines Mediums müsse nachvollziehbar sein, wer der letzte Ausleiher war, ist keine längere Speicherungsdauer als sechs Monate erforderlich. Je länger der Zeitpunkt der Rückgabe zurückliegt, desto weniger dürfte bei einer späteren Feststellung einer Beschädigung eines Buches die Information darüber, wer Vorentleiher war, dazu führen, daß ein entsprechender Regreßanspruch durchsetzbar wäre. Die Beweislage dürfte grundsätzlich nicht so sein, daß nach Ablauf dieser Frist noch eine Beschädigung einem bestimmten Vorentleiher zuordenbar wäre. Zu weiteren technisch-organisatorischen Fragen bei einem automatisierten Bibliotheksdatenverarbeitungssystem s. u. Tz. 21.2.7.

9. Umweltschutz

9.1 Novelle des Landesabfallwirtschafts- und Altlastengesetzes

Im Berichtszeitraum ist das Kreislaufwirtschafts- und Abfallgesetz in Kraft getreten. Ziel ist die Neuordnung der Abfallentsorgung. Aufgrund der umfassenden bundesrechtlichen Änderungen bestand die Notwendigkeit, das Landesabfallrecht entsprechend anzupassen. In diesem Zusammenhang hat das Ministerium für Umwelt und Forsten den LfD auf der Grundlage der eingebrachten Entwürfe zum Landesabfallwirtschafts- und Altlastengesetz um Bewertung der Frage gebeten, ob eine spezifische Regelung über die Datenerhebung, -übermittlung und sonstige Verarbeitung für den Vollzug des Abfallrechts erforderlich ist. Bislang waren außerhalb des Altlastenbereiches keine spezifischen datenschutzrechtlichen Regelungen vorgesehen.

Der LfD hat unter Bezugnahme auf die verfassungsgerichtliche Rechtsprechung insbesondere die folgenden Überlegungen angestellt:

Das der Abfallwirtschaftsplanung zukommende überwiegende Allgemeininteresse dokumentiert sich im Ziel des im Oktober 1996 in Kraft getretenen Kreislaufwirtschafts- und Abfallgesetzes, das die umfassende Neuordnung der Abfallentsorgung zum Inhalt hat. Das Gesetz übernimmt wortgleich den EG-Abfallbegriff, wie er in Art. 1 a der Abfallrahmenrichtlinie der EG

(91/156/EWG) festgelegt ist. Damit wird gewährleistet, daß es bei der Umsetzung und dem Vollzug der EG-Abfallverbringungsverordnung, die seit dem 6. Mai 1994 die grenzüberschreitende Verbringung von Abfällen regelt, nicht zu Widersprüchen zwischen nationalem und europäischem Recht kommt. Das Kreislaufwirtschafts- und Abfallgesetz erfaßt in seinem Anwendungsbereich sowohl Abfälle zur Beseitigung als auch Abfälle zur Verwertung. Abfälle werden hierzu unterschieden nach „besonders überwachungsbedürftig", „überwachungsbedürftig" und „nicht überwachungsbedürftig". In § 3 KrW-/AbfG ist bestimmt, daß alle beweglichen Sachen, deren sich ihr Besitzer entledigt, entledigen will oder entledigen muß, Abfälle sind. Im Gegensatz zu der „alten" Nomenklatur des Abfallartenkatalogs folgt der in das deutsche Recht eingeführte europäische Abfallkatalog daher im wesentlichen einer herkunftsorientierten Zuordnung. Das Kreislaufwirtschafts- und Abfallgesetz macht also mit dem Verursacherprinzip ernst. Richteten sich im außer Kraft getretenen Abfallgesetz die Regelungen zur Verwertung und sonstigen Entsorgung im wesentlichen an die öffentlich-rechtlichen Entsorgungsträger, werden nun im Grundsatz die Erzeuger und Besitzer von Abfällen selbst zur Vermeidung, Verwertung und Beseitigung verpflichtet. Den Abfallerzeugern und Abfallbesitzern wird die Möglichkeit eingeräumt, ihre Entsorgungspflichten eigenverantwortlich wahrzunehmen oder hierzu Dritte, Verbände oder Einrichtungen der Wirtschaft einzuschalten. In diesem Zusammenhang wird es vermehrt Sachverhalte geben, die personenbezogene oder personenbeziehbare Datenerhebungen erforderlich machen. Hinzu kommt, daß der Kreis der Aufgabenträger, und entsprechend der Kreis der zur Datenverarbeitung Berechtigten, gewachsen ist. Aus diesen Gründen war es nach Auffassung des LfD durchaus sinnvoll, bereichsspezifische Regelungen zum Datenschutz aufzunehmen.

Nunmehr soll mit § 31 LAbfWAG des Gesetzentwurfs der Landesregierung für den Vollzug des Abfallrechts eine bereichsspezifische Regelung geschaffen werden. Vorkehrungen zur Mißbrauchssicherung sind durch die Festlegung der Zwecke (so u. a. die Überwachung und Durchführung der Abfallentsorgung, die Durchführung der Abfallwirtschaftsplanung, die Durchführung von Anzeige-, Genehmigungs-, Planfeststellungs- und sonstigen Zulassungsverfahren im Bereich der Abfallentsorgung) sowie durch den Verweis auf die ergänzende Geltung der Vorschriften des LDSG in hinreichender Weise getroffen. Was die Zulassung der Datenerhebung ohne Kenntnis der Betroffenen anbelangt, so regelt § 31 Satz 2 ausdrücklich, daß solche Datenerhebungen nur dann erfolgen dürfen, wenn andernfalls die Erfüllung der in Satz 1 genannten Zwecke gefährdet würde.

9.2 Datenübermittlung aus dem Klärschlammkataster

Ein Kulturamt hat in einer Ortsgemeinde ein Flurbereinigungsverfahren durchgeführt und in diesem Zusammenhang Einsicht in das bei der Verbandsgemeinde geführte Klärschlammkataster begehrt. Der Bürgermeister der Verbandsgemeinde fragte an, ob die Einsichtnahme in das Klärschlammkataster zur Erfüllung der Aufgaben der Flurbereinigungsbehörde notwendig ist. Nach dem vorgetragenen Sachverhalt war davon auszugehen, daß aufgrund der Zuordenbarkeit des entsprechenden Grundstücks zu einer lebenden, natürlichen Person personenbezogene Daten im Sinne von § 3 Abs. 1 LDSG betroffen sind. In § 5 Abs. 1 Nr. 1 LDSG ist geregelt, daß die Verarbeitung personenbezogener Daten dann zulässig ist, wenn die Betroffenen in diese Verarbeitung eingewilligt haben. Weiterhin ist die Verarbeitung nach Abs. 1 Nr. 2 auch ohne Einwilligung möglich, wenn die Verarbeitung personenbezogener Daten aufgrund einer Regelung des LDSG oder einer sonstigen Rechtsvorschrift erlaubt ist. Die Übermittlung personenbezogener Daten an öffentliche Stellen ist nach § 14 LDSG zulässig, wenn dies entweder für Aufgaben des Empfängers oder für Aufgaben der übermittelnden Stelle erforderlich ist und wenn die Voraussetzungen vorliegen, die ausnahmsweise eine Zweckänderung erlauben. Diese Voraussetzungen sind insgesamt in elf Fallgruppen in den §§ 12 Abs. 4 und 13 Abs. 2 LDSG geregelt. Die Notwendigkeit einer entsprechenden Datenübermittlung kann sich insbesondere in jenen Fällen ergeben, in denen eine Überprüfung der Angaben Betroffener notwendig erscheint oder dies wegen eines überwiegenden Interesses der Allgemeinheit oder von dritten Personen erforderlich ist. Eine Möglichkeit, auf dieser Grundlage die Einsichtnahme in das Klärschlammkataster für zulässig zu erachten, sah der LfD nicht.

Gemäß der spezialgesetzlichen Regelung in § 135 FlurbG hat die Verbandsgemeindeverwaltung der Flurbereinigungsbehörde Rechts- und Amtshilfe zu gewähren sowie Auskünfte zu erteilen. Auch hier ist die Einsichtnahme nicht erfaßt. Es war in diesem Zusammenhang indessen zu berücksichtigen, daß gem. § 44 Abs. 4 FlurbG die Landabfindung eines Teilnehmers in der Nutzungsart, Beschaffenheit und Bodengüte seinen alten Grundstücken entsprechen soll.

Hier wird die Funktion der Flurbereinigungsbehörde als „Wertermittlungsbehörde" deutlich, so daß die Auskunftsregelung in § 135 FlurbG nach Auffassung des LfD die Mitteilung der Verbandsgemeindeverwaltung an die Flurbereinigungsbehörde, auf welche von der Flurbereinigung betroffene Grundstücke Klärschlamm aufgebracht wird, umfaßt. Diese Sichtweise wird auch durch die Ausführungen der Landesregierung zur Klärschlammkonzeption für Rheinland-Pfalz gestützt (vgl. Landtagsdrucksache 13/566). Dort wird auf das Gesetz zur Vermeidung, Verwertung und Beseitigung von Abfällen vom 27. September 1994 (BGBl. I S. 2705 ff.) hingewiesen, das im Düngemittelgesetz eine Ermächtigungsgrundlage zur Errichtung eines Entschädigungsfonds für durch die Klärschlammverwertung entstehende Sach- und Folgeschäden schafft. Darin kommt zum Ausdruck, daß die Klärschlammaufbringung als Faktor bei der Ermittlung der Bodengüte eine Rolle spielen kann.

9.3 Einsicht in das Altlastenkataster

In einer Stadt war der Bau eines Sport- und Freizeithallenbades im Gespräch. Wegen einem der möglichen Standorte hat ein Mitglied des Sportausschusses des Stadtrats bei dem städtischen Umweltamt Einsicht in das Altlastenkataster verlangt. Die

Ablehnung dieses Begehrens führte zu einer Anfrage an den LfD. Dieser äußerte sich wie folgt: Aus der Sicht des Datenschutzes geht es um die Sicherung des Rechts auf informationelle Selbstbestimmung. So können umweltbezogene Informationen sensible personenbezogene Daten enthalten. Die Frage, ob personenbezogene Umweltdaten offenbart werden dürfen, richtete sich im vorliegenden Fall nach den speziellen Regelungen im Abfallwirtschafts- und Altlastengesetz, das die Einrichtung und den Betrieb der 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 für ihren Bezirk das Verdachtsflächen- und Altlastenkataster. Nach Abs. 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, Gefahrenabwehr, Überwachung und Planung gesetzlich obliegenden Aufgaben übermittelt werden. In diesem Zusammenhang war auch § 33 GemO zu beachten, der das Unterrichtungsrecht des Gemeinderats regelt und damit grundsätzlich Informationseingriffe rechtfertigt. Mithin könnte zwar nach dieser Vorschrift das Mitglied des Sportausschusses als Übermittlungsempfänger in Betracht kommen. Da es sich jedoch bei den gespeicherten Flächen um Verdachtsflächen handelt – es steht also gegenwärtig noch nicht fest, ob die Fläche letztlich als Altlast eingestuft wird – waren nach Auffassung des LfD 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 Grundstückeigentümer oder Nutzungsberechtigten existenzgefährdend sein. Nach allem hat der LfD im vorliegenden Fall eine Übermittlung als unzulässig angesehen.

9.4 Zustellung von Gebührenbescheiden per Infopost

Ein Petent beklagte, daß die für ihn zuständige Kreisverwaltung die Versendungsform der (preiswerten) Infopost nutze, um Gebührenbescheide für Abfallentsorgung zu übersenden; wobei hier seitens der Deutschen Post AG die Möglichkeit besteht, verschlossene Sendungen stichprobenweise daraufhin zu prüfen, ob die Bedingungen für den Versand mittels Infopost eingehalten wurden.

Die in § 9 LDSG für alle öffentlichen Stellen begründete allgemeine Verpflichtung, die zur Ausführung der Datenschutzvorschriften erforderlichen technischen und organisatorischen Maßnahmen zu treffen, bezweckt den Schutz des Rechts auf informationelle Selbstbestimmung Betroffener beim Umgang mit ihren personenbezogenen Daten. Es ist Aufgabe der für die Organisation zuständigen Stelle, bei der Einführung einer neuen Verfahrensweise die für den ordnungsgemäßen Ablauf erforderlichen Maßnahmen zu treffen. Insoweit ist der datenverarbeitenden Stelle ein gewisser Gestaltungsspielraum hinsichtlich der zu treffenden Festlegungen eingeräumt. Des weiteren ist nach § 9 Abs. 1 Satz 2 LDSG der Grundsatz der Verhältnismäßigkeit zu berücksichtigen. Damit soll sichergestellt werden, daß bei der Festlegung der nach § 9 Abs. 1 zu treffenden Maßnahmen die bei realistischer Betrachtungsweise bestehenden Risiken für eine Verletzung der Rechte der Betroffenen abgewogen werden mit dem entsprechenden finanziellen Aufwand beispielsweise für andere Versendeformen oder für zusätzliche Vorkehrungen bei dem Versand von amtlichen Schriftstücken. Im Rahmen dieser Abwägung sind insbesondere die Art der personenbezogenen Daten und die Wahrscheinlichkeit einer etwaigen mißbräuchlichen Datennutzung zu berücksichtigen. Der Spielraum ist um so größer, je milder die Beeinträchtigung ausfällt.

Im vorliegenden Fall führte die Abschätzung der möglichen Risiken zu dem Ergebnis, daß die Beeinträchtigung des Rechts auf informationelle Selbstbestimmung von vergleichsweise geringem Gewicht ist. Angesichts des Massengeschäfts „Infopost" bleibt das stichprobenweise Öffnen einer Sendung auf wenige Einzelfälle beschränkt. In diesen seltenen Fällen erhält der Absender die Sendung zurück, um sie wieder ordnungsgemäß verschließen zu können. Im vorliegenden Fall waren die Daten aus der Abrechnung für die Abfallentsorgung aus Sicht des LfD nicht sehr sensibel. Denn aufgrund der jeweiligen Abfallgebührensatzung stehen die für die einzelnen Haushalte anfallenden Gebühren fest. Eine andere Einschätzung würde sich beispielsweise bei dem Versand von Einkommensteuerbescheiden per Infopost ergeben, da hier äußerst sensible Daten enthalten sind, die Rückschlüsse auf die Einkommensverhältnisse und individuelle Abschreibungstatbestände erlauben.

Nach allem war nach Auffassung des LfD das von der Kreisverwaltung gewählte Verfahren des Versands der Gebührenbescheide für Abfallentsorgung per Infopost nicht zu beanstanden.

9.5 Datenschutzrechtliche Belange bei der Aufstellung eines Flächennutzungsplans

Im Rahmen der Aufstellung eines Flächennutzungsplans hat eine Stadtverwaltung die Frage des Datenschutzes bei der Neuaufstellung eines – öffentlich einsehbaren und zugänglichen – Flächennutzungsplanes, insbesondere hinsichtlich der Kennzeichnung von Flächen mit Bodenbelastungen, an den LfD herangetragen.

Aufgrund des dargestellten Sachverhalts war davon auszugehen, daß Grundstücke eindeutig identifiziert werden konnten. Datenschutzrechtlich relevant ist dies insoweit, als die Plandarstellung Rückschlüsse auf einzelne natürliche lebende Personen im Sinne von § 3 Abs. 1 LDSG zuläßt, etwa dergestalt, daß aus den entsprechenden Plänen die Lage einzelner Grundstücke und mittelbar ihre Eigentümer erkennbar sind. Für diese Fälle ist in § 32 Abs. 3 LDSG klargestellt, daß eine Veröffentlichung, eine Übermittlung oder eine sonstige Offenbarung nur zulässig ist, wenn die Betroffenen eingewilligt haben oder dies für die Darstellung der Planungsergebnisse unerläßlich ist und überwiegende schutzwürdige Interessen der Betroffenen nicht entgegenstehen. Die Voraussetzungen für die Offenbarung personenbezogener Daten nach § 32 Abs. 3 Nr. 2 LDSG waren nach Auffassung des LfD gegeben. Denn der Zweck des nach § 5 Abs. 3 Nr. 3 BauGB zu beachtenden Kennzeichnungserfordernisses – wonach zur baulichen Nutzung vorgesehene Flächen, deren Böden erheblich mit umweltgefährdenden Stoffen belastet sind, zu kennzeichnen sind – liegt in der Schutzfunktion mit Blick auf den weiteren Vollzug der Bauleitplanung. So dienen Kennzeichnungen dem Schutz künftiger baulicher oder sonstiger Nutzungen des Grundstücks, indem sie den späteren Nutzer auf mögliche Gefährdungen der planerisch vorgesehenen Nutzung hinweisen. Die in der Planstufe der Flächennutzungsplanung vorgenommene Gefährdungsabschätzung ermöglicht es aber gerade auch dem Eigentümer des möglicherweise unter die entsprechende Kennzeichnung fallenden Grundstücks, auf den Gang der weiteren Planung Einfluß zu nehmen – etwa dadurch, daß beispielsweise Fehler bei der Tatsachenermittlung aufgedeckt werden können.

Mithin standen datenschutzrechtliche Belange der Aufstellung des Flächennutzungsplanes nicht entgegen.

10. Gesundheitswesen

a) Gesetz zur Neuordnung seuchenrechtlicher Vorschriften

Das Bundesministerium für Gesundheit hat den Referentenentwurf eines Gesetzes zur Neuordnung seuchenrechtlicher Vorschriften erstellt. Die Maßnahme zielt auf eine Verbesserung der Infektionsepidemiologie und eine höhere Effizienz des öffentlichen Gesundheitsdienstes. So soll beispielsweise ein epidemiologisches Informationsnetz auf Bundesebene aufgebaut und die Meldepflicht für bestimmte Krankheiten präzisiert werden.

Der LfD teilte dem Ministerium für Arbeit, Soziales und Gesundheit mit, daß keine grundsätzlichen Bedenken gegen den Entwurf bestünden, insbesondere aber unter dem Aspekt der Normenklarheit in einer Reihe von Punkten Nachbesserungsbedarf bestehe. Dies betrifft vor allem die Datenschutzvorschrift des § 72, die die erforderlichen engen Zweckbindungs- und Übermittlungsvorschriften vermissen läßt.

b) Transplantationsgesetz

Nachdem auch der Bundesrat zugestimmt hat, tritt das Transplantationsgesetz wie geplant am 1. November 1997 nach langen schwierigen Beratungen in Kraft. Ziel des Gesetzes ist vor allem, die Spendebereitschaft in der Bevölkerung für dringend benötigte Organe zu erhöhen und eventuelle Mißbräuche, wie z. B. den Organhandel, zu verhindern. Aus datenschutzrechtlicher Sicht ist zu begrüßen, daß das Gesetz eine enge Zweckbindungsvorschrift enthält und sicherstellt, daß die Angehörigen eines Organspenders den Namen des Organempfängers und der Organempfänger den Namen des Organspenders grundsätzlich nicht erfahren dürfen. Die 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte am 14./15. März 1996 eine Entschließung verabschiedet, die in der schwierigen Frage der Einwilligung eine „enge Zustimmungslösung" forderte. Dies bedeutet, daß eine ausdrückliche Zustimmung des Organspenders für eine Organentnahme erforderlich ist. Diese Lösung stellte nach Auffassung der Datenschutzbeauftragten den geringsten Eingriff in das Recht auf informationelle Selbstbestimmung dar. Der Gesetzgeber hat sich jedoch für die „erweiterte Zustimmungslösung" entschieden, wonach der nicht dokumentierte Wille des Spenders bei den Angehörigen erforscht werden kann. Da aber auch diese Lösung den potentiellen Spender nicht zwingt, eine Ablehnung zu dokumentieren, wie dies bei der Widerspruchs- oder Informationslösung der Fall gewesen wäre, hat das Recht auf informationelle Selbstbestimmung hinreichend Berücksichtigung gefunden.

c) Transfusionsgesetz

In eine ähnliche Richtung geht der vorliegende Entwurf eines Transfusionsgesetzes (Stand 29. Juli 1997). Ziel des Gesetzes ist eine gesicherte Versorgung der betroffenen Patienten mit Blut sowie der Schutz der spendenden Person und der Blutprodukte. Die datenschutzrechtliche Kritik richtete sich in erster Linie gegen die unzureichenden Anforderungen an die Einwilligung des Spenders. Insbesondere wird nunmehr klargestellt, daß eine Einwilligung zur Blutentnahme keinesfalls auch die Einwilligung zur Datenübermittlung bedeutet, wie dies ursprünglich vorgesehen war. Weitere Forderungen betreffen die Anonymisierung von Daten, insbesondere wenn diese übermittelt werden.

10.1 Öffentlicher Gesundheitsdienst

Im 15. Tb. berichtete der LfD unter Tz. 10.2.1 über die Vorarbeiten an dem Gesetz über den öffentlichen Gesundheitsdienst. Dieses Gesetz wurde im November 1995 verabschiedet und trat mit seinen wesentlichen Bestimmungen am 1. Januar 1996 in Kraft. Die von dem federführenden Ressort zunächst ins Auge gefaßte datenschutzrechtliche Minimallösung wurde nicht realisiert; das Gesetz enthält in den §§ 11 ff. angemessene Regelungen über den Datenschutz. In den rund eineinhalb Jahren der

Gesetzesanwendung zeigte sich, daß datenschutz- und praxisgerechte Lösungen für einen Schwerpunktbereich des Datenschutzes gefunden wurden. Eine Ausnahme bildet indessen der Vorgang, über den nachfolgend unter Tz. 10.1.1 berichtet wird. Es ist bedauerlich, daß trotz einer gesetzlichen Regelung, die den Konflikt zwischen Organisationshoheit und Arztgeheimnis vermeiden wollte (§ 11 Abs. 6 ÖGdG), eine so banale Sache wie der Postlauf in der Kreisverwaltung zum Datenschutzproblem werden konnte.

Auch das Landesgesetz für psychisch kranke Personen wurde im Berichtszeitraum verabschiedet und trat am 1. Januar 1996 in Kraft. Seine datenschutzrechtlichen Regelungen (§§ 32 ff.) sind im Ergebnis ebenso positiv zu beurteilen wie die des Landesgesetzes über den öffentlichen Gesundheitsdienst. Über die Novellierung des Heilberufsgesetzes wird unter Tz. 10.6.1 berichtet. Zur Zeit berät der LfD die Landesärztekammer in datenschutzrechtlichen Fragen, die im Zusammenhang mit einer Neufassung der Berufsordnung für die Ärzte aufgetreten sind.

10.1.1 Arztpost auf dem Schreibtisch des Landrats

Am 1. Januar 1997 wurden die Aufgaben der unteren Gesundheitsbehörden auf die Kreisverwaltungen übertragen, d. h. den Landräten stehen nun Leitungs- und Organisationsbefugnisse für die Gesundheitsämter zu. In Wahrnehmung dieser neuen Befugnisse ordneten Landräte an, daß die gesamte eingehende Post zunächst in der Kreisverwaltung geöffnet, ihnen zur Kenntnis gegeben und erst dann an den Gesundheitsamtsleiter weitergegeben wird. Bis zur Aufgabenübertragung auf die Kreisverwaltungen wurde die Post in den Gesundheitsämtern unmittelbar dem Amtsleiter – einem Arzt – vorgelegt.

Nach Meinung des LfD müssen nach der bestehenden Gesetzeslage (§ 11 Abs. 6 ÖGdG) Postsendungen, die den durch das Arztgeheimnis geschützten Bereich der amtsärztlichen Tätigkeit betreffen, unmittelbar, d. h. ohne den Umweg über den Landrat, dem Leiter des Gesundheitsamtes vorgelegt werden. Da ungeöffnete Postsendungen nur in Ausnahmefällen erkennen lassen, ob sie medizinische Informationen enthalten, die in die Zuständigkeit der Amtsärzte fallen, müssen bei einer Lösung des Problems die gegenüber der Leitungs- und Organisationsbefugnis eines Landrats höherwertigen Rechtsgüter, nämlich das Grundrecht auf Datenschutz und das Arztgeheimnis, Vorrang haben. Gestützt auf diese Überlegung forderte der LfD, daß alle nicht eindeutig als reine Verwaltungsvorgänge erkennbaren Postsendungen dem Gesundheitsamt in der Kreisverwaltung zugeleitet, dort geöffnet und nur dann, wenn sie keinen medizinischen Bezug haben, an den Landrat weitergegeben werden. Nur auf diese Weise kann zuverlässig gewährleistet werden, daß ärztliche Befundberichte, Untersuchungsergebnisse, fachärztliche Gutachten und Gerichtsakten mit medizinischen Informationen, die zusammen bis zu 80 % des Posteingangs eines Gesundheitsamtes ausmachen, unmittelbar dorthin gelangen, wo sie durch das Arztgeheimnis geschützt sind.

Der Vorschlag des LfD wurde in dieser Form nicht realisiert. Das Ministerium des Innern und für Sport unterstützte vielmehr den Vorschlag einer Fraktionsarbeitsgruppe, daß Bürger, Ärzte und Behörden, die mit einem Gesundheitsamt in Briefkontakt treten, ihre Briefsendungen auf dem Umschlag als „Arztsache" oder als „Vertraulich" kennzeichnen und damit bewirken, daß diese Post ungeöffnet in den ärztlichen Bereich des Gesundheitsamtes gelangt und daß eine besondere Verpflichtung des Personals der Posteingangsstellen der Kreisverwaltungen im Hinblick auf die besondere Sensibilität der datenschutzrelevanten Vorgänge im Gesundheitsamt erfolgt.

Das Ministerium unterrichtete den Vorsitzenden des Landkreistages über diese Vorschläge und bat, die Kreisverwaltungen entsprechend zu informieren.

Nun ist es sicherlich kaum möglich, das Problem in der Weise zu lösen, daß die Empfänger von Briefen darauf hingewiesen werden, wie diese zu adressieren sind. Da der Bevölkerung die notwendigen Zusätze zur Adressierung jedenfalls noch weitestgehend unbekannt waren, wies der LfD in einer Presseerklärung darauf hin, daß für den Amtsarzt bestimmte Mitteilungen mit „Arztsache" oder „Vertraulich" zu kennzeichnen sind, wenn vermieden werden soll, daß sie wie die sonstigen Posteingänge der Kreisverwaltung behandelt werden und Nichtberechtigten zur Kenntnis gelangen.

10.1.2 Auskunft und Akteneinsicht nach den Vorschriften des Landesgesetzes über psychisch kranke Personen

Nach § 32 Abs. 2 PsychKG ist Personen, über die Daten gespeichert sind, unentgeltlich

1. Auskunft über die im Zusammenhang mit der Durchführung von Hilfen, Schutzmaßnahmen und Unterbringungen zu ihrer Person gespeicherten Daten, auch soweit sie sich auf die Herkunft und die Personen und Stellen, an die die Daten übermittelt worden sind, beziehen, zu erteilen und
2. Einsicht in die im Zusammenhang mit der Durchführung von Hilfen, Schutzmaßnahmen und Unterbringungen zu ihrer Person geführten Akten zu gewähren.

Die Gewährung von Auskunft und Akteneinsicht kann unterbleiben, soweit und solange dies nach ärztlichem Zeugnis wegen einer Lebensgefahr oder einer Gefahr schwerwiegender gesundheitlicher Nachteile für die betroffene Person erforderlich ist (Absatz 3).

Der Gesetzgeber hat die Auskunfts- und Einsichtsrechte durch diese Regelungen eindeutig gestärkt: Nur besonders qualifizierte Gründe können die Ablehnung entsprechender Anträge rechtfertigen. Er folgte damit dem Bundesverfassungsgericht, das in der Auskunft und Einsicht ein Äquivalent zu den mit der automatisierten Datenverarbeitung einhergehenden Gefährdungen sah. Nur ein Betroffener, der weiß, welche Informationen die Verwaltung über ihn besitzt, kann seine Datenschutzrechte wahrnehmen.

Ein Gesundheitsamt verweigerte einem Betroffenen Akteneinsicht, weil sich die psychische Erkrankung, die bei ihm bestehe, aufgrund der Einsichtnahme „verschlimmern könne".

Der LfD erkannte diese Begründung nicht an. Eine bloße „Verschlimmerung" der Erkrankung ist nicht unter die Tatbestandsvoraussetzungen „Lebensgefahr" oder „schwerwiegende gesundheitliche Nachteile" zu subsumieren. Er forderte das Gesundheitsamt auf, das Vorliegen der Gründe nach § 32 Abs. 3 entweder durch ein ärztliches Zeugnis zu belegen oder die Akteneinsicht zu gewähren.

10.1.3 Vorlage der Einwilligungserklärung bei der Übersendung von Arztbriefen

Die Anfrage eines beamteten Arztes an den LfD betraf die Weitergabe von Informationen aus der ärztlichen Tätigkeit an niedergelassene Ärzte. Er wollte wissen, ob es genügt, daß sich der Arzt bei dem Übermittlungsersuchen auf eine vorliegende Erklärung über die Entbindung von der Schweigepflicht beruft oder ob es erforderlich ist, daß er die Schweigepflichtsentbindungserklärung im Original oder in Kopie vorlegt.

Wegen der über den konkreten Fall hinausreichenden Bedeutung der Sache in anderen, nicht der Kontrollzuständigkeit des LfD unterliegenden Bereichen wurde die Landesärztekammer Rheinland-Pfalz um eine Äußerung gebeten. Diese verwies auf § 2 Abs. 6 der Berufsordnung für die Ärzte in Rheinland-Pfalz, der folgenden Wortlaut hat: „Wenn mehrere Ärzte gleichzeitig oder nacheinander denselben Patienten untersuchen oder behandeln, so sind sie untereinander von der Schweigepflicht insoweit befreit, als das Einverständnis des Patienten anzunehmen ist." Die Berufsordnung unterstelle demnach im Regelfall, so die Landesärztekammer, daß der Patient mit der Einsichtnahme in Vorbefunde einverstanden sei, anderenfalls müßte er einen entgegenstehenden Willen ausdrücklich erklären. Sie folgerte hieraus, daß es einer Übersendung der Schweigepflichtsentbindungserklärung im Original oder in Kopie nicht bedürfe.

Der LfD schloß sich dieser Beurteilung im Grundsatz an, wies jedoch ergänzend darauf hin, daß es auch zu den Pflichten des um Offenbarung ersuchten Arztes gehöre, zu beurteilen, ob „das Einverständnis des Patienten anzunehmen ist." Wenn das Vorliegen einer schriftlichen Einwilligung in die Offenbarung medizinischer Daten nur behauptet, aber nicht durch Vorlage der Erklärung oder einer Kopie nachgewiesen wird, habe der vorbehandelnde Arzt selbst zu beurteilen, ob die Offenbarungsvoraussetzung der Berufsordnung vorliegt. Danach gibt es also keinen Automatismus bei der Weitergabe ärztlicher Informationen; der mit dem bloßen Hinweis auf eine Schweigepflichtsentbindungserklärung um Übermittlung ersuchte Arzt darf Informationen übermitteln, er ist hierzu aber nicht verpflichtet. Bestehen Zweifel am Vorhandensein oder der Rechtswirksamkeit einer Einwilligungserklärung, kann er die Informationsweitergabe von der Vorlage abhängig machen.

Solche Zweifel können insbesondere dann bestehen, wenn Datenanforderungen bei Ärzten nicht konkret formuliert sind. Die anfordernde Stelle muß spezifizieren, welche Unterlagen sie benötigt; der um Übermittlung ersuchte Arzt muß sich – im Sinne einer Plausibilitätsprüfung – ein Urteil darüber bilden, ob die Übermittlung medizinischer Daten in dem erbetenen Umfang erforderlich ist.

Im Ergebnis gleich zu beurteilen ist die Datenübermittlung durch Ärzte an Behörden – beispielsweise an die Versorgungsverwaltung –.

10.2 Methadonsubstitution; Anzeigen nach § 2 a Abs. 9 BtMVV

§ 2 a Abs. 9 BtMVV bestimmt, daß die Durchführung von Substitutionsmaßnahmen einschließlich der Einbindung in eine Begleittherapie vom behandelnden Arzt für jeden Patienten zu dokumentieren und der zuständigen Behörde anzuzeigen ist. Die Dokumentation ist auf Verlangen der zuständigen Landesbehörde zur Einsicht und Auswertung vorzulegen. Durch Landesverordnung vom 28. Juni 1994 wurden in Rheinland-Pfalz die Bezirksregierungen für zuständig erklärt.

Die Vorschrift will die Voraussetzungen dafür schaffen, daß die gleichzeitige Verschreibung eines Substitutionsmittels durch mehrere Ärzte für denselben Patienten verhindert und Kontrollen der zuständigen Landesbehörden ermöglicht werden.

Bei einer Bezirksregierung wurden nähere Feststellungen zur Handhabung des Anzeigeverfahrens in der Praxis getroffen. Im Vordergrund stand, welche Erkenntnisse aus einer Auswertung der Anzeigen gewonnen und welche Maßnahmen zur Aufdeckung von Mehrfachsubstitutionen eingeleitet werden.

Die Bezirksregierung wies die zur Substitutionsbehandlung zugelassenen Ärzte in größeren Zeitabständen, zuletzt im November 1996, auf die Anzeigepflichten nach der BtMVV hin. Die Hinweise blieben weitgehend wirkungslos; der letzte hatte zur Folge, daß nur ein Zehntel dieser Ärzte überhaupt Anzeigen vorlegte. Mit größerem zeitlichen Abstand zu den Hinweisen geht der Anteil der anzeigenden Ärzte noch weiter zurück. Mitarbeiter der Bezirksregierung bestätigten, daß auf dieser Grundlage die Zielsetzung des § 2 a Abs. 9 BtMVV nicht erreichbar ist. Die wenigen eingehenden Anzeigen werden in Akten abgeheftet; Kontrollmaßnahmen nach Anforderung der Dokumentation finden nicht statt. Die Aufgabenerfüllung wird weiter dadurch erschwert, daß wegen einer fehlenden Übermittlungsbefugnis für Anzeigedaten Mehrfachsubstitutionen dann nicht erkannt werden können, wenn ein Patient Ärzte im Zuständigkeitsbereich mehrerer Bezirksregierungen in Anspruch nimmt.

Der LfD wies in seiner Stellungnahme darauf hin, daß diese Situation unter Datenschutzgesichtspunkten nicht zu akzeptieren ist. Der mit der Übermittlung bzw. Verarbeitung dieser sensiblen Daten verbundene Eingriff in das Recht auf informationelle Selbstbestimmung könnte allenfalls dann verhältnismäßig sein, wenn sie tatsächlich für die Aufgabenerfüllung geeignet wären. Vor dem Hintergrund der Praxis sind sie es eindeutig nicht. Danach wäre zu fordern, daß die Beachtung der Anzeigepflicht mit allen zur Verfügung stehenden rechtlichen Mitteln durchgesetzt oder auf eine patientenbezogene Anzeige der Ärzte im Blick auf die Befugnis, im Einzelfall die Dokumentation einzusehen, verzichtet wird.

Soweit bekannt, beruht die Haltung der Ärzte in der Sache auf der – nicht zutreffenden – Annahme, daß mit der Anzeige das Arztgeheimnis verletzt werde. Diesem Vorbehalt könnte begegnet werden, wenn ein anonymisiertes Meldeverfahren eingeführt würde. Die Anonymisierung könnte in der Weise erfolgen, daß nur bestimmte Buchstaben-Zahlen-Kombinationen (Bestandteile des Namens und des Geburtsdatums) als Zuordnungsmerkmale verwendet werden. Da die Grundgesamtheit der Substitutionspatienten verhältnismäßig gering sein dürfte, ist davon auszugehen, daß Verwechslungen zuverlässig ausgeschlossen werden können und die zuständigen Behörden gleichwohl in der Lage wären, Mehrfachsubstitutionen zu erkennen. Auch das Problem der Inanspruchnahme von Ärzten im Zuständigkeitsbereich mehrerer Bezirksregierungen wäre lösbar, denn gegen eine Übermittlung und Auswertung von anonymisierten Anzeigen bestünden keine Bedenken. Zu einer Identifizierung von Patienten käme es erst dann, wenn das Vorhandensein einer Mehrfachsubstitution erkannt und die Dokumentation vom Arzt auf Verlangen der Bezirksregierung zur Auswertung vorgelegt wird.

Das Ministerium für Arbeit, Soziales und Gesundheit ließ die Absicht erkennen, diesen Vorschlag zu realisieren.

10.3 Schutz des Persönlichkeitsrechts der Frauen im Rahmen von Leistungen nach dem Schwangeren- und Familienhilfeänderungsgesetz

Mit dem Schwangeren- und Familienhilfeänderungsgesetz wurde der Forderung des Bundesverfassungsgerichts Rechnung getragen, daß in Fällen, in denen das Schutzkonzept der Beratungsregelung dies erfordert, bei Bedürftigkeit der Frau eine Kostenübernahme durch den Staat erfolgen soll. Erfüllt die Frau die Voraussetzungen des § 1 des Gesetzes zur Hilfe für Frauen bei Schwangerschaftsabbrüchen in besonderen Fällen, hat sie Anspruch auf Sachleistungen nach diesem Gesetz.

Die Abrechnung der Leistungen ist in hohem Maße datenschutzrelevant, denn eine patientenbezogene Abrechnung mit der zuständigen Landesbehörde – Landesamt für Soziales, Jugend und Versorgung – ließe dort eine außerordentlich sensitive zentrale Datensammlung entstehen. Das Ministerium zeigte großes Verständnis für dieses vom LfD vorgetragene Problem. Das Verfahren wurde so organisiert, daß bei der fallbezogenen Leistungsabrechnung sowohl zwischen dem Arzt und der Kassenärztlichen Vereinigung als auch zwischen dieser und dem Landesamt für Soziales, Jugend und Versorgung nur solche Daten weitergegeben werden, die keinen Personenbezug zulassen (Name der Krankenkasse, die die Bescheinigung über die Kostenübernahme ausgestellt hat, Wohnort der Patientin).

10.4 Datenschutz im Krankenhaus

10.4.1 Outsourcing und Fernwartung

Die wirtschaftlich schwierige Lage zwingt die Krankenhäuser nach neuen Wegen zu suchen, um ihre Aufgaben effizienter zu erfüllen. Im Zentrum der Überlegungen steht auch die automatisierte Datenverarbeitung. Wiederholt wurde an den LfD die Frage herangetragen, ob und in welchem Umfange es nach geltendem Datenschutzrecht zulässig ist, Datenverarbeitungsleistungen nicht selbst zu erbringen, sondern auf die Ressourcen Dritter zurückzugreifen. Gekennzeichnet werden diese Bestrebungen durch die Begriffe „Outsourcing" und „Fernwartung".

Diese Formen der Leistungserbringung sind von hoher Datenschutzrelevanz, dies insbesondere dann, wenn Stellen außerhalb des öffentlichen Bereichs in Anspruch genommen werden und wenn es diesen Stellen möglich ist, auf personenbezogene Daten zuzugreifen.

Im allgemeinen werden Outsourcing und Fernwartung als „Auftragsdatenverarbeitung" qualifiziert; ist ein Krankenhaus Auftraggeber, so ist § 36 Abs. 9 LKG einschlägig.

Vor dem Hintergrund der zitierten gesetzlichen Vorschrift hält der LfD die Auslagerung der Datenverarbeitung (Outsourcing) für zulässig, wenn folgendes gewährleistet ist:

- Dem auftraggebenden Krankenhaus wird im Rechner des Auftragnehmers eine eigene virtuelle Betriebssystemumgebung zum Betrieb der Anwendungen, zur Speicherung auf Festplatten und zur Datensicherung und Archivierung auf Magnetbändern bereitgestellt. Damit ist der Zugriff auf Daten anderer Krankenhäuser wirksam verwehrt.
- Der Betrieb des virtuellen Betriebssystems und der Anwendungen sowie der Ausdruck von Daten erfolgt über Systeme, die auch weiterhin von den Krankenhäusern selbst vorgehalten werden.
- Die Anwendungen stehen dem Auftragnehmer nur als ausführbare Codes und nicht als Quellprogramme zur Verfügung, so daß eine Interpretation der Daten für den Auftragnehmer nicht möglich ist.
- Die übergeordnete Verwaltung des virtuellen Betriebssystems durch den Auftragnehmer schließt aus, daß dieser ohne ein besonderes Paßwort, das nur dem Krankenhaus zur Verfügung steht, Zugang zu interpretationsfähigen Anwendungsdaten erhält.
- Die Datenübertragung zwischen dem Krankenhaus und dem Auftragnehmer erfolgt verschlüsselt.
- Die Daten auf den Sicherungsbändern und -kassetten werden anwendungsabhängig und paßwortgeschützt komprimiert. Sie dürfen durch ein Fremdsystem nicht interpretierbar sein.

Wird die Auftragsverarbeitung anders organisiert, ist davon auszugehen, daß der Auftragnehmer Zugang zu den Patientendaten hat. Dies wäre nach § 36 Abs. 9 LKG nur dann zulässig, wenn die Einhaltung der Datenschutzbestimmungen des LKG und eine § 203 StGB entsprechende Schweigepflicht beim Auftragnehmer sichergestellt sind. Die letztgenannte Voraussetzung liegt nur bei ärztlich geleiteten Einrichtungen – also etwa anderen Krankenhäusern – oder bei Auftragnehmern vor, die der Strafandrohung des § 203 Abs. 1 und 3 StGB unterliegen. Wesentlich ist, daß auch die im Auftrag verarbeiteten Daten durch das strafprozessuale Zeugnisverweigerungsrecht und Beschlagnahmeverbot geschützt sind.

Ähnlich verhält es sich mit der Fernwartung, und zwar unabhängig davon, ob diese als Auftragsdatenverarbeitung i. S. v. § 36 Abs. 9 LKG oder als sonstige Nutzung von Daten i. S. v. § 36 Abs. 2 LKG angesehen wird.

Keine Bedenken wären zu erheben, wenn sich die Fernwartung auf folgende Funktionen erstreckt:

- Reine Ferndiagnose, bei welcher vorbeugend hardwarebezogene Fehler- und Statusmeldungen des Systems überwacht und ausgewertet werden (Schreib-/Lesefehler, Betriebsdauerangaben, Prüfsummenfehler, Wartungs-Timer, Speicherplatzbelegung usw.). Die Weiterleitung der erforderlichen Daten erfolgt automatisiert (periodisch, in Abhängigkeit von Schwellenwerten); ein Zugriff der Fernwartungsstelle auf das System, insbesondere auf personenbezogene Daten, ist ausgeschlossen.
- Fernbetreuung in dem Sinne, daß über die Auswertung bestimmter Systemzustände hinaus softwarebezogene Eingriffe an Anwendungen oder am Betriebssystem erfolgen, ohne daß der Zugriff auf Patientendaten erforderlich ist (z. B. Einstellung von Programm- und Systemparametern, Ändern von Konfigurationsangaben).

Eine Fernwartung, die über die vorgenannten Funktionen hinaus, den Zugang zu anderen als Patientendaten (z. B. Personaldaten) ermöglicht, ist im Rahmen von § 4 LDSG zulässig.

Nur mit der Zustimmung von Patienten wäre eine Fernwartung zulässig, bei der ein Zugriff auf Patientendaten möglich ist (§ 36 Abs. 2 LKG). Würde die Fernwartung als Auftragsdatenverarbeitung qualifiziert, stünden ihr die gleichen rechtlichen Hindernisse entgegen wie dem Outsourcing der Patientendatenverarbeitung.

Die zwingende Folge der Anwendung der gesetzlichen Vorschrift über die Auftragsdatenverarbeitung im Krankenhausbereich (§ 36 Abs. 9 LKG) ist danach, daß Outsourcing und Fernwartung durch nichtöffentliche Stellen, die nicht der Strafandrohung des § 203 StGB unterliegen, nur in sehr eingeschränktem Umfange zulässig ist. Es kann nicht bestritten wrden, daß die Umsetzung der obigen Vorschläge mit Erschwernissen verbunden ist, und es kann auch nicht ausgeschlossen werden, daß ein höherer Aufwand bei der Datenverarbeitung entsteht. Auch ein Einwilligungsverfahren wird kaum zu praktizieren sein. Dies ändert aber nichts daran, daß es nach der gegenwärtigen Rechtslage unzulässig ist, Patientendaten an nichtöffentliche Stellen, die nicht die gesetzlichen Voraussetzungen erfüllen, zum Zwecke der Auftragsdatenverarbeitung weiterzugeben oder einem beauftragten Unternehmen oder Rechenzentrum zu ermöglichen, kurzfristig auf die Datensärze zuzugreifen, um gegebenenfalls per Ferndiagnose die Weiterverarbeitung zu ermöglichen.

Aus der Prüfungstätigkeit ist bekannt, daß auch Praktiker in der Fernwartung eine besondere Gefährdung des Datenschutzes sehen. Der Leiter des Großrechenzentrums einer gesetzlichen Krankenkasse lehnt im Blick auf die Empfindlichkeit der Datenverarbeitung eine Fernwartung kategorisch ab, obwohl das Sozialgesetzbuch – Zehntes Buch – keine mit dem LKG vergleichbare Einschränkung enthält.

10.4.2 Fehlbelegungsprüfungen in Krankenhäusern

Nach § 17a KHG stellen die Krankenhausträger sicher, daß keine Patienten in das Krankenhaus aufgenommen werden oder dort verbleiben, die nicht oder nicht mehr der stationären Krankenhausbehandlung bedürfen. Die Krankenkassen wirken insbesondere durch gezielte Einschaltung des Medizinischen Dienstes der Krankenversicherung darauf hin, daß Fehlbelegungen vermieden und bestehende Fehlbelegungen zügig abgebaut werden. Zu diesem Zweck darf der Medizinische Dienst Einsicht in die Krankenunterlagen nehmen. Er hat der Krankenkasse das Ergebnis der Begutachtung und die erforderlichen Angaben über den Befund mitzuteilen.

In Durchführung dieser gesetzlichen Bestimmung kündigte der Medizinische Dienst in zehn Krankenhäusern des Landes Fehlbelegungsprüfungen an. Die Begutachtung sollte sich auf Krankenakten von Patienten aus den Abteilungen Innere Medizin und Chirurgie des Jahres 1996 erstrecken.

Von seiten der Krankenhäuser wurde in Frage gestellt, ob die Erhebung von Patientendaten zur systematischen retrospektiven Begutachtung durch § 276 SGB V gedeckt ist. Absatz 4 der Vorschrift regelt nämlich die Befugnisse des Medizinischen Dienstes bei der Erstattung gutachtlicher Stellungnahmen „im Einzelfall".

Der LfD vertrat die Auffassung, daß § 17 a KHG einen Sachverhalt regelt, der unabhängig von den Befugnisnormen des § 276 SGB V zu beurteilen ist. Die „gezielte" Einschaltung des Medizinischen Dienstes nach der Bestimmung des KHG bezieht sich nicht auf einzelne Patienten, sondern auf die Auswahl der Krankenhäuser, die in die Untersuchung einbezogen werden. Es ist weiter zu berücksichtigen, daß die erhobenen Patientendaten zum frühestmöglichen Zeitpunkt anonymisiert und nur in dieser Form weiterverarbeitet werden. Im Ergebnis waren gegen die Vorgehensweise des Medizinischen Dienstes keine datenschutzrechtlichen Bedenken zu erheben.

10.4.3 Datenübermittlung zum Zwecke der Regulierung von Haftpflichtversicherungsschäden

Eine Klinik in der Trägerschaft des Landes erbat die Stellungnahme des LfD zur Zulässigkeit der Übermittlung von Patientendaten an eine private Haftpflichtversicherung. Diese ging davon aus, daß sie als Haftpflichtversicherer des Landes Rheinland-Pfalz ein rechtliches Interesse an der Kenntnisnahme von Informationen über Patientenunfälle habe und demnach die Übermittlungsvoraussetzungen des § 16 LDSG vorlägen.

Der LfD wies in seiner Stellungnahme darauf hin, daß sich die Zulässigkeit der Datenübermittlung nicht nach § 16 LDSG, sondern nach der insoweit abschließenden Regelung in § 36 Abs. 3 LKG bestimmt. Unter keine der in Satz 1 dieser Vorschrift aufgezählten sieben Fallgruppen läßt sich die Übermittlung von Patientendaten an den Haftpflichtversicherer einer Klinik subsumieren. Eine Datenübermittlung ist also ausschließlich auf der Grundlage einer Einwilligung des Patienten zulässig. Dabei sind die Formerfordernisse des § 36 Abs. 2 LKG zu beachten (Schriftform, Nachteilshinweis). Bei fehlender Grundrechtsmündigkeit von Patienten kann die Einwilligung auch durch Betreuer erteilt werden.

10.5 Einbehaltung des Personalausweises von Besuchern in Maßregelvollzugseinrichtungen

Mit dem Ziel, die Sicherheit des Maßregelvollzugs zu erhöhen, ging eine Einrichtung dazu über, von Besuchern für die Dauer ihres Aufenthalts den Personalausweis einzubehalten. Das Ministerium für Arbeit, Soziales und Gesundheit sah die Rechtsgrundlage für derartige Maßnahmen in § 16 Maßregelvollzugsgesetz, der bestimmt, daß Besuche aus Gründen der Behandlung, des geordneten Zusammenlebens in der Einrichtung oder der öffentlichen Sicherheit oder Ordnung überwacht, eingeschränkt, abgebrochen oder untersagt und aus Gründen der Sicherheit von einer Durchsuchung der Besucherin oder des Besuchers abhängig gemacht werden dürfen.

Bei der datenschutzrechtlichen Beurteilung der Kontrollmaßnahmen, um die der LfD vom Bürgerbeauftragten gebeten wurde, war zu berücksichtigen, daß das Maßregelvollzugsgesetz keine speziellen Regelungen für die Erhebung von Besucherdaten enthält. Demnach ist § 12 LDSG anzuwenden; die Datenerhebung ist danach zulässig, wenn sie zur rechtmäßigen Aufgabenerfüllung erforderlich ist. Im Blick auf die besonderen Notwendigkeiten einer sicheren Besucheridentifizierung im Maßregelvollzug sah der LfD die Datenerhebung unter Verwendung des Personalausweises als Legitimationspapier als zulässig und verhältnismäßig an. Gesetzliche Bestimmungen, etwa des Personalausweis- oder Paßgesetzes, stehen der Verfahrensweise nicht entgegen.

Die Aufbewahrung des Personalausweises an der Pforte ist unter datenschutzrechtlichen Gesichtspunkten als eine vorübergehende Datenspeicherung zu qualifizieren. Diese Datenspeicherung ist nach § 13 Abs. 1 LDSG zulässig, wenn sie zur Aufgabenerfüllung erforderlich ist und für Zwecke erfolgt, für die die Daten erhoben worden sind. Der LfD ging auch vom Vorliegen dieser Voraussetzung aus, denn nur dann, wenn die erhobenen Daten – vorübergehend – gespeichert werden, kann festgestellt werden, welche Besucher sich noch in der Anstalt befinden.

Ob die vorübergehende Datenspeicherung in der beschriebenen Weise erfolgt oder ob die Daten in einer Kartei oder Liste aufgezeichnet werden, ist unter Datenschutzgesichtspunkten nicht relevant. Außerhalb einer datenschutzrechtlichen Beurteilung mag es freilich gute Gründe geben, den Personalausweis für die Dauer des Besuchs aufzubewahren und nicht eine andere Form der Datenspeicherung zu wählen. So könnte es beispielsweise wichtig sein, Besucher beim Verlassen der Anstalt wiederum eindeutig zu identifizieren. Dies dürfte nur dann möglich sein, wenn die Paßdaten unter Einbeziehung des Lichtbildes zur Verfügung stehen und für den Besucher ein faktischer Zwang besteht, diese erneute Identifizierungsprozedur hinzunehmen.

10.6 Patientenchipkarten

10.6.1 Bestimmungen über die Einführung und Verwendung von Patientenchipkarten in der Berufsordnung für die Ärzte

Im Rahmen der Novellierung des Heilberufsgesetzes empfahl der LfD, in die Berufsordnung für die Ärzte nähere Bestimmungen über den Datenschutz bei der Einführung und Verwendung von Patientenchipkarten aufzunehmen. Im Gesetzgebungsverfahren wurde dieser Vorschlag aufgegriffen; § 23 des Heilberufsgesetzes in der geänderten Fassung bestimmt, daß die Berufsordnung Regelungen über die Einführung und Verwendung maschinell lesbarer Patientenkarten einschließlich des Datenschutzes enthalten kann. Unter Bezugnahme auf die Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu den datenschutzrechtlichen Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen (Anlage 5) konkretisierte der LfD in einem Schreiben an die Landesärztekammer Rheinland-Pfalz seine Erwartungen an die Novellierung der Berufsordnung. Er wies darauf hin, daß die massenhafte Einführung der Karten einen sozialen Druck auf die Betroffenen erzeuge, sie mitzuführen und vorzuzeigen. Diesen Erwartungen könnten sich die Betroffenen vielfach nur unter Befremden des Arztes oder sogar der Gefahr, daß dieser die Behandlung ablehne, verweigern. Die Berufsordnung sollte diesen Gedanken aufgreifen und ein Benachteiligungsverbot statuieren. Ein weiteres Anliegen ist, daß sich das therapeutische Verhältnis zwischen Arzt und Patient durch den Einsatz von Chipkarten nicht verschlechtern dürfe. Das sich im Gespräch entwickelnde Vertrauensverhältnis zwischen Arzt und Patient dürfe nicht durch eine chipkartenvermittelte Kommunikation verdrängt werden, und verkürzte Darstellungen medizinischer Sachverhalte auf der Chipkarte dürften nicht zu einer Minderung der Qualität des therapeutischen Verhältnisses führen. Einer solchen Entwicklung sollte nach Meinung des LfD durch einen Hinweis auf die Pflichten des Arztes entgegengewirkt werden. Ferner sollte eine Pflicht des Arztes statuiert werden, dem Patienten Auskunft über die auf der Chipkarte gespeicherten Daten zu erteilen; ferner könnte der Arzt verpflichtet werden, von einer Chipkarte nur die Daten in seine Patientenkartei (Praxiscomputer) zu übernehmen, die für seine Behandlungszwecke erforderlich sind.

Zur Zeit ist noch nicht bekannt, ob und ggf. in welchem Umfange die Empfehlungen des LfD aufgegriffen werden.

10.6.2 Modellversuch Neuwied/Rhein

Im 15. Tb. berichtete der LfD unter Tz. 10.8 über den Modellversuch, der in der Projektverantwortung der Kassenärztlichen Vereinigung Koblenz, des Zentralinstituts für die kassenärztliche Versorgung und der Bundesvereinigung Deutscher Apothekerverbände in Neuwied/Rhein durchgeführt wird. Die datenverarbeitungstechnischen Grundlagen wurden geschaffen, und den vom LfD für den Modellversuch definierten technisch-organisatorischen Datenschutzanforderungen ist entsprochen. Dennoch ist es trotz größter Anstrengungen bisher nicht gelungen, die ins Auge gefaßten Teilnehmerzahlen sowohl im Bereich der Ärzte und Apotheken wie auch der Patienten und Kunden zu erreichen. Dadurch sind nicht nur wichtige Projektziele – Verbesserung der ärztlichen und medikamentösen Versorgung – in Frage gestellt; aufgrund der mangelnden Akzeptanz ist auch zu befürchten, daß die wissenschaftliche Begleitung wenig ertragreich ist. Dies ist – auch aus der Sicht des Datenschutzes – zu bedauern, denn auch datenschutzrechtliche Fragestellungen bilden Schwerpunkte dieser wissenschaftlichen Begleitung.

Es gibt keinerlei Anhaltspunkte dafür, daß die mangelnde Akzeptanz auf Befürchtungen der Bevölkerung beruht, der Datenschutz könnte nicht hinreichend gewährleistet sein. Den LfD erreichten im Berichtszeitraum keine Eingaben zu diesem Themenbereich. Im übrigen hat der LfD stets deutlich gemacht, daß er datenschutzrechtliche Belange in dem regional und zeitlich begrenzten Modellversuch hinreichend berücksichtigt sieht. Dementsprechend hat er sich Versuchen von dritter Seite widersetzt, die Patientenchipkarte in der Erprobungsphase mit zusätzlichen Funktionen – z. B. als Kundenkarte im Apothekenbereich – zu versehen. Auch eine direkte Übernahme des Speicherinhalts der Patientenchipkarte in den im Praxiscomputer vorhandenen Patientendatensatz kommt in der Versuchsphase nicht in Betracht, denn den Teilnehmern am Modellversuch wird in den mit der Einwilligungserklärung verbundenen Hinweisen versichert, daß die „persönlichen Daten, außer auf der Karte, nirgendwo elektronisch gespeichert" werden. Mit den Projektverantwortlichen besteht in der Beurteilung der datenschutzrechtlichen Erfordernisse weitgehende Übereinstimmung. Mitarbeiter des LfD nehmen beratend an den Sitzungen des Projektausschusses teil. Der LfD ist dadurch zeitnah über die Entwicklung des Modellversuchs informiert und kann erforderlichenfalls die aus seiner Sicht gebotenen Datenschutzanforderungen konkretisieren. Die Aufsichtsbehörden für den nichtöffentlichen Bereich wurden im Berichtszeitraum wiederholt über die Entwicklung und den Stand des Modellversuchs unterrichtet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Sitzung am 9./10. November 1995 erneut eine Entschließung zum Einsatz von Chipkarten im Gesundheitswesen verabschiedet (Anlage 5).

10.7 Arzt- und Zahnarztadressen in Informationsbroschüren von Gemeinden

Es ist nicht die Aufgabe des Datenschutzes, sich den Bemühungen von Gemeinden, Einwohnern und Ortsfremden sich umfassend über Dienstleistungsangebote zu informieren, entgegenzustellen. Er hat freilich darauf zu achten, daß Datenübermittlungen an die Gemeinden für diesen Zweck sowie die Veröffentlichungen den datenschutzrechtlichen Anforderungen entsprechen. Eine Veröffentlichung personenbezogener Daten in Informationsbroschüren ist datenschutzrechtlich als „Datenübermittlung an nichtöffentliche Stellen" zu qualifizieren und nur beim Vorliegen der Voraussetzungen des § 16 LDSG zulässig.

Eine Kassenzahnärztliche Vereinigung (KZV) wollte wissen, ob sie befugt sei, eine Liste mit allen Zahnarztpraxen im Bereich einer Verbandsgemeinde zum Zwecke der Veröffentlichung in einer Informationsbroschüre zur Verfügung zu stellen. Der LfD wies darauf hin, daß den einschlägigen für die KZV geltenden Vorschriften (§ 95 Abs. 2 SGB V i. V. m. § 9 Zahnärzte-ZV) eine Übermittlungsbefugnis nicht zu entnehmen ist. Auch nach den allgemeinen Übermittlungsbestimmungen des SGB X, hier insbesondere § 69 Abs. 1 Nr. 1, ist eine Adressenweitergabe durch die KZV unzulässig. Die enge Bindung der KZV als Sozialleistungsträger an die gesetzlichen Bestimmungen zum Schutze des Sozialgeheimnisses stehen also einer Übermittlung entgegen.

Weniger restriktive Übermittlungsbestimmungen fänden indessen Anwendung, wenn die Daten durch die öffentliche Berufsvertretung (Zahnärztekammer oder Ärztekammer) übermittelt würden. Diese Stelle hätte zwar zu berücksichtigen, daß die Daten zur Veröffentlichung durch die Gemeinde bestimmt sind. Es wäre nicht zulässig, wenn personenbezogene Daten trotz der Kenntnis, daß eine Veröffentlichung, also die Datenübermittlung an nichtöffentliche Stellen, mit geltendem Datenschutzrecht nicht zu vereinbaren ist, zu diesem Zweck an eine öffentliche Stelle übermittelt würden. Liegen aber diese Übermittlungsvoraussetzungen (§ 16 LDSG) vor, so bestehen gegen die Datenweitergabe keine Bedenken. Voraussetzung ist also, daß die Datenübermittlung im öffentlichen Interesse liegt und die Betroffenen nach Unterrichtung über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck der Datenübermittlung nicht widersprochen haben.

Wenn die Daten unmittelbar aus allgemein zugänglichen Quellen (etwa einer Vorauflage der Informationsbroschüre, dem Fernsprechbuch oder einem Branchenadreßbuch) entnommen werden könnten, wäre die Datenübermittlung durch Veröffentlichung auch ohne Unterrichtung über ein Widerspruchsrecht zulässig (§ 16 Abs. 1 Nr. 2 i. V. m. § 12 Abs. 4 Nr. 9 LDSG).

11. Sozialdatenschutz

Verschärfte Kontrollen im Sozialbereich

Gesetzgebung und Verwaltung sehen in der Bekämpfung des Sozialleistungsmißbrauchs einen besonderen Handlungsschwerpunkt. So wurde beispielsweise durch eine Ergänzung des BSHG (§ 117) zugelassen, daß die Daten von Sozialleistungsempfängern mit den bei anderen Sozialleistungsträgern und sonstigen Stellen gespeicherten Daten im automatisierten Verfahren mit dem Ziel abgeglichen werden, Anhaltspunkte für Leistungsmißbrauch zu gewinnen.

Im Gesetzesvollzug sind die Behörden zunehmend bemüht, dem Leistungsmißbrauch durch stärkere Kontrolle der Leistungsempfänger entgegenzuwirken. Da Kontrollmaßnahmen in aller Regel mit Datenverarbeitungsvorgängen verbunden sind, äußert sich die stärkere Kontrolldichte auch durch eine Zunahme der Zahl von Eingaben an den LfD.

Betroffen ist aber nicht nur der Sozialhilfebereich. Handlungsbedarf wird beispielsweise auch bei der Bekämpfung der illegalen Ausländerbeschäftigung oder der Schwarzarbeit und Scheinselbständigkeit gesehen. Gesetzgeberische Maßnahmen zur Erhöhung der Transparenz des Abrechnungsverfahrens in der gesetzlichen Krankenversicherung, Pflegeversicherung, Renten- und Unfallversicherung zielen auch auf die Erkennung und Verhinderung von Leistungsmißbrauch.

Alle diese Maßnahmen werden indessen noch nicht als ausreichend angesehen. Die 72. ASMK setzte im September 1995 eine länderübergreifende Arbeitsgruppe ein, die prüfen sollte, ob und in welchem Umfang im Bereich der Sozialleistungen weitere Verbesserungen des Datenaustausches gefordert werden sollen. Nach mehreren Sitzungen legte die Arbeitsgruppe am 26. Mai 1997 Vorschläge zum verbesserten Datenaustausch bei Sozialleistungen vor.

Die Vorschläge der Arbeitsgruppe beziehen sich auf Einzelmaßnahmen, die keine gesetzgeberischen Maßnahmen voraussetzen, so beispielsweise bei BSHG-Leistungen auf die Nachfrage beim Wohnsitzfinanzamt des Hilfesuchenden zu Schenkungen und Erbschaften und auf die Nachfrage bei Steuerstellen potentieller Schenker. Im Vordergrund steht aber die Schaffung zusätzlicher rechtlicher Möglichkeiten des Datenaustauschs. Hier geht es beispielsweise im BSHG-Bereich um einen automatisierten Datenabgleich mit der Wohngeldstelle, um die Mitteilung über Zweitsozialversicherungsausweise, den Zugriff auf die Außenprüfungsdaten der Bundesarbeits- und Bundeszollverwaltung, um Auskunftspflichten der Banken und Lebensversicherungen, um Auskunftspflichten der Grundbuchämter, Auskunftsrechte gegenüber dem zentralen Fahrzeugregister oder die Zusammenarbeit mit den Ordnungswidrigkeitenbehörden.

Gleichermaßen werden auch für die anderen oben genannten Sozialleistungsbereiche Empfehlungen in bezug auf gesetzgeberische Maßnahmen, die auf eine stärkere Kontrolle zielen, ausgesprochen.

Der Arbeitskreis „Sozialwesen" der Datenschutzbeauftragten des Bundes und der Länder hat sich in einer Sitzung am 15. September 1997 in Mainz mit den o. a. Arbeitsergebnissen befaßt. Im Vordergrund der Beratungen stand das Problem der „anlaßunabhängigen Mißbrauchskontrolle". Anlaßunabhängige Datenverarbeitungsvorgänge würden eine neue Eingriffskategorie darstellen, die die bisherigen am Erforderlichkeitsgrundsatz orientierten abgestuften Formen der Datenverarbeitung ergänzt. Sie sind deshalb problematisch, weil die Datenübermittlung an oder die Datenerhebung bei Dritten ohne Kenntnis der Betroffenen einen schwerwiegenden Eingriff in die Informationsrechte darstellt, der nur in konkreten und begründeten Ausnahmefälle zulässig sein kann. Die DSB erheben im Blick auf das verfassungsrechtliche Verhältnismäßigkeitsprinzip Bedenken gegen eine pauschale und undifferenzierte Datenverarbeitung ohne Anlaß. Sie wenden sich nicht gegen einzelne Veränderungen, warnen aber davor, die bestehende Systematik der abgestuften Eingriffsbefugnisse zu verändern oder gar aufzuheben.

11.1 Informationsrechte des Parlaments versus Sozialgeheimnis

Die Neuordnung des Parlamentsdatenschutzes vor dem Hintergrund eines „Parlamentsvorbehalts", wie er im Datenschutzgesetz von Rheinland-Pfalz enthalten ist, ließ auch die Diskussion um die Informationsrechte des Parlaments in Petitionsverfahren wieder aufleben. Im Mittelpunkt stehen dabei die Bereiche, in denen auf Bundesrecht beruhende besondere Geheimhaltungspflichten, wie z. B. das Sozialgeheimnis, zu beachten sind.

Zwischen dem zuständigen Fachministerium und dem LfD besteht in der Beurteilung der Grundsatzfragen kein Dissens: Die Leistungsträger und die sonstigen in § 35 SGB I genannten Stellen haben das Sozialgeheimnis auch im Zusammenhang mit der Behandlung von Petitionen zu beachten, und die mit der Petition erteilte ausdrückliche oder konkludente Einwilligung deckt die zur Bearbeitung einer Petition erforderliche Übermittlung von Sozialdaten des Petenten an den Petitionsausschuß.

Auch der Landtag selbst hat freilich zu prüfen, ob bei der Weitergabe der Petition an die Landesregierung in jedem Fall der Name des Einsenders übermittelt werden muß. In Zweifelsfällen sollte der Petent gefragt werden, ob er mit personenbezogenen Recherchen bei der Bearbeitung seiner Petition einverstanden ist.

Wesentlich schwieriger ist die Frage zu beantworten, ob im Rahmen der Behandlung einer Petition Daten über Dritte an den Landtag – Petitionsausschuß – übermittelt werden dürfen. Solche Fälle lassen sich sich nicht immer durch die Weitergabe anonymisierter Vorgänge an den Petitionsausschuß lösen.

Der Anspruch des Petitionsausschusses auf Auskunft und Zugängigmachen der Akten ist in Art. 90 a Abs. 2 der Verfassung für Rheinland-Pfalz wie folgt geregelt: „Die Landesregierung und alle Behörden des Landes sowie die Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, soweit sie der Aufsicht des Landes unterstehen, sind verpflichtet, dem Petitionsausschuß jederzeit die notwendigen Auskünfte zu erteilen und die erforderlichen Akten zugängig zu machen."

Neben diesem geschriebenen Verfassungsrecht besteht – ebenfalls mit Verfassungsrang – das allgemeine Informationsrecht des Parlaments und seiner Mitglieder. Es konkretisiert sich insbesondere in den geschäftsordnungsrechtlich geregelten parlamentarischen Fragerechten – Mündliche Anfragen, Große und Kleine Anfragen –.

Der Bund als Sozialrechtsgesetzgeber ist grundsätzlich nicht befugt, diese landesverfassungsrechtlichen Auskunftsansprüche des Parlaments gegenüber der Exekutive einzuschränken. Einfachgesetzliche Geheimhaltungsbestimmungen – wie das Sozialgeheimnis – setzen sich, auch wenn sie keine Ausnahmebestimmungen zugunsten der parlamentarischen Aktenvorlage- und Informationsrechte enthalten, nicht ohne weiteres gegenüber den parlamentarischen Aktenvorlage- und Informationsrechten durch. Wenn das Verfassungsrecht eines Landes dem Homogenitätsprinzip des Art. 28 Abs. 1 Satz 1 und 2 GG entspricht, dann bleibt es von Art. 31 GG unberührt (BVerfGE 36, 342).

Hieraus folgt, daß bundesgesetzliche Geheimhaltungsbestimmungen dem landesverfassungsrechtlichen Aktenvorlage- und Informationsanspruch nicht entgegenstehen. Ein Ausgleich zwischen dem Recht des Parlaments und dem Persönlichkeitsrecht des Betroffenen ist nach dem Prinzip der praktischen Konkordanz herbeizuführen. Die verfassungsrechtlich geschützten Rechtsgüter müssen „in der Problemlösung einander so zugeordnet werden, daß jedes von ihnen Wirklichkeit gewinnt" (Hesse, Grundzüge des Verfassungsrechts, 20. Aufl., 1995, 28).

Der zulässige Umfang des parlamentarischen Informationsrechts begrenzt zugleich auch das Informationsrecht des Petitionsausschusses, soweit Dritte betroffen sind, m. a. W., der Petitionsausschuß hat keine weitergehenden Informationsrechte als der Landtag und seine Mitglieder bei der Ausübung der parlamentarischen Fragerechte. Die Exekutive kann die öffentliche Beantwortung von parlamentarischen Anfragen und die Erteilung von Auskünften ablehnen, wenn dem Bekanntwerden schutzwürdige Interessen einzelner entgegenstehen. Sie bleibt jedoch grundsätzlich zur Antwort im erforderlichen Umfang verpflichtet, wenn das Parlament die notwendigen Vorkehrungen für den Geheimnisschutz getroffen hat. Dabei ist zu berücksichtigen, daß die Behandlung der Petitionen in nichtöffentlichen Sitzungen des Petitionsausschusses erfolgt und daß wirksame rechtliche (Datenschutzordnung des Landtags), organisatorische und verfahrensmäßige Vorkehrungen zum Schutze des Rechts auf informationelle Selbstbestimmung bei der Behandlung von Petitionen getroffen sind.

Der BfD hat sich in seinem 14. Tb. (Bundestagsdrucksache 12/4805, S. 33) zum Inhalt des parlamentarischen Kontrollrechts wie folgt geäußert: „Angesichts der herausragenden Bedeutung der parlamentarischen Regierungskontrolle kann die Rolle des Datenschutzes jedoch keinesfalls darin bestehen, die Verweigerung einer Antwort auf unbequeme Fragen zu begründen. Umgekehrt läßt sich freilich auch nicht sagen, daß Belange des Persönlichkeitsschutzes allein deswegen unbeachtlich sind, weil eine Frage von einem oder mehreren Abgeordneten in einer geschäftsordnungsmäßig vorgesehenen Form gestellt wird. Dabei ist zu prüfen, ob eine personenbezogene Antwort ohne wesentlichen Informationsverlust vermieden werden kann. Andererseits muß gefragt werden, welche Beeinträchtigungen der informationellen Selbstbestimmung oder anderer Grundrechte der Betroffenen mit einer solchen Antwort verbunden sind, insbesondere welcher Grad der persönlich-privaten Betroffenheit zu erwarten ist." Unter Berücksichtigung dieser Überlegungen können in den sicherlich nicht allzu häufigen Fällen, in denen der Petitionsausschuß personenbezogene Informationen über Dritte anfordert, angemessene Ergebnisse erzielt werden. Gleichwohl sollte angestrebt werden, die Übermittlungsbestimmungen im Interesse der Rechtsklarheit an die Verfassungsrechtslage anzupassen.

(Anmerkung: Der vorstehende Beitrag wurde bereits in „Datenschutz und Datensicherheit", 96, 646, abgedruckt.)

11.2 Krankenkassen, Kassenärztliche Vereinigungen

11.2.1 Übermittlung von ärztlichen Leistungsdaten

Zahnärzte

Die Spitzenverbände der Krankenkassen und die Kassenzahnärztliche Bundesvereinigung vereinbaren nach § 295 Abs. 3 SGB V das Nähere zur Übermittlung von Leistungsdaten zwischen den Zahnärzten, den Kassenzahnärztlichen Vereinigungen (KZV) und den Krankenkassen. Da sich die Vertragspartner nicht einigen konnten, setzte das Bundesschiedsamt für die vertragszahnärztliche Versorgung eine Vereinbarung in Kraft, die unter Datenschutzgesichtspunkten angreifbar war.

Nach § 295 Abs. 2 SGB V darf die KZV den Krankenkassen die erforderlichen Angaben über die abgerechneten Leistungen zwar fallbezogen, nicht jedoch versichertenbezogen übermitteln. Um dies zu gewährleisten, erhalten die Kassen einen Versichertendatensatz und einen Leistungsdatensatz, die nur in den in der Vereinbarung genannten Fällen zusammengeführt werden dürfen. Sofern in beiden Datensätzen identische Daten vorkommen, besteht die Möglichkeit einer Zusammenführung auch in sonstigen Fällen.

Im Zusammenwirken der Landesbeauftragten für den Datenschutz und des BfD konnte erreicht werden, daß im Versichertendatensatz die Angaben „Zahnarztnummer/Zahnarztname" und der „Fallwert in Punkten und DM" entfallen. Umstritten ist noch die Erforderlichkeit anderer Daten (z. B. Zahnbezug, Tag der Behandlung). Die Kassen wollen sich hierzu erst dann abschließend äußern, wenn das DV-Projekt für das Abrechnungsverfahren genügend entwickelt ist. Als Alternative steht zur Diskussion, ob eine teilweise Löschung des Versichertendatensatzes vor der Übermittlung des Leistungsdatensatzes erfolgen kann.

Der Verband der Angestellten-Krankenkassen e. V. (VdAK), der als einziger Spitzenverband dieser Vereinbarung über einen reduzierten Datensatz nicht zustimmte, wurde durch Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (vgl. Anlage 14) aufgefordert, sich der Vereinbarung anzuschließen. Dies ist inzwischen geschehen.

Ärzte

Im ärztlichen Bereich trafen die Spitzenverbände der Krankenkassen und die Kassenärztliche Bundesvereinigung sowohl für die Übermittlung von Daten für Abrechnungszwecke als auch für Wirtschaftlichkeitsprüfungen Vereinbarungen. Die technischen Voraussetzungen für eine in vollem Umfange automatisierte Datenweitergabe liegen indessen noch nicht vor. Aus den Listenausdrucken, die den Krankenkassen von den Kassenärztlichen Vereinigungen nach wie vor zugeleitet werden, ist aber ersichtlich, welche Leistungen für die einzelnen Versicherten aufgrund welcher Diagnose erbracht wurden. Dies entspricht nicht den Anforderungen des § 295 Abs. 2 SGB V. Es ist das Anliegen aller Datenschutzbeauftragten, daß die vertraglichen Vorgaben rasch umgesetzt und, falls sich Probleme wie bei den Kassenzahnärzten ergeben, eine vergleichbare Vertragsänderung erfolgt.

11.2.2 Kündigung aufgrund einer unzulässigen Datenübermittlung

Nummer 25 der Richtlinien des Bundesausschusses der Ärzte und Krankenkassen über die Beurteilung der Arbeisunfähigkeit und der Maßnahmen zur stufenweisen Wiedereingliederung bestimmt: „Kann der Versicherte nach dem Urteil des behandelnden Arztes die ausgeübte Tätigkeit nicht mehr ohne nachteilige Folgen für seine Gesundheit oder den Gesundungsprozeß verrichten, kann die Krankenkasse mit Zustimmung des Versicherten beim Arbeitgeber die Prüfung anregen, ob eine für den Gesundheitszustand des Versicherten unbedenkliche Tätigkeit bei demselben Arbeitgeber möglich ist."

Eine gesetzliche Krankenkasse informierte den Arbeitgeber, daß der Versicherte aufgrund ärztlichen Urteils seine Tätigkeit als Kraftfahrer nicht mehr ausüben kann. Dies hatte zur Folge, daß das Arbeitsverhältnis gekündigt wurde.

Örtliche Feststellungen in der Geschäftsstelle der Krankenkasse ergaben, daß der Sachverhalt von dem Petenten richtig dargestellt worden war. Die Datenübermittlung erfolgte im Rahmen von Maßnahmen zur stufenweisen Wiedereingliederung. Eine gesetzliche Übermittlungsgrundlage existierte nicht; eine den formalen Anforderungen des SGB X entsprechende Einwilligungserklärung wurde nicht eingeholt. Auch eine vom Betroffenen in sonstiger Weise eingeholte Zustimmung war in den Akten nicht dokumentiert.

Der LfD beanstandete die Datenübermittlung der Krankenkasse an den Arbeitgeber als Verstoß gegen die gesetzlichen Bestimmungen zum Schutze des Sozialgeheimnisses.

11.2.3 Beschlagnahme und Auswertung maschinenlesbarer Datenträger bei Kassenärztlichen Vereinigungen

Das Ministerium des Innern und für Sport erbat eine Stellungnahme des LfD zu der Frage, ob und ggf. unter welchen Voraussetzungen Polizeibehörden befugt sind, bei den Kassenärztlichen Vereinigungen erhobene Abrechnungsdaten von Ärzten zu nutzen.

Der LfD vertrat folgende Rechtsauffassung:

Als Vorfrage zur datenschutzrechtlichen Beurteilung der Nutzung von Abrechnungsdaten ist zu klären, ob die Daten befugt übermittelt worden sind.

Die Kassenärztlichen Vereinigungen sind als Sozialleistungsträger Normadressaten des Sozialgesetzbuchs. Sie sind damit verpflichtet, das Sozialgeheimnis, das Sozialdaten vor unbefugter Erhebung, Verarbeitung und Nutzung schützt (§ 35 SGB I), zu beachten. Bei den Abrechnungsdaten handelt es sich um Sozialdaten, denn sie wurden von einem Sozialleistungsträger im Hinblick auf seine Aufgaben nach dem Sozialgesetzbuch erhoben (§ 67 SGB X). Nach § 35 Abs. 2 SGB I ist eine Erhebung, Verarbeitung und Nutzung von Sozialdaten nur unter den Voraussetzungen des Zweiten Kapitels des Zehnten Buches zulässig. Absatz 3 bestimmt, daß, soweit eine Übermittlung nicht zulässig ist, keine Auskunftspflicht, keine Zeugnispflicht und keine Pflicht zur Vorlegung oder Auslieferung von Schriftstücken, Akten und Dateien besteht. Die Vorschrift stellt damit klar, daß auch die Prozeßordnungen das Sozialgeheimnis nicht durchbrechen; sie statuiert eine Ausnahme von der zentralen Bestimmung des § 94 Abs. 1 und 2 StPO, daß generell alle Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können und vom Gewahrsamsinhaber nicht freiwillig herausgegeben werden, der Beschlagnahme unterliegen (BGH, Beschluß vom 18. März 1992 – 1 BGs 90/92 – 2 BJs 186/91-5; LG Goslar, Beschluß vom 13. Juni 1986, RDV 87, 202).

Eine einschlägige Übermittlungsregelung im Zweiten Kapitel des Zehnten Buchs für die Durchführung eines Strafverfahrens ist § 73. Absatz 1 dieser Vorschrift enthält keine Einschränkung der zur Übermittlung zugelassenen Daten, soweit dies wegen eines Verbrechens oder wegen einer sonstigen Straftat von erheblicher Bedeutung erforderlich ist. Eine Übermittlung von Sozialdaten zur Durchführung eines Strafverfahrens wegen einer anderen Straftat ist zulässig, soweit die Übermittlung auf die in § 72 Abs. 1 Satz 2 genannten Angaben und die Angaben über erbrachte oder demnächst zu erbringende Geldleistungen beschränkt ist. Von Bedeutung ist also, ob es sich bei Abrechnungsmanipulationen um eine Straftat i. S. v. § 73 Abs. 1 handelt und ob die Übermittlung von einem Richter angeordnet worden ist (Absatz 3). Auf Absatz 2 kann die Übermittlung nicht gestützt werden, weil der Datenkatalog des § 72 Abs. 1 Satz 2 bei weitem nicht alle Abrechnungsdaten umfaßt.

Es bestünden keine Bedenken, besonders schwerwiegende Fälle von Abrechnungsbetrug als Straftat von erheblicher Bedeutung zu qualifizieren. Die KV kann jedoch nur dann vom Vorliegen einer Übermittlungs„befugnis" i. S. v. § 73 ausgehen, wenn die richterliche Anordnung erkennen läßt, daß sie unter Beachtung der Übermittlungsvoraussetzungen dieser Vorschrift erlassen wurde. Der Leistungsträger muß sich die richterliche Anordnung in jedem Fall vorlegen lassen, und er hat eine entsprechende Prüfungspflicht (Walz in GK-SGB X 2, § 73 Rdnr. 37).

Als weitere Übermittlungsgrundlage kommt § 69 Abs. 1 Nr. 1 2. Alt. SGB X in Betracht. Danach darf der Sozialleistungsträger Sozialdaten übermitteln, soweit dies für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach dem Sozialgesetzbuch erforderlich ist. Diese Vorschrift greift, wenn mit der Unterrichtung der Staatsanwaltschaft gleichzeitig eine gesetzliche Aufgabe des Leistungsträgers erfüllt wird. Sie legitimiert eine Datenübermittlung an Strafverfolgungsbehörden im Zusammenhang mit der Verfolgung von Straftaten, die einem Leistungsträger gegenüber begangen worden sind (Hauck/Haines, SGB X 1,2, K § 69 Rdnr. 23). Ob und ggf. in welchem Umfange Sozialdaten übermittelt werden, hat der Sozialleistungsträger nach pflichtgemäßem Ermessen unter Beachtung des Erforderlichkeitsgrundsatzes zu entscheiden. Die Vorschrift deckt sowohl die Datenübermittlung im Zusammenhang mit der Erstattung einer Anzeige durch einen Sozialleistungsträger als auch die Datenübermittlung auf Ersuchen der Staatsanwaltschaft oder von Polizeidienststellen im Ermittlungsverfahren. § 69 Abs. 1 Nr. 2 kann als Rechtsgrundlage von Datenübermittlungen zur Durchführung gerichtlicher Verfahren (einschließlich Strafverfahren) herangezogen werden; das außergerichtliche Strafverfahren, d. h. das Ermittlungsverfahren der Staatsanwaltschaft oder ihrer Hilfsorgane, wird von dieser Vorschrift nicht erfaßt (Hauck/Haines, a. a. O., Rdnr. 34).

Sowohl § 69 wie auch § 73 SGB X unterliegen den Einschränkungen des § 76 Abs. 1 für besonders schutzwürdige Daten; soweit es sich um Sozialdaten handelt, die von einem Arzt oder einer anderen in § 203 Abs. 1 und 3 StGB genannten Person zugänglich gemacht worden sind, dürfen sie nur unter den Voraussetzungen übermittelt werden, unter denen diese Person selbst übermittlungsbefugt wäre. Der LfD stimmt insoweit der in der Literatur vertretenen – allerdings nicht unbestrittenen – Auffassung zu, daß eine Mitteilungsbefugnis aus § 2 Abs. 4 der Ärztlichen Berufsordnung hergeleitet werden kann, und zwar wegen des Überwiegens des Interesses der Versichertengemeinschaft an einem Schutz vor ungerechtfertigter Inanspruchnahme der Krankenkassen gegenüber dem Geheimhaltungsinteresse des Versicherten (Walz, a. a. O., Rdnr. 42, m. w. N.).

Die Zulässigkeit der Nutzung übermittelter Sozialdaten ist nach § 78 SGB X zu beurteilen. Sozialdaten dürfen von den Empfängern nur zu dem Zweck verarbeitet oder genutzt werden, zu dem sie ihnen befugt übermittelt worden sind. Für unbefugt übermittelte Daten besteht danach ein Verwertungsverbot. Sofern bei den Strafverfolgungsbehörden Datenträger zur Auswertung vorliegen, die unter Berücksichtigung der gesetzlichen Bestimmungen zum Schutze des Sozialgeheimnisses unbefugt weitergegeben worden sind, kann dieser Mangel geheilt werden, indem entweder eine richterliche Anordnung nach § 73 SGB X oder eine Entscheidung der KV auf der Grundlage von § 69 Abs. 1 Nr. 1 SGB X herbeigeführt wird.

11.3 Gegenseitige Beauftragung der Träger der gesetzlichen Rentenversicherung mit der Versichertenbetreuung

Zum Zwecke einer Verbesserung der Versichertenbetreuung vereinbarte die LVA Rheinland-Pfalz mit anderen Rentenversicherungsträgern gegenseitige Hilfeleistungen bei der Erstellung, Anforderung, Aushändigung und Erläuterung von Versicherungsverläufen, Rentenauskünften, Lückenauskünften und Auskünften über Beitragserstattungen. Den Versicherten soll ermöglicht werden, diese Informationen nicht nur bei dem nach den einschlägigen Organisationsvorschriften für ihn zuständigen Rentenversicherungsträger, sondern auch bei allen anderen an der Vereinbarung beteiligten Rentenversicherungsträgern erhalten zu können. Die LVA geht davon aus, daß diese Zusammenarbeit als eine Form der Verarbeitung oder Nutzung von Sozialdaten im Auftrag (§ 80 SGB X) anzusehen sei. Sie begründet dies damit, daß nach den organisations- und kompetenzrechtlichen Vorschriften des SGB VI und der Zweiten Datenerfassungs-Verordnung (2. DEVO) sowohl für die Verarbeitung, als auch für die Nutzung der im Versicherungskonto gespeicherten Sozialdaten allein der kontoführende Rententersicherungsträger zuständig sei. Die Leistungen ließen erkennen, daß sie im Auftrag und Namen des kontoführenden Rentenversicherungsträgers erbracht würden und daß dieser für ihre Richtigkeit verantwortlich bleibe.

Datenverarbeitung im Auftrag liegt vor, wenn sich der Auftrag ausschließlich auf die Verarbeitung (und Nutzung) personenbezogener Daten bezieht und nicht auch noch andere Tätigkeiten zum Gegenstand hat, für die die Datenverarbeitung nur Grundlage oder Folge ist (Borchert/Hase/Walz, GK SGB X 2 § 80 Rz. 8).

Vom Auftragnehmer dürfen nur Hilfs- bzw. Unterstützungsfunktionen ausgeführt werden. Werden die den Verarbeitungsvorgängen zugrundeliegenden Aufgaben ganz oder teilweise mit abgegeben, handelt es sich nicht mehr um bloße Auftragsdatenverarbeitung, sondern um eine Funktionsübertragung (Simitis/Dammann/Geiger/Mallmann/Walz, Komm. z. BDSG, § 11, Rz. 18).

Der LfD folgt nicht der von den Rentenversicherungsträgern vertretenen Auffassung, daß die Zusammenarbeit als Datenverarbeitung im Auftrag qualifiziert werden kann. Er geht davon aus, daß die gegenseitige Hilfeleistung auch Beratungsleistungen umfaßt, die über Erläuterungen bzw. die Beantwortung von Fragen des Versicherten zu ausgedruckten Dokumenten hinausgeht und individuelle fachliche Ratschläge zur Gestaltung des Versicherungsverlaufs einschließen. Die in Anspruch genommenen Versicherungsträger haben die rechtliche Stellung von Dritten, an die Versichertendaten zur Aufgabenerfüllung übermittelt werden. Da die Datenübermittlung im automatisierten Verfahren erfolgt, ist § 79 SGB X einschlägig. Die gesetzlichen Voraussetzungen für die Einrichtung eines automatisierten Abrufverfahrens liegen nach Auffassung des LfD vor.

Das Interesse des LfD an dem Verfahren bezieht sich freilich nicht nur auf dessen rechtliche Einordnung in die besonderen Datenverarbeitungsarten des Dritten Abschnittes SGB X, sondern auf die Schaffung angemessener technischer und organisatorischer Sicherungsmaßnahmen i. S. v. § 78 a SGB X. Diese Vorschrift ist sowohl in Fällen des § 79 SGB X bei Übermittlungen als auch in Fällen des § 80 SGB X bei Nutzungen im Rahmen der Auftragsdatenverarbeitung zu beachten. In Übereinstimmung mit dem BfD hält er folgende Maßnahmen für geboten:

- Begrenzung der Anzahl der zur Dialognutzung zugelassenen Mitarbeiter auf den erforderlichen Umfang;
- technische Beschränkung der Zugriffsmöglichkeiten der zugelassenen Mitarbeiter;
- Identitätsprüfung des Antragstellers anhand eines Lichtbildausweises;
- Schriftlichkeit des Antrags (formularmäßig);
- sichere Identifizierung und Authentisierung;
- Protokollierung der Online-Zugriffe sowohl beim zuständigen als auch beim anfordernden Rentenversicherungsträger;
- stichprobenmäßige Kontrolle, daß für protokollierte Zugriffe ein Antrag vorliegt.

11.4 Pflegeversicherung

11.4.1 Einwilligungserklärung nach § 18 Abs. 3 SGB XI

Eine Überprüfung der Vordrucke für die Beantragung von Leistungen der Pflegeversicherung im Zuständigkeitsbereich des LfD hatte zum Ergebnis, daß diese ohne Ausnahme in datenschutzrechtlicher Hinsicht verbesserungsbedürftig waren. Ein Schwerpunkt war die sog. Schweigepflichtentbindungsklausel mit folgender Fassung: „Ich bin damit einverstanden, daß der Pflegekasse bzw. dem Medizinischen Dienst der Krankenversicherung vorhandene ärztliche Berichte, Gutachten und Befunddokumentationen zur Einsichtnahme zur Verfügung gestellt werden."

Diese Erklärung entspricht aus folgenden Gründen nicht den gesetzlichen Anforderungen:

- Sie läßt nicht erkennen, welcher Arzt oder welche andere Person oder Stelle befugt sein soll, die in der Erklärung genannten Unterlagen zur Verfügung zu stellen.

- Nach der Erklärung sollen die Unterlagen nicht nur dem Medizinischen Dienst der Krankenkasse (MDK), sondern auch den Pflegekassen zur Verfügung gestellt werden. Letzteres widerspricht § 18 Abs. 3 SGB XI, der lediglich den MDK als Übermittlungsempfänger nennt. Es ist ausschließlich dessen Aufgabe, das Vorliegen und ggf. den Umfang der Pflegebedürftigkeit zu überprüfen. Den Pflegekassen ist nur das Ergebnis der Prüfung mitzuteilen; sie haben keinen Anspruch auf Übermittlung der ärztlichen Unterlagen. Eine unzulässige Datenerhebung kann auch durch die Einwilligung von Betroffenen nicht legitimiert werden.

- Nach § 18 Abs. 3 SGB XI sollen ärztliche Auskünfte eingeholt und Unterlagen nur angefordert werden können, soweit das Wissen um die Vorerkrankungen für die Begutachtung der Pflegebedürftigkeit sowie für die Art, den Umfang und die Dauer der Hilfebedürftigkeit wichtig ist. Demgegenüber erstreckt sich die Einwilligungserklärung auf alle vorhandenen ärztlichen Berichte, Gutachten und Befunddokumentationen und geht damit inhaltlich zu weit.

Weitere Monita bezogen sich auf die Zusammenfassung der Einwilligungserklärung mit der Antragserklärung und die drucktechnische Darstellung der Einwilligungserklärung, die nicht § 67 b Abs. 2 SGB X entsprach.

Die Pflegekassen entsprachen den Empfehlungen des LfD.

11.4.2 Gemeinsame Empfehlung nach § 75 Abs. 5 SGB XI

Ein Träger der freien Wohlfahrtspflege berichtete in einem Schreiben an den LfD über die vorbereitenden Beratungen zum Abschluß von gemeinsamen und einheitlichen Rahmenverträgen unter Beteiligung des MDK und der Vereinigung der Träger der ambulanten oder stationären Pflegeeinrichtungen nach § 75 SGB XI. Die Entwurfsfassung einer Regelung über den Datenschutz enthielt u. a. folgenden Satz: „Die Pflegeeinrichtung unterliegt hinsichtlich der Person des Pflegebedürftigen der Schweigepflicht; ausgenommen hiervon sind Angaben gegenüber der leistungspflichtigen Pflegekasse und dem Medizinischen Dienst der Krankenversicherung, soweit sie zur Erfüllung der gesetzlichen Aufgaben erforderlich sind."

Der LfD wies in seiner Stellungnahme darauf hin, daß Rahmenverträge i. S. v. § 75 SGB XI den Anforderungen an Einschränkungen des Rechts auf informationelle Selbstbestimmung nicht genügen. Diese bedürfen nämlich, wie das Bundesverfassungsgericht im Volkszählungsurteil (BVerfGE 65,1) klargestellt hat, einer gesetzlichen Grundlage. Es ist also rechtlich nicht möglich, daß Kostenträger und Leistungsanbieter Vorgehensweisen vereinbaren, die als Eingriffe in die Persönlichkeitsrechte Betroffener zu qualifizieren sind. Es ist allenfalls zulässig, daß Rahmenverträge auf der Grundlage gesetzlicher Übermittlungsregelungen, wie z. B. des § 104 SGB XI, nähere Bestimmungen über die Aufzeichnung von leistungsrelevanten Daten oder beispielsweise über die technische Durchführung von Datenübermittlungen treffen. Vor diesem Hintergrund wurde die Streichung der Bestimmung empfohlen.

11.5 Sozialhilfe

11.5.1 Zusammenarbeit zwischen Sozialleistungsträgern und der Polizei

Seit vielen Jahren wird die Frage erörtert, ob Sozialämter und andere Sozialleistungsträger der Polizei im Rahmen der Amtshilfe mitteilen dürfen, daß sich eine bestimmte Person in der Dienststelle aufhält. Problematisch ist hierbei, ob sich unter die in § 68 Abs. 1 Satz 1 SGB X genannte Angabe „derzeitige Anschrift des Betroffenen" auch der derzeitige Aufenthalt fassen läßt. Das Berliner Kammergericht hatte dies in einer vielbeachteten Entscheidung 1983 bejaht und das auf einer entgegenstehenden Rechtsauffassung beruhende Handeln eines Abteilungsleiters im Arbeitsamt als rechtswidrig bezeichnet. Das Ministerium für Soziales und Familie äußerte sich zu der Thematik im Jahre 1988 in einer gutachtlichen Stellungnahme, deren Ergebnis vom

Ministerium des Innern und für Sport und der DSK akzeptiert wurde. Die Sozialleistungsträger im Lande wurden mit Rundschreiben vom 26. August 1988 wie folgt informiert: „Das Ministerium des Innern und für Sport und die Datenschutzkommission Rheinland-Pfalz haben sich der in unserem Gutachten vertretenen Rechtsansicht angeschlossen, wonach es unzulässig ist, daß die Polizei ohne richterlichen Beschluß Sozialbehörden die Namen gesuchter Personen überläßt, verbunden mit der Bitte, sie zu informieren, sobald eine dieser Personen dort eintrifft. Das Ministerium des Innern und für Sport hat die ihm nachgeordneten Polizeidienststellen inzwischen entsprechend informiert."

Der DSK und dem LfD wurden keine Fälle bekannt, in denen diese Rechtsauffassung in der Praxis nicht beachtet wurde. Aufgrund einer Mündlichen Frage für die Fragestunde der Sitzung des Deutschen Bundestages am 19. Februar 1997 beurteilte das BMA die rechtliche Zulässigkeit der Datenübermittlung in einem Schreiben vom 18. Februar 1997. Es wies auf die Regelung in § 68 SGB X hin, wonach die Übermittlung der derzeitigen Anschrift des Betroffenen zur Erfüllung von Aufgaben der Polizeibehörden, der Staatsanwaltschaften, Gerichte usw. zulässig ist. Es führte weiter aus: „Das Kammergericht Berlin hat in einem Urteil aus dem Jahre 1983 festgestellt, daß § 68 SGB X der Verpflichtung nicht entgegenstehe, den Aufenthaltsort des Betroffenen bekanntzugeben. Nach dieser Rechtsprechung ist der tatsächliche Aufenthaltsort unter dem Begriff ‚derzeitige Anschrift des Betroffenen' zu subsumieren. Die Bundesregierung hat diese Auffassung geteilt . . ."

Dieses Schreiben wurde am 4. März 1997 wie folgt ergänzt: „Die Bundesregierung teilt nicht die Auffassung, daß es aufgrund der Vorschriften des Sozialgesetzbuches unzulässig sei, wenn ein Sozialamtsbediensteter auf ein polizeiliches Ersuchen ohne richterliche Übermittlungsanordnung eine Terminvereinbarung in der Dienststelle mitteilt bzw. wenn die Sozialbehörde Aufenthaltsanfragen der Polizei speichert oder sonst vermerkt und der Polizei künftige Aufenthalte des Betroffenen in der Sozialbehörde mitteilt."

Das Ministerium des Innern und für Sport unterrichtete die Polizeibehörden des Landes mit Rundschreiben vom 16. Juni 1997 über diese Rechtsauffassung und bat um weitere Veranlassung. Der LfD erhielt auf die Frage nach den Gründen für diese von von der früheren Auffassung abweichenden Meinung die Antwort, daß die Unterrichtung des nachgeordneten Bereichs über die aktuelle Rechtsauffassung des BMA im Hinblick auf entsprechende polizeiliche Maßnahmen erfolgte, denn eine von dieser Rechtsauffassung des zuständigen Ressorts abweichende Verfahrensweise der rheinland-pfälzischen Polizei erscheine nicht vertretbar.

Dieses Schreiben erklärt mit keinem Wort, warum sich das Ministerium trotz unveränderter Rechtslage veranlaßt sieht, die früher vertretene und den zuständigen Behörden bekanntgegebene Rechtsauffassung aufzugeben. Die Meinung, daß eine von der Rechtsauffassung des „zuständigen Ressorts" abweichende Verfahrensweise der rheinland-pfälzischen Polizei nicht vertretbar erscheine, läßt unberücksichtigt, daß zu den Sozialleistungsträgern nicht nur die Arbeitsämter, sondern auch Sozialämter, Jugendämter, gesetzliche Krankenkassen, Berufsgenossenschaften und Rentenversicherungsträger gehören, für die das Ministerium für Arbeit, Soziales und Gesundheit „zuständiges Ressort" ist.

Im Rahmen einer datenschutzrechtlichen Beurteilung ist folgendes zu berücksichtigen: Obwohl das Merkmal „derzeitige Anschrift" des Betroffenen, für das nach § 68 SGB X eine Übermittlungsbefugnis besteht, sprachlogisch kaum mit dem „tatsächlichen Aufenthalt" gleichgesetzt werden kann, wird es vor dem Hintergrund der Entscheidung des Kammergerichts Berlin kein Leiter einer Sozialbehörde verantworten können, die Strafverfolgungsbehörde auf Anfrage nicht über den gegenwärtigen Aufenthalt eines zur Festnahme Ausgeschriebenen in der Dienststelle zu informieren, denn es droht ihm sonst eine Verurteilung nach § 258 a StGB.

Von dieser Fallgruppe, die in dem Schreiben des BMA vom 18. Februar 1997 angesprochen ist, müssen freilich die Fallgruppen unterschieden werden, die Gegenstand der ergänzenden Stellungnahme des BMA vom 4. März 1997 sind. Hier wird nämlich die Auffassung vertreten, daß es zulässig sei, daß ein Sozialamtsbediensteter auf ein polizeiliches Ersuchen ohne richterliche Übermittlungsanordnung eine Terminvereinbarung in der Dienststelle übermittelt und daß die Sozialbehörde Aufenthaltsanfragen der Polizei speichert oder sonst vermerkt und der Polizei künftige Aufenthalte des Betroffenen in der Sozialbehörde mitteilt. Diese Auffassung läßt eine schlüssige Begründung vermissen, inwiefern der im Verhältnis zur Anfrage der Polizei zukünftige Aufenthalt des Betroffenen im Sozialamt noch unter das Tatbestandsmerkmal „derzeitige Anschrift" fallen soll. Die vom Gesetz nicht gestützte Rechtsauffassung des BMA eröffnet eine völlig neue Dimension der Einbeziehung von Sozialämtern und anderen Sozialleistungsträgern in die polizeiliche Fahndung. Aus § 68 SGB X, der dem Wortlaut nach zur Übermittlung der „derzeitigen Anschrift" berechtigt, kann nicht entnommen werden, daß der Gesetzgeber den Sozialleistungsträgern im Zusammenhang mit deren Amtshilfeverpflichtung solch umfassende Mitwirkungspflichten bei der polizeilichen Fahndung auferlegen wollte. In begründeten Einzelfällen ist eine derartige Mitwirkung durch die Befugnisse nach den §§ 69 und 73 SGB X gewährleistet.

Der LfD wies das Ministerium des Innern und für Sport darauf hin, daß er, falls in diesem Punkt keine Klarstellung erfolgt, eine Beanstandung nach § 25 LDSG aussprechen werde.

Bei Drucklegung dieses Tätigkeitsberichts hatte das Ministerium noch nicht Stellung genommen.

11.5.2 Abrechnung von Behandlungskosten

Ein Arzt beschwerte sich beim LfD über einen Sozialleistungsträger. Dieser hatte ihm die Kopie des Krankenscheines einer Sozialhilfeempfängerin zurückgegeben und gefragt, welche der abgerechneten Leistungen mit einer Karzinomerkrankung in Zusammenhang stünden. Der Arzt war der Meinung, es könne doch nicht angehen, daß Sachbearbeiter von Sozialämtern – medizinische Laien – solch empfindliche Informationen zur Kenntnis nehmen dürften.

Datenschutzrechtlich wurde der Vorgang wie folgt beurteilt:

Behandlungskosten für Sozialhilfeempfänger werden, sofern diese nicht krankenversichert sind, mit dem örtlichen Sozialhilfeträger unmittelbar abgerechnet. Sachbearbeitern des Sozialhilfeträgers obliegt die sachliche und rechnerische Prüfung der Abrechnung in ähnlicher Weise, wie sie für Mitglieder der gesetzlichen Krankenkassen durch die Kassenärztlichen Vereinigungen durchgeführt wird. Zum Zwecke der Prüfung müssen sie alle abrechnungsrelevanten Informationen, zu denen auch die Diagnosen gehören, zur Kenntnis nehmen können. Ebenso wie die Mitarbeiter von Krankenkassen oder von Kassenärztlichen Vereinigungen haben die Sachbearbeiter im Sozialamt das Sozialgeheimnis zu wahren. Näheres hierzu bestimmt § 35 SGB I i. V. m. §§ 67 ff. SGB X. Für medizinische Daten existieren Sonderregelungen, die eine Verarbeitung, insbesondere aber die Übermittlung solcher Daten, nur unter besonders engen Voraussetzungen zulassen. Im übrigen unterliegen die Mitarbeiter von Sozialleistungsträgern ebenso wie Ärzte der Strafandrohung des § 203 StGB bei der Verletzung von Privatgeheimnissen.

Die Frage nach den für Karzinomerkrankungen abgerechneten Leistungen hängt mit der Kostenträgerschaft zusammen. Nach § 3 Abs. 1 Nr. 1 des Landesgesetzes zur Ausführung des Bundessozialhilfegesetzes ist der überörtliche Träger der Sozialhilfe – dies ist das Landesamt für Soziales, Jugend und Versorgung – bei Krebserkrankungen sachlich zuständig und hat demzufolge die Behandlungskosten zu tragen. Die Durchführung der Aufgabe ist indessen nach § 1 Abs. 1 Nr. 6 der Vierten Landesverordnung zur Durchführung des Landesgesetzes zur Ausführung des Bundessozialhilfegesetzes an die örtlichen Träger übertragen. Diese müssen, wenn die Behandlung einer Krebserkrankung zusammen mit anderen ärztlichen Leistungen abgerechnet wird, feststellen, welcher Kostenanteil auf diese Behandlung entfällt, damit sie ihn mit dem überörtlichen Sozialhilfeträger abrechnen können.

11.5.3 Übermittlung von Sozialdaten zur Durchführung einer Vollstreckung

Die Übermittlung von Sozialdaten zur Durchführung einer Vollstreckung war Anfang 1996 Gegenstand der Presseberichterstattung. Unter der Schlagzeile „Knöllchenjagd mit Krankenkasse" wurde berichtet, daß eine Ersatzkasse auf Ersuchen eines städtischen Ordnungsamtes die Anschrift des Arbeitgebers eines Mitgliedes mitgeteilt und die Behörde so in die Lage versetzt hatte, einen Pfändungsbescheid wegen Falschparkens in Höhe von 148,– DM zuzustellen. Mit dem Fall war der Petitionsausschuß des Deutschen Bundestags und, obwohl sich die Geschichte in einem anderen Bundesland zugetragen hatte, auch der Bürgerbeauftragte des Landes Rheinland-Pfalz befaßt. Wegen des datenschutzrechtlichen Bezugs unterrichtete dieser den LfD.

Gesetzliche Grundlage für die Datenübermittlung eines Sozialleistungsträgers an die Gemeinde als Vollstreckungsbehörde ist § 67 d Abs. 1 i. V. m. § 68 Abs. 1 Satz 1 SGB X. Diese Vorschriften lassen die Übermittlung von Name, Vorname, Geburtsdatum, Geburtsort, derzeitige Anschrift des Betroffenen sowie Namen und Anschriften seiner Arbeitgeber zu, soweit kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Letzteres ist bei einer Offenbarung zur Vollstreckung öffentlicher Geldforderungen regelmäßig nicht der Fall. Nachteile, die ein Schuldner als Folge der Offenbarung erleidet, muß er auf sich nehmen. Seine Interessen sind insoweit nicht als schutzwürdig anzusehen, denn die Rechtsordnung verpflichtet ihn, Forderungen zu begleichen und gegebenenfalls Vollstreckungsmaßnahmen zu dulden, wenn er seine Zahlungsverpflichtungen nicht erfüllt. Die Übermittlung der Arbeitgeberanschrift an die Vollstreckungsbehörde zur Durchsetzung öffentlich-rechtlicher Ansprüche ist aufgrund der ab dem 1. Juli 1994 geltenden Änderung des § 68 SGB X aber nur noch dann zulässig, wenn sich der Anspruch auf mindestens eintausend Deutsche Mark beläuft. Die Verantwortung für die Zulässigkeit der Übermittlung trägt die Krankenkasse. Sie hat zu prüfen, ob – von Fällen der Einwilligung abgesehen – eine gesetzliche Übermittlungsgrundlage existiert; ist ein Übermittlungsersuchen nicht in vollem Umfang schlüssig, darf eine Übermittlung nicht erfolgen.

In dem der Medienberichterstattung zugrundeliegenden Fall war die Datenübermittlung also nicht zulässig.

Der LfD entspricht mit der Darstellung der rechtlichen Voraussetzungen für die Datenübermittlung der Empfehlung des Petitionsausschusses des Deutschen Bundestages, die auskunftserteilenden wie auch die auskunftsersuchenden Stellen auf die seit dem 1. Juli 1994 geltende Neuregelung hinzuweisen.

11.5.4 Zulässiger Umfang der Datenerhebung bei Anfragen an den Arbeitgeber nach § 116 BSHG

Das Sozialamt einer Stadt verwendet für Anfragen über den Arbeitsverdienst nach § 116 BSHG einen Vordruck, der auf der Kopfseite diese einschlägige gesetzliche Vorschrift zwar im Wortlaut wiedergibt, daneben aber auch die §§ 1605 BGB und

96 SGB VIII als Rechtsgrundlagen nennt und in einem Teil „Bescheinigung über Arbeitsverdienst" Angaben abfragt, die erheblich über die Auskunftspflicht hinausgehen. § 116 BSHG nennt enumerativ die Angaben, auf die sich die Auskunftspflicht des Arbeitgebers erstreckt. Es sind dies die Art und Dauer der Beschäftigung, die Arbeitsstätte und der Arbeitsverdienst. In der Literatur (Schellhorn/Jirasek/Seipp, Komm. z. BSHG, 14. Aufl., § 116 RdNr. 10 m. w. N.) wird die Auffassung vertreten, daß hierzu auch Angaben über die Unterbrechung des Arbeitsverhältnisses sowie über die maßgebende Steuerklasse, evtl. auch Angaben über Kinderzuschlag oder Kindergeld gehören, wenn der Zuschlag oder das Kindergeld im Nettoeinkommen des Arbeitgebers mit enthalten ist. Hingegen lassen sich in dem Vordruck enthaltene Angaben wie „Pfändungen/Vorschuß", nähere Angaben darüber, ob der Abzug vermögenswirksamer Leistungen tarifvertraglich oder durch freiwilligen Anlagevertrag erfolgt, die Angabe „keine Lohnsteuerermäßigung", Angaben zu Lohnpfändungen und Abtretungen sowie Angaben über die Krankenkasse und Angaben zur zweiten Lohnsteuerkarte nicht unter den Begriff „Arbeitsverdienst" fassen. Gleiches gilt für die Aufschlüsselung einmaliger Leistungen und für „detaillierte" Angaben über Ersatzleistungen bei Verdienstausfall. Hier bestehen keine Bedenken gegen die Erhebung der Gesamtleistung, sondern nur gegen die Erhebung von Detailangaben.

§ 1605 BGB gibt einen Anspruch auf Auskunft ausschließlich gegen den Unterhaltsschuldner und nicht auch gegen dessen Arbeitgeber. § 96 SGB VIII betrifft die Überleitung von Ansprüchen gegen einen nach bürgerlichem Recht Unterhaltspflichtigen; ein Auskunftsanspruch des Sozialleistungsträgers kann auf diese Vorschrift ebenfalls nicht gestützt werden.

Der LfD wies in seiner Stellungnahme gegenüber dem Sozialamt ferner darauf hin, daß der Erstbefragungsgrundsatz zu beachten ist: Nach § 67 a Abs. 2 SGB X sind Sozialdaten grundsätzlich beim Betroffenen zu erheben. Im Sinne dieser Vorschrift überwiegen die schutzwürdigen Belange des Betroffenen das Informationsinteresse des Sozialleistungsträgers, wenn dieser trotz der Bereitschaft des Betroffenen zur Mitwirkung eine Anfrage zum Arbeitsverdienst usw. an den Arbeitgeber richtet. Da der Sozialleistungsträger zunächst wenig Bereitschaft zeigte, die Rechtsauffassung des LfD anzuerkennen, drohte dieser eine Beanstandung an, stellte diese aber zurück, weil die betroffene Stadtverwaltung den Städtetag Rheinland-Pfalz und dieser wiederum das Ministerium für Arbeit, Soziales und Gesundheit um eine Stellungnahme ersuchte. Ein Ergebnis lag trotz sechsmonatigen Nachdenkens dieser Stellen und Erinnerung bei Redaktionsschluß dieses Berichts noch nicht vor.

11.5.5 Arbeit statt Sozialhilfe

Im Blick auf die ständig steigenden Kosten der Sozialhilfe sind die Leistungsträger stärker denn je bemüht, Hilfeempfänger in Arbeitsverhältnisse zu vermitteln. Mehrere Landkreise führen Qualifizierungsmaßnahmen „Arbeit statt Sozialhilfe" durch, die auf die berufliche, soziale und sozialrechtliche Integration der Hilfeempfänger zielen. Sie sollen in die Lage versetzt werden, ihre Lebenssituation in materieller, aber wesentlich auch in sozialer und psychischer Hinsicht zufriedenstellender zu gestalten. Ein weiteres wichtiges Ziel ist selbstverständlich die Einsparung von Sozialhilfemitteln. Zielgruppe sind sowohl einheimische Sozialhilfeempfänger als auch Aussiedler, sofern diese nach Erhalt der aussiedlerspezifischen Integrationshilfen (Eingliederungshilfe und Sprachkurs) keiner Erwerbstätigkeit nachgehen können und somit auf Sozialhilfe angewiesen sind. Für den LfD stellte sich im Rahmen einer datenschutzrechtlichen Beurteilung dieser Qualifizierungsmaßnahmen die Frage, ob eine Aufgabenwahrnehmung durch die Kreisverwaltungen zulässig ist, obwohl die Gewährung von Hilfe zur Arbeit als Leistung nach dem BSHG auf Verbandsgemeinden und verbandsfreie Gemeinden übertragen wurde. Eine Klärung dieser Frage war deshalb geboten, weil die „Zuständigkeit für die rechtmäßige Aufgabenerfüllung" bestimmend ist für die Anwendung der gesetzlichen Vorschriften über den Sozialdatenschutz. Es kann beispielsweise nicht angehen, daß Datenübermittlungsbestimmungen dadurch umgangen werden, daß eine gesetzliche Aufgabe ohne Rechtsgrundlage von mehreren Verwaltungen gemeinsam wahrgenommen wird.

Das Ministerium für Arbeit, Soziales und Gesundheit sieht indessen in der allgemeinen Aufgabenübertragung von den Landkreisen an die Verbandsgemeinden und Gemeinden keinen Fall der Delegation von Aufgaben, sondern ein öffentlich-rechtliches Auftragsverhältnis i. S. v. § 96 BSHG. Trotz Beauftragung der Verbandsgemeinden und verbandsfreien Gemeinden obliege den Landkreisen weiterhin die Verantwortung für die Durchführung der dem örtlichen Träger der Sozialhilfe zugewiesenen Aufgaben. Hieraus folge, daß die Landkreise auch weiterhin zuständig seien für die Aufgaben, die die Verbandsgemeinden und verbandsfreien Gemeinden in ihrem Auftrag durchführten. Die Wahrnehmung einer gesetzlichen Aufgabe durch die Landkreise selbst bedeute also nicht, daß Sozialdaten von den Verbandsgemeinden und Gemeinden übermittelt und hierfür ggf. gesetzliche Grundlagen geschaffen werden müßten.

Der LfD teilt diese Rechtsauffassung.

Aufgrund von Eingaben hatte der LfD ferner zu beurteilen, ob die Übermittlung von Sozialdaten an eine externe Einrichtung, die Qualifizierungs- und Vermittlungsleistungen erbringt, nur mit der Einwilligung der Betroffenen zulässig ist. Nach Auffassung des LfD ist eine Datenübermittlung im erforderlichen Umfange aufgrund § 69 Abs. 1 Nr. 1 SGB X zulässig. Daraus folgt, daß die Einwilligung der Betroffenen als Rechtsgrundlage für die Übermittlung von Sozialdaten nicht in Betracht kommt. Der Rückgriff auf die Offenbarungsbefugnis nach § 67 Satz 1 Nr. 1 ist insoweit nicht nur „überflüssig", sondern unzulässig. Öffent-

lichen Stellen ist es nämlich verwehrt, Maßnahmen als zustimmungsbedürftig zu deklarieren, die sie ohnehin durchführen dürften, die der Bürger also mit seinem Willen letztlich nicht verhindern kann (Hase in Borchert, Hase, Walz; GK SGB X 2 RdNr. 20 f. zu § 67).

11.5.6 Unterrichtung des Personalrats bei der Schaffung von Arbeitsgelegenheiten nach § 19 Abs. 1 BSHG im kommunalen Bereich

Ein behördlicher Datenschutzbeauftragter erbat eine Stellungnahme des LfD zu der Frage, in welchen Fällen der Personalrat über die Schaffung von Arbeitsgelegenheiten nach den Vorschriften des Bundessozialhilfegesetzes im kommunalen Bereich unterrichtet werden darf.

Der LfD vertrat folgendes: Wenn gemeinnützige und zusätzliche Arbeit bei Gewährung von Hilfe zum Lebensunterhalt zuzüglich einer angemessenen Entschädigung für Mehraufwendungen gem. § 19 Abs. 2 1. HS 2. Alt. BSHG geleistet wird oder wenn eine Arbeit nach § 20 BSHG erbracht wird, liegt kein Arbeitsverhältnis im Sinne des Arbeitsrechts vor (dies ergibt sich ausdrücklich bereits aus §§ 19 Abs. 3 Satz 1 i. V. m. 20 Abs. 2 Satz 2 BSHG). Soweit aber ein Arbeitsverhältnis bei gemeinnütziger und zusätzlicher Arbeit gem. § 19 Abs. 2 1. HS 1. Alt. BSHG begründet wird, für das das übliche Arbeitsentgelt gewährt wird, liegt ein Arbeitsverhältnis im Sinne des Arbeitsrechts vor. Gleiches gilt selbstverständlich für die nach § 18 BSHG aufgezeigte oder nachgewiesene Arbeit und für die nach § 19 Abs. 1 BSHG geschaffene nicht gemeinnützige und zusätzliche Arbeit.

Daraus folgt, daß der Personalrat über alle Arbeitsverhältnisse, die nach § 19 Abs. 2 1. Alt. BSHG begründet worden sind, zu unterrichten ist. Für die Verhältnisse jedoch, die gem. § 19 Abs. 2 2. Alt. BSHG unter Zahlung von Hilfe zum Lebensunterhalt sowie Mehraufwendungsentschädigung begründet und abgewickelt werden, gilt, daß diese allein sozialhilferechtlichen Charakter haben. In diesem Zusammenhang hat der Personalrat keine Funktion. Eine Übermittlung von Informationen über solche Dienstleistungsverhältnisse an den Personalrat wäre unzulässig.

11.5.7 Abruf von Daten der Zulassungsstelle durch das Sozialamt

Der Datenschutzbeauftragte einer Stadtverwaltung erbat eine Äußerung des LfD zu der Frage, ob § 7 LDSG einer automatisierten Datenübermittlung durch die Kfz-Zulassungsstelle an das Sozialamt entgegensteht.

Sozialleistungsträger sind nach § 20 SGB X befugt, den Sachverhalt in konkreten Verdachtsfällen des Leistungsbetrugs zu ermitteln. Im Rahmen dieser Ermittlungen dürfen sie nach § 69 Abs. 1 Nr. 1 SGB X Einzelanfragen an die Zulassungsstelle richten und damit die Tatsache des Sozialhilfebezugs offenbaren, denn es gehört zu ihren „Aufgaben nach diesem Gesetzbuch", Fälle unberechtigten Sozialhilfebezugs aufzuklären. Die vom Sozialamt begehrten Auskünfte können durch die Zulassungsstelle erteilt werden, wenn dies zur Verfolgung von Straftaten oder zur Verfolgung von Ordnungswidrigkeiten erforderlich ist (§ 35 Abs. 1 Nr. 2 und 3 StVG).

Neben der Einzelfallüberprüfung ist im Rahmen der Amtsermittlung nur der automatisierte Datenabgleich zugelassen (§ 117 Abs. 3 BSHG). Danach darf das Sozialamt Identitätsdaten (Abs. 1 Satz 2) von Leistungsempfängern an die Zulassungsstelle übermitteln, die einen automatisierten Abgleich dieser Daten mit eigenen Datenbeständen zur Feststellung der Eigenschaft als Kraftfahrzeughalter (Abs. 3 Satz 4 Buchst. f) durchführt und Daten über Feststellungen dem Sozialamt mitteilt. Andere Formen der automatisierten Datenübermittlung der Zulassungsstelle an das Sozialamt (beispielsweise im Online-Verfahren) sind nach dieser Vorschrift, aber auch nach den Bestimmungen des Straßenverkehrsgesetzes und der Fahrzeugregisterverordnung unzulässig. Die Anwendung des § 7 LDSG kommt wegen des Vorranges der o. a. spezialgesetzlichen Regelungen nicht in Betracht.

11.5.8 Verwendung von Vordrucken im Sozialleistungsbereich

Der Inhalt von Vordrucken, die im Sozialleistungsbereich verwendet werden, ist immer wieder Gegenstand von Eingaben. Dabei geht es häufig um Einverständniserklärungen, die nicht den Anforderungen an eine freie, durch keine sachfremden Erwägungen bestimmte Willenserklärung entsprechen (vgl. 14. Tb., Tz. 11.3.2). So meinen beispielsweise Sozialämter, sie könnten die Übermittlungsrestriktionen des Sozialgesetzbuchs (§§ 67 d ff. SGB X) dadurch umgehen, daß sie sich für jede, aus ihrer Sicht sachdienliche Datenübermittlung schon bei der Antragstellung vorsorglich eine Einwilligungserklärung der Betroffenen unterschreiben lassen. Es gab sogar schon Fälle, in denen Sozialhilfeträger den Antragstellern eine Erklärung über den „freiwilligen" Verzicht auf die Anwendung der gesetzlichen Vorschriften zum Sozialdatenschutz zur Unterschrift vorlegten. Selbstverständlich ist eine solche Erklärung rechtlich unwirksam: Ein Antragsteller, der existentiell auf die Hilfe des Staates angewiesen ist, kann in dieser Situation nicht frei über die Zulässigkeit von Eingriffen in das Recht auf informationelle Selbstbestimmung entscheiden. Die Sozialleistungsträger beachten nicht genügend, daß die Übermittlungsregelungen des Sozialleistungsrechts fast keinen Raum mehr lassen für Datenübermittlungen auf der Grundlage der Einwilligung. Nur wenn der Betroffene wirklich frei und ohne Furcht vor den Nachteilen einer Auskunftsverweigerung, wozu auch eine „klimatische" Verschlechterung des Verhältnisses zum Leistungsträger zählt, entscheiden kann, bildet die Erklärung eine tragfähige Grundlage der Datenübermittlung.

Nicht selten wird auch die Auffassung vertreten, daß eine schriftliche Einverständniserklärung zwar bei Bestehen einer gesetzlichen Übermittlungsgrundlage überflüssig sein könne, ein entsprechendes Verwaltungshandeln aber weder unzulässig noch rechtswidrig sei. Dem ist nicht so. Die Einwilligung des Betroffenen und gesetzliche Übermittlungsbefugnisse schließen sich als Rechtsgrundlagen für die Offenbarung von Sozialdaten wechselseitig aus. Grundsätzlich verdrängen die gesetzlichen Befugnistatbestände die Einwilligung des Betroffenen.

Einen geradezu dreisten Fall der Nichtbeachtung datenschutzrechtlicher Vorschriften hatte der LfD im Berichtszeitraum zu beklagen. Ein Sozialamt war darauf hingewiesen worden, daß Einwilligungserklärungen in einer ganzen Reihe von Vordrucken nicht den gesetzlichen Anforderungen entsprachen. Nach einem längeren Schriftwechsel und ausführlicher Darlegung der datenschutzrechtlichen Gründe zeigte sich die Behörde einsichtig: Sie legte Vordrucke vor, die den gesetzlichen Anforderungen entsprachen, und teilte mit, daß die veralteten Vordrucke vernichtet wurden. Eine Überprüfung durch den LfD, wenige Monate danach, ergab, daß die Vordrucke in der „veralteten" Fassung doch noch verwendet wurden. Das Sozialamt sprach in seiner Stellungnahme zu dem Vorgang von einem bedauerlichen Versehen, das zustande kam, „als eine Auszubildende mit der Vervielfältigung von Formularen beschäftigt war". Unerwähnt blieb, daß die Vordrucke von Sachbearbeitern des Sozialamtes weiterbenutzt wurden, die aufgrund ihrer Gesetzeskenntnis, zumindest aber aufgrund des vorangegangenen Schriftwechsels mit dem LfD hätten wissen müssen, daß die Vordrucke nicht den datenschutzrechtlichen Anforderungen entsprachen.

Im Grundsatz sieht der LfD in der Verwendung von Vordrucken mit teilweise unzulässigem Inhalt eher einen unerheblichen Mangel i. S. v. § 25 Abs. 2 LDSG. In dem geschilderten Falle erschien diese Beurteilung aber unangemessen; der Vorgang wurde als Verstoß gegen datenschutzrechtliche Vorschriften beanstandet.

11.5.9 Verweisung von Antragstellern auf Sozialhilfe an freie Träger

Im 12. Tb. berichtete die DSK unter Tz. 12.8.3 über die Praxis von Sozialämtern, Antragsteller auf Bekleidungsbeihilfen vorrangig an Kleiderkammern der freien Wohlfahrtspflege zu verweisen. Hiermit ist eine Übermittlung von Sozialdaten verbunden, wenn die Antragsteller einen „Laufzettel" erhalten, auf dem die benötigten Kleidungsstücke genannt und Eintragungen vorgesehen sind, die den Leistungsträger darüber informieren, ob ein Bekleidungsstück vorhanden war und angenommen wurde, ob es vorhanden war und die Annahme verweigert wurde oder ob es nicht vorhanden war.

Die DSK hielt seinerzeit die mit der Anwendung des Laufzettelverfahrens verbundene Übermittlung von Sozialdaten in Ausnahmefällen für zulässig, in denen Zweifel an der Richtigkeit der Antragsangaben im Rahmen der Mitwirkung nach §§ 60 ff. SGB I nicht auszuräumen sind.

Im übrigen vertrat sie in Übereinstimmung mit dem Ministerium für Soziales und Familie die Auffassung, daß die Abgabe der Bekleidungsstücke in den Kleiderkammern so organisiert werden muß, daß die berechtigten Belange der Betroffenen soweit wie möglich berücksichtigt werden. Es dürfte insbesondere nicht erforderlich sein, den Betroffenen namentlich als Empfänger aufzurufen mit der Folge, daß alle übrigen in der Kleiderkammer anwesenden Personen hiervon Kenntnis erlangen. Die freien Träger der Wohlfahrtspflege sollten dafür sorgen, daß in ihren Kleiderkammern das Verfahren der Abgabe von Kleidungsstücken an Bedürftige – unabhängig davon, ob es sich um Sozialhilfeempfänger handelt oder nicht – so gestaltet wird, daß den berechtigten Diskretionsbedürfnissen der Betroffenen Rechnung getragen wird. Wo dies nicht der Fall sei, sollten die örtlichen Träger der Sozialhilfe auf ein entsprechendes Verfahren hinwirken. Das Fehlen einer angemessenen Verfahrensweise bei der Leistungsgewährung in den Kleiderkammern sei im übrigen bei der Ermessensentscheidung über die Form der Hilfegewährung zu berücksichtigen. Es könne zur Folge haben, daß die Leistungsgewährung in dieser Form von vornherein unzulässig sei.

Auch das Ministerium für Arbeit, Soziales und Gesundheit hat sich nun nach Abstimmung mit der Arbeitsgemeinschaft der Sozialhilfeträger zu der Thematik geäußert. Es hält eine Bestätigung für den Besuch der Kleiderkammer für zwingend, da es jeglicher Praxiserfahrung widerspreche, daß die betroffenen Personen selbständig oder nach Aufforderung durch das Sozialamt ohne Nachweisverfahren den Versuch unternehmen würden, den Bedarf durch Kleiderkammern zu decken. Der Verweis an Kleiderkammern erfolge in der Regel aber nur dann, wenn der Hilfeempfänger einen über dem Durchschnitt liegenden Bedarf an Kleidern geltend mache oder bekannte Unzuverlässigkeit vorliege. Im übrigen werde den berechtigten Diskretionsbedürfnissen der Betroffenen selbstverständlich Rechnung getragen. So sei in allen Fällen gewährleistet, daß lediglich Mitarbeiterinnen und Mitarbeiter der Kleiderkammer, die entweder Bedienstete der Kommune oder aber eines Wohlfahrtsverbandes seien, Einsicht in den Laufzettel erhielten. Hierbei sei es unschädlich, daß dabei in geringem Umfange personenbezogene Daten übermittelt würden, denn die datenschutzrechtlichen Normen seien auch von den freien Trägern zu beachten. Dies werde insbesondere durch die „Verlängerung" des Sozialgeheimnisses i. S. v. § 35 SGB I auf die freien Träger nach § 78 SGB X deutlich.

Der LfD vertritt die Auffassung, daß eine an dieser Verfahrensbeschreibung orientierte Inanspruchnahme von Kleiderkammern und die damit verbunden Sozialdatenübermittlung zulässig sind. Ob freilich die dargestellten Konventionen – Ausnahmecharakter der Inanspruchnahme von Kleiderkammern und Beachtung der Diskretionsbedürfnisse – von beiden Seiten beachtet

werden, muß vor dem Hintergrund von Informationen, die der LfD über die Praxis erhält, eher bezweifelt werden. Bisher bestand zwar noch kein Anlaß, eine Beanstandung auszusprechen; der LfD wird aber die Entwicklung weiter sorgfältig beobachten. Auch in Zeiten knapper Kassen dürfen Sozialämter jedenfalls nicht dazu übergehen, die Leistungsgewährung mit einer Prangerwirkung zu verbinden, die auf die Antragsteller abschreckend wirkt.

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

Gegenstand der Berichterstattung im 15. Tb. (Tz. 11.6) war die Archivierung besonders sensibler Akten von Beratungsstellen. Der LfD vertrat die Auffassung, daß Beratungsakten mit personenbezogenen Informationen, die zum Zweck persönlicher und erzieherischer Hilfe anvertraut worden sind (§ 65 Abs. 1 SGB VIII), dem Archiv nicht angeboten werden dürfen.

Ein Datenschutzbeauftragter erbat zu dieser Auslegung gesetzlicher Vorschriften nähere Erläuterungen. Er sah einen Widerspruch zwischen dieser Auslegung und § 7 LArchG, der die Anbietungspflicht „sogar auf Unterlagen, die der Geheimhaltungspflicht unterliegen" erstrecke und damit § 2 Abs. 4 BundesarchivG folge.

Der LfD wies in seiner Stellungnahme darauf hin, daß sich die Archivierung von Sozialdaten ausschließlich nach § 71 Abs. 1 Satz 3 SGB X richtet und daß diese Regelung gegenüber den Archivgesetzen vorrangig ist. Soweit die Archivgesetze des Bundes oder der Länder Anbietungspflichten begründen, sind diese Pflichten nur nach Maßgabe der speziellen sozialgesetzlichen Regelungen anzuwenden.

§ 71 Abs. 1 SGB X begründet nun aber gerade keine Übermittlungsbefugnis für anvertraute Daten i. S. d. § 65 SGB VIII. Diese Bestimmung ist nämlich wiederum eine spezielle Regelung im Verhältnis zu §§ 69 ff. SGB X. Da bei den Übermittlungsbestimmungen des § 65 Abs. 1 Nrn. 1 bis 3 SGB VIII nicht auf § 71 SGB X Bezug genommen wird, ist eine Weitergabe der Unterlagen mit solchen anvertrauten Daten zu Archivierungszwecken nicht zulässig. Insoweit ist das Schweigen des § 65 SGB VIII ein beredtes Schweigen, das eine Archivierung solcher Daten ausschließt. Eine solche Auslegung ist nach Sinn und Zweck des § 65 SGB VIII auch deshalb geboten, weil die im Rahmen persönlicher und erzieherischer Hilfen anvertrauten Daten einen besonders qualifizierten Schutz erfordern. Dem Vertrauensverhältnis bei der Datenerhebung nach § 65 SGB VIII kommt eine Bedeutung zu, die über das Berufsgeheimnis des § 203 StGB und über andere Amtsgeheimnisse hinausgeht. Bezüglich § 203 StGB folgt dies daraus, daß der besondere Vertrauensschutz in der persönlichen und erzieherischen Hilfe nur „anvertraute" und nicht auch „sonst bekanntgewordene" Geheimnisse umfaßt.

Dieser Archivierungsausschluß gilt selbstverständlich nur für personenbezogene oder personenbeziehbare Daten. Es bestehen also keine Bedenken gegen die Archivierung solcher Unterlagen von Beratungsstellen, die nicht personenbezogen oder personenbeziehbar sind. Diese Archivierung wäre aus der Sicht des LfD nicht nur zulässig, sondern im Interesse der Archivarbeit auch zu unterstützen. Der mit der Anonymisierung verbundene Arbeitsaufwand dürfte sich in Grenzen halten, wenn er nur für solche Unterlagen geleistet wird, die von einem Archiv auch tatsächlich übernommen werden.

11.7 Zahlung von Kriegsbeschädigtenrenten an ehemalige Mitglieder der Waffen-SS

Im Frühjahr 1997 gab es im In- und Ausland eine breite Medienberichterstattung über die Gewährung von Kriegsbeschädigtenrenten vor allem an ehemalige Mitglieder der Waffen-SS. In den USA wurden einige Personen ausfindig gemacht, die auf deutscher Seite an Kriegsverbrechen beteiligt waren und die von Deutschland Versorgungsbezüge erhielten. Da der Ausschlußtatbestand des § 64 BVG vorlag, wurde die Zahlung der Versorgungsbezüge in zwei Fällen eingestellt.

Das Bundesministerium für Arbeit wandte sich in einem Rundschreiben an die Bundesländer und bat um Namenslisten der Empfänger von Versorgungsleistungen, die im Ausland leben. Er beabsichtigte, die zuständigen Justizbehörden in westlichen Nachbarstaaten und in einigen osteuropäischen Ländern um Prüfung zu bitten, ob sich Personen unter den Leistungsempfängern befinden, über die dort weitergehende Erkenntnisse im Blick auf den Ausschlußtatbestand des § 64 BVG vorliegen.

Das Landesamt für Soziales, Jugend und Versorgung übermittelte aufgrund dieser Anforderung die Anschriften von 78 in Luxemburg lebenden Versorgungsberechtigten. Zur Zulässigkeit dieser Datenübermittlung vertrat das Ministerium für Arbeit, Soziales und Gesundheit die Auffassung, der Bund habe die Aufsicht über die Gesetzmäßigkeit der Ausführung des Bundesversorgungsgesetzes und und deshalb auch einen Anspruch auf Übermittlung von Namenslisten der Empfänger von Versorgungsleistungen im Ausland. Anders verhalte es sich bei der Übermittlung einzelner Listen an die Wohnsitzstaaten der Versorgungsempfänger. Hier seien die datenschutzrechtlichen Vorgaben unbedingt zu beachten, für deren Einhaltung das BMA jedoch die alleinige Verantwortung trage.

Auch das BMA verwies in einer Stellungnahme zur Zulässigkeit der Datenübermittlung durch die Versorgungsverwaltungen der Länder auf die Rechtsaufsicht nach Art. 84 GG, die ihm zustehe. Art. 84 GG sei gegenüber den datenschutzrechtlichen Vorschriften vorrangig.

Diese Rechtsauffassung ist aus verschiedenen Gründen angreifbar, insbesondere aber deshalb, weil es sich bei der erbetenen Datenübermittlung nicht um eine Maßnahme der Rechtsaufsicht handelt, sondern um Sachverhaltsermittlungen, also Maßnahmen des Verwaltungsvollzugs, für die die Länder zuständig sind. Daß die Länder sich nicht an das geltende Recht hielten, machte das BMA selbst nicht geltend.

Zugleich konkretisierte das BMA aber auch seine Vorgehensweise. Es nannte als Grundvoraussetzung für eine Datenübermittlung an die Wohnsitzstaaten, daß dort ein rechtsstaatliches Verfahren gewährleistet ist. Beeinträchtigungen schutzwürdiger Interessen nicht betroffener Leistungsempfänger – beispielsweise mögliche Repressalien im Anschluß an die Veröffentlichung der Identität betroffener Personen oder Einsichtsmöglichkeit durch Private oder sonstige Organisationen – müßten ausgeschlossen sein. § 77 Abs. 3 SGB X werde beachtet, d. h. mit dem Wohnsitzstaat werde vorher in geeigneter Weise geklärt, daß die Daten nur unter der Voraussetzung herausgegeben werden dürfen, daß die andere Seite bereit ist, sie insbesondere nicht öffentlich bekanntzugeben und nur für Zwecke der Feststellung des Ausschlußtatbestandes zu verwenden. Auch außenpolitische und Opportunitätserwägungen könnten der Übermittlung entgegenstehen, ebenso innenpolitische Gesichtspunkte der Wohnsitzstaaten. So würden also keineswegs alle von den Versorgungsverwaltungen zur Verfügung gestellten Daten weitergegeben, sondern es werde streng geprüft, in welchen Einzelfällen die rechtlichen Voraussetzungen vorlägen.

Diese Gesichtspunkte hätten freilich die Überlegungen der übermittelnden Stelle (Landesamt) zur rechtlichen Zulässigkeit der Datenübermittlung an das BMA bestimmen müssen. Soweit z. B. eine Weiterübermittlung von Daten durch das BMA an andere Staaten allein schon wegen § 77 SGB X nicht in Betracht kam, hätte auch eine Übermittlung an das Ministerium nicht erfolgen dürfen. Gleiches gilt, wenn für die Versorgungsverwaltung erkennbar war, daß ein Leistungsentzug nach § 64 BVG von vornherein ausscheidet.

Grundvoraussetzung einer Datenübermittlung an das BMA hätte also die fachliche Beurteilung der Zulässigkeit i. S. v. § 69 Abs. 1 Nr. 1 SGB X durch die übermittelnden Stellen sein müssen. Das BMA hätte durchaus Hinweise geben können, die für diese fachliche Beurteilung von Bedeutung sind; es konnte jedoch nicht, wie geschehen, Weisung zur Datenübermittlung erteilen, um dann selbst über die Weiterübermittlung zu entscheiden.

12. Ausländerrecht

12.1 Verwaltungsvorschriften zum Ausländergesetz

Die Verwaltungsvorschriften zum Ausländergesetz scheinen nun doch in eine abschließende Bearbeitungsphase zu geraten. Aus der Sicht des Datenschutzes ist dies ausdrücklich zu begrüßen, da mit ihrer endgültigen Inkraftsetzung viele Unklarheiten beseitigt werden, die in der Praxis nicht selten zu Lasten des Datenschutzes gingen.

Im Laufe der Vorbereitungen, bei denen der LfD beteiligt wurde, sind dessen Vorschläge im wesentlichen mit Unterstützung durch das Ministerium des Innern und für Sport berücksichtigt worden. So werden Behörden, die der Ausländerbehörde von sich aus bestimmte Mitteilungen zu machen haben, nur noch eingeschränkt angehalten, bestehende Zweifel durch eigene umfassende Ermittlungen abzuklären, was mit zusätzlichen Eingriffen in das Recht auf informationelle Selbstbestimmung der Betroffenen verbunden gewesen wäre. Bei Mitteilungen an die Ausländerbehörde über die bloße Einleitung von Straf- und Bußgeldverfahren unterbleibt jetzt die Nennung anderer Personen.

Neu hinzugekommen sind Regelungen über die Behandlung der Verpflichtungserklärungen nach § 84 AuslG von Personen, die einen Ausländer einladen wollen. Diese Regelungen entsprechen nicht den in diesem Bericht („Verpflichtungserklärung vor Visum an ausländischen Gast", Tz. 12.5) dargestellten datenschutzrechtlichen Erfordernissen. Das Ministerium wurde insoweit um Unterstützung bei den Abstimmungen über die Endfassung gebeten.

12.2 Versehen der Behörde: Festnahmen an der Grenze

Ein im Jahre 1989 bestandskräftig ausgewiesener kroatischer Staatsangehöriger wird vier Jahre später aufgrund der in diesen Fällen üblichen Fahndungsnotierung in INPOL nach einem Kurzaufenthalt von wenigen Tagen in Deutschland an der bayerischen Grenze bei der Ausreise festgenommen und erhält einen Strafbefehl über 4 500,– DM. Sein Einwand, die Ausländerbehörde einer rheinland-pfälzischen kreisfreien Stadt habe ihm die befristete Betretenserlaubnis mündlich erteilt, hilft nicht.

Am 21. Dezember 1993 wird die aufgrund der alten Ausweisung von 1989 fortbestehende Wiedereinreisesperre auf Antrag des Betroffenen von der zuständigen Kreisverwaltung als Ausländerbehörde beendet; dennoch wird er im April 1994 und im Juni 1996 an der Grenze in Bayern festgenommen.

Der Grund: Die Fahndungsausschreibung in INPOL sowie die entsprechende Notiz im AZR besteht noch immer. Die Folge: zwei überflüssige Festnahmen mit insgesamt mehrtägigem Freiheitsentzug.

Erst nach Intervention des Rechtsanwalts des Betroffenen und des leider erst Anfang August 1996 eingeschalteten LfD wurde die Fahndungsnotierung in INPOL und AZR gelöscht.

Die anschließenden Feststellungen führten zu einer massiven Beanstandung des LfD gegenüber der zuständigen Kreisverwaltung als Ausländerbehörde.

Der Vorgang von 1993 ließ sich mit hinreichender Bestimmtheit nicht mehr aufklären, denn weder bei der zuständigen Ausländerbehörde der Kreisverwaltung noch bei der unzuständigen Stadtverwaltung, die die mündliche Betretenserlaubnis erteilt haben soll, war entsprechender Aktenrückhalt vorhanden. Für die Version des Betroffenen spricht jedoch, daß in der fraglichen Zeit vor dem Vorfall die Ausländerakte zwischen der Kreisverwaltung und der Stadtverwaltung hin- und herging. Der Grund hierfür war aber bei beiden nicht festgehalten.

Die Löschung der Fahndungsnotierung in INPOL wie auch die entsprechende Speicherung im AZR hätte von der Ausländerbehörde der zuständigen Kreisverwaltung bereits im Dezember 1993 im zeitlich unmittelbaren Zusammenhang mit der Befristung (Beendigung) der Wiedereinreisesperre erfolgen müssen. Aufgrund eines Vermerks in den Akten soll dies am 10. Januar 1994 verfügt worden sein, wurde aber tatsächlich nicht vollzogen. Im Februar 1996 wurde ausweislich der Vorgänge – aus welchem Anlaß auch immer – erneut die Löschung verfügt. Tatsächlich erfolgte diese jedoch erst nach der erneuten und letzten Festnahme des Betroffenen an der Grenze. Die Kreisverwaltung räumt dies ein und bedauert es. Dort wurden inzwischen die notwendigen organisatorischen und personellen Veränderungen getroffen, daß künftig die beanstandeten Unregelmäßigkeiten ausgeschlossen werden können.

Außerdem wird jetzt bei Erteilung einer befristeten Betretenserlaubnis nach § 9 Abs. 3 AuslG durch einen gesonderten Vermerk sichergestellt, daß während deren zeitlicher Geltung die Ausschreibung zur Festnahme ausgesetzt ist. Die vom Ministerium des Innern und für Sport an das Bundesinnenministerium weitergegebene Anregung des LfD, im AZR in geeigneter Weise auf befristete Betretenserlaubnisse hinzuweisen, hat bis jetzt noch nicht zu einem konkreten Ergebnis geführt.

12.3 Gruppenauskünfte aus dem Ausländerzentralregister

Nach §§ 12, 15 bis 17 und 20 AZRG können auf Antrag vom AZR u. a. an Ausländerbehörden, Polizeivollzugsbehörden, Staatsanwaltschaften und Gerichte unter bestimmten Voraussetzungen Gruppenauskünfte übermittelt werden. Das sind Daten einer Mehrzahl von Ausländern, die in einem Übermittlungsersuchen nicht mit vollständigen Grundpersonalien bezeichnet sind und die aufgrund im Register gespeicherter und im Übermittlungsersuchen angegebener gemeinsamer Merkmale zu einer Gruppe gehören. Soweit eine Gruppenauskunft an eine öffentliche Stelle des Landes übermittelt wurde, hat die Registerbehörde nach § 12 Abs. 3 AZRG den LfD davon zu unterrichten.

Seit Inkrafttreten des AZRG im Oktober 1994 sind insgesamt vier derartige Gruppenauskünfte erteilt worden, davon entfallen drei auf die Berichtsperiode. Soweit der Grund des Auskunftsersuchens aus der Mitteilung des Bundesverwaltungsamtes nicht eindeutig hervorging, wurden vom LfD im Lande ergänzende Feststellungen getroffen.

In allen Fällen waren jedoch die gesetzlichen Voraussetzungen erfüllt.

12.4 Förderung der freiwilligen Rückkehr bosnischer Flüchtlinge durch die Europäische Union

EU-Mittel zur Unterstützung der freiwilligen Rückkehr bosnischer Bürgerkriegsflüchtlinge werden für die jeweils einzelnen Förderobjekte (z. B. Häuser) nur dann zur Verfügung gestellt, wenn konkret die Namen der entsprechenden Bewohner/Eigentümer genannt werden. Den Hintergrund bildet die Regelung im sog. Dayton-Abkommen, wonach Betroffene die Wahl haben, entweder an ihren Heimatort oder an einen anderen von ihnen gewünschten Ort zurückzukehren. Das Bundesministerium des Innern benötigt alle Daten der in Frage kommenden Flüchtlinge, damit sie im Bedarfsfall ohne weitere Rückfrage der EU sofort und gezielt übermittelt werden können.

In jedem einzelnen Fall wird das zu fördernde Objekt in Bosnien-Herzegowina besichtigt und anschließend Kontakt mit den Betroffenen hier aufgenommen.

Aus der Sicht des Ministeriums des Innern und für Sport ist es außerordentlich wichtig, daß die Mittel sobald wie möglich abfließen, damit auch die dazugehörigen Maßnahmen zur Wiederherstellung der Infrastruktur anlaufen können.

Zur Durchführung der von Deutschland aus erforderlichen Vorbereitungen der Fördermaßnahmen wurde eine Projektgruppe beim Bundesamt für die Anerkennung ausländischer Flüchtlinge gebildet.

Das Ministerium hat daher den LfD von der Absicht unterrichtet, die Ausländerbehörden zu bitten, ihm die Namen und die Anschriften aller Flüchtlinge aus Bosnien-Herzegowina zu übermitteln, damit diese dem Bundesamt übermittelt werden

können. Dem Ministerium wurde daraufhin mitgeteilt, daß mit ihm Übereinstimmung besteht, daß die Übermittlung der Daten durch das Land von der Gemeinwohlregelung im allgemeinen Datenschutzrecht (§ 14 Abs. 1 sowie § 12 Abs. 4 LDSG) umfaßt und damit zulässig ist. Dies muß insbesondere vor dem Hintergrund gelten, daß die rasche Realisierung wesentlicher Bestandteile des Dayton-Abkommens im offensichtlichen Interesse des Gemeinwohls liegt.

Im übrigen war darauf hinzuweisen, daß die Verantwortung für die Zulässigkeit der Datenübermittlung bei der empfangenden Stelle liegt, da diese (Bundesministerium des Innern bzw. das Bundesamt für die Anerkennung ausländischer Flüchtlinge) das entsprechende Ersuchen stellt. Die übermittelnde Stelle des Landes prüft nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben der empfangenden Stelle liegt. Hier wäre also in erster Linie der BfD gefragt.

Aufgrund näherer Feststellungen durch den LfD kann auch davon ausgegangen werden, daß die Daten „Ethnie" und „Religion" zur Aufgabenerfüllung erforderlich sind, im Zweifel sogar zum Schutze der Betroffenen. Außerdem ist die „Ethnie" praktisch mit Religion identisch und geht ohnehin überwiegend aus dem Namen hervor. Dies wurde dem Ministerium gesondert mitgeteilt.

Für die Durchführung der Übermittlungen hat der LfD jedoch besondere Sicherungsmaßnahmen gefordert. Wegen der großen Anzahl zum Teil sensibler Daten sollte deren Versendung auf Diskette nur in verschlüsselter Form erfolgen. Außerdem ist die genutzte Festplatte zu verschlüsseln. Das Ministerium hat die Forderungen in einem Rundschreiben an die Ausländerbehörden im wesentlichen weitergegeben.

12.5 Verpflichtungserklärung vor Visum an ausländischen Gast

Nach § 84 Abs. 1 AuslG kann jemand, der Ausländer aus bestimmten Staaten einlädt, sich, falls dies Voraussetzung für die Visumerteilung ist, gegenüber der zuständigen Ausländerbehörde verpflichten, die Kosten des Lebensunterhaltes des Ausländers zu tragen. Die Erklärung bedarf der Schriftform.

Für die Erklärung wird ein bundeseinheitliches Formular verwendet. Da § 84 AuslG die Kenntnis der erforderlichen Daten in schriftlicher Form voraussetzt, ist ihre Erhebung in Form der Verpflichtungserklärung gem. § 75 Abs. 1 AuslG im Grundsatz zulässig. In einigen Punkten stellt sich allerdings die Frage nach der Erforderlichkeit der Datenerhebung. Dies gilt z. B. für die Frage, ob der Verpflichtete Mieter oder Wohnungseigentümer ist, ebenso wie für die weiteren Fragen nach dem Beruf und dem Arbeitgeber. Letzteres wird ohnehin nur in Ausnahmefällen akut, wenn sich aufgrund der Verpflichtungserklärung eine Zwangsvollstreckung ergibt. Die Angabe kann dann immer noch erhoben werden.

Besonderer Prüfung aus der Sicht des Datenschutzes bedarf die Frage, ob und inwieweit der Verpflichtete tatsächlich in der Lage ist, für alle Kosten einschließlich Versorgung im Krankheits- oder Pflegefall aufzukommen, die durch seinen Gast verursacht werden. Hier ist gemäß dem Grundsatz der Erforderlichkeit ein enger Maßstab anzulegen. Dem Verpflichteten sollte es zunächst freigestellt sein, wie und durch Vorlage welcher Nachweise er der Ausländerbehörde glaubhaft macht, daß er zur Tragung der Kosten in der Lage ist. Die Frage ist am einzelnen Fall zu entscheiden. Eine schematische Prüfung eignet sich nicht. Festgehalten werden sollte lediglich das erforderliche Ergebnis der Glaubhaftmachung bzw. des Nachweises.

Bei der datenschutzrechtlichen Bewertung des Vordrucks muß besonders bedacht werden, daß die darin enthaltenen Angaben nicht nur bei der Ausländerbehörde verbleiben, sondern daß eine Ausfertigung an den eingeladenen Ausländer geht. Dieser erhält auf diese Weise Kenntnis von den Angaben. Der Erklärende hat dabei keinerlei Sicherheit, daß die Angaben nur zur Erlangung des Visums verwendet werden.

Darüber hinaus muß der eingeladene Ausländer u.U. die Verpflichtungserklärung nochmals bei der Grenzkontrolle vorweisen.

Der LfD hat die wesentlichen Überlegungen hierzu dem Ministerium des Innern und für Sport mitgeteilt. Der Gedankenaustausch ist noch nicht abgeschlossen.

12.6 Machbarkeitsstudie für ASYLCARD

Das informationelle Selbstbestimmungsrecht gilt auch für Asylbewerber. Die Zusammenführung von personenbezogenen Daten aus dem Arbeitsbereich verschiedener Stellen auf einer Asylchipkarte stellt wegen der damit verbundenen Rundumerfassung im Grundsatz einen erheblichen Eingriff in dieses Recht dar.

Schon im 15. Tb. (Tz. 12.1) wurde die Frage nach der Verhältnismäßigkeit gestellt und darauf hingewiesen, daß allgemein mit der Zunahme der Bereiche mit Kartenlösungen das Bedürfnis nach „praktischer und effizienter" Vereinheitlichung oder Zusammenführung wächst.

Nunmehr ist im Bundesausschreibungsblatt die „Leistungsbeschreibung zur Durchführung einer Machbarkeitsstudie zum Einsatz einer Smart-Card im Asylverfahren" durch das Bundesministerium des Innern veröffentlicht worden. Der LfD hat auch bei diesem Anlauf bereits im Vorfeld gegenüber dem Ministerium des Innern und für Sport die früher geäußerten grundsätzlichen Bedenken wiederholt und ausdrücklich aufrechterhalten. Dabei hat er u. a. auf die Gefahr hingewiesen, daß ggf. Stellen, die lesend zugriffsberechtigt sein sollen, Daten abfragen können, die für ihre Aufgabenerfüllung nicht erforderlich sind. Auch die mit dem möglichen manipulativen Verlust von Karten zusammenhängenden Fragen sollten eingehend geprüft werden. Dem Ergebnis der Machbarkeitsstudie wird daher aus der Sicht des Datenschutzes größte Aufmerksamkeit zu widmen sein, denn es ist nicht ganz von der Hand zu weisen, daß durch das Ergebnis der Machbarkeitsstudie Fakten geschaffen werden könnten, die eine Diskussion in der Öffentlichkeit und die Entscheidung in den Parlamenten von Bund und Ländern im Hinblick auf Änderungen der Rechtslage (insbesondere der Datenschutzgesetze) quasi vorwegnehmen würden.

13. Finanzverwaltung

13.1 Novellierung der Abgabenordnung

Die Situation bezüglich der Ergänzung der Abgabenordnung um datenschutzrechtlich relevante Vorschriften hat sich seit der im 15. Tb. geschilderten Sachlage (Tz. 13.1) nicht grundsätzlich geändert. Nach wie vor bestreitet das Bundesministerium der Finanzen prinzipiell die Erforderlichkeit solcher datenschutzrechtlichen Ergänzungen. Die Datenschutzbeauftragten des Bundes und der Länder haben eine Bestandsaufnahme der aus ihrer Sicht wünschenswerten und notwendigen Änderungen der Abgabenordnung erstellt. In diesem Zusammenhang besteht nach ihrer Auffassung Handlungsbedarf, beispielsweise bezüglich der Frage, in welchem Umfang Aufgaben der Steuerverwaltung privatisiert werden dürfen.

Der LfD wird die Bestrebungen weiterhin unterstützen, in die Abgabenordnung normenklare datenschutzrechtlich gebotene Regelungen aufzunehmen.

13.2 Die Steuerdaten-Abrufverordnung

Seit dem 11. Tb. (Tz. 15.2.4) hat Anlaß bestanden zu beklagen, daß der Erlaß der Steuerdaten-Abrufverordnung nicht vorankommt (s. zuletzt den 15. Tb., Tz. 13.2). Nunmehr dürfte endgültig festzustellen sein, daß die Bemühungen um den Erlaß der Verordnung gescheitert sind. Es war keine Einigkeit darüber zu erzielen, ob bzw. in welchem Umfang die kommunalen Steuerbehörden in den Geltungsbereich der Verordnung einzubeziehen sind.

Es ist derzeit allerdings beabsichtigt, den für die Rechtsverordnung vorgesehenen Regelungsinhalt im Wege einer zwischen den Ländern und dem Bund einheitlich vereinbarten Verwaltungsanordnung in Kraft zu setzen. Damit wären die Gemeinden vom Geltungsbereich ausgenommen.

Falls der Inhalt dieser Verwaltungsanordnung nicht hinter den zuletzt vorliegenden Entwürfen der Steuerdaten-Abrufverordnung zurückbleibt, wäre auch dies als datenschutzrechtlich nützlicher Schritt zu begrüßen. Diese Verwaltungsvorschrift würde auch im Bereich der Kommunen eine beispielgebende Wirkung entfalten; bereits der Entwurf der Steuerdaten-Abrufverordnung hat dem LfD wiederholt als Argumentationshilfe gegenüber den Steuerbehörden gedient. Die förmliche Inkraftsetzung dieser Regelungen würde den Datenschutz im Steuerbereich fördern.

13.3 Datenschutz in der Landesfinanzverwaltung

13.3.1 Ermittlung der Empfänger von Dorferneuerungsmitteln

Ein Finanzamt verlangte von der Kreisverwaltung eine namentliche und betragsmäßige objektbezogene Aufstellung über die in den vergangenen Jahren gezahlten Zuschüsse zur Förderung der Dorferneuerung aus Mitteln des kommunalen Steuerverbundes in einer bestimmten Gemeinde. Auf Wunsch der Kreisverwaltung hatte der LfD den Sachverhalt zu beurteilen. Er nahm wie folgt Stellung:

Seitens der Finanzverwaltung muß sich die Datenerhebung im Rahmen des Verhältnismäßigkeitsgrundsatzes halten. Diesem Grundsatz kommt bei Sammelauskunftsersuchen der vorliegenden Art besondere Bedeutung zu. Nach Auskunft des Finanzamtes stellte sich der steuerrechtliche Hintergrund der Anfrage wie folgt dar: Die gezahlten Landeszuschüsse sind dann steuerlich relevant, wenn die geförderten Aufwendungen durch die Förderungsempfänger als Erhaltungsaufwendungen steuermindernd geltend gemacht werden. Dann würden die Förderungsbeträge die Höhe des abzugsfähigen Erhaltungsaufwandes reduzieren. Da im Bereich der betroffenen Gemeinde dem Finanzamt nur ein Fall bekannt geworden ist, in dem ein Steuerpflichtiger selbst diesen Förderungsbetrag in Abzug gebracht hat, da andererseits aber in einer größeren Zahl von Fällen Förderleistungen ausgezahlt worden sind, besteht die nicht ganz fernliegende Vermutung, daß Bauherren es unterlassen haben, diese Förderung in ihrer Steuererklärung anzugeben.

In Anbetracht der Tatsache, daß sich das Auskunftsverlangen vorerst auf eine bestimmte Gemeinde beschränkte (eine Erweiterung auf den gesamten Landkreis würde nur in Betracht kommen, wenn sich die o. g. Vermutung für den Bereich dieser Gemeinde bestätigen würde), und angesichts der möglicherweise folgenden nicht unerheblichen steuerlichen Auswirkungen hielt der LfD das vorliegende Auskunftsverlangen für verhältnismäßig.

Die Erstbefragungspflicht des § 93 AO griff nicht ein: sie findet nur Anwendung, wenn feststeht, wer Steuerpflichtiger ist (BFH BStBl. 82, 141, 144). Außerdem dient diese Regelung unter dem Gesichtspunkt dem Schutz des Steuerpflichtigen, daß die befragte Stelle nicht ohne Notwendigkeit über steuerliche Verhältnisse des Betroffenen informiert werden soll, was sich häufig bei der Befragung nicht vermeiden läßt (Tipke/Kruse, Kommentar zur Abgabenordnung, 16. Auflage, § 93 AO Tz. 4). Auch dieser Zweck spielt bei der vorliegenden Fallgestaltung keine Rolle: die Kreisverwaltung erfährt anläßlich der Befragung über die steuerlichen Verhältnisse der Betroffenen nichts.

Aus der Sicht der Kreisverwaltung bestand im vorliegenden Zusammenhang in jedem Fall eine Übermittlungspflicht: Gemäß § 93 Abs. 1 AO haben öffentliche Stellen den Auskunftsersuchen der Finanzverwaltung Folge zu leisten. Gemäß § 14 Abs. 2 Satz 2 LDSG trägt die empfangende Stelle die Verantwortung für die Zulässigkeit der Übermittlung, wenn die Übermittlung auf ihr Ersuchen hin erfolgt. In diesem Fall prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben der empfangenden Stelle liegt, es sei denn, daß besonderer Anlaß zur Prüfung der Zulässigkeit der Übermittlung bestünde. In diesem Fall hätte die erhebende Stelle (vorliegend das Finanzamt) der um Übermittlung ersuchten Stelle (im vorliegenden Fall der Kreisverwaltung) die für ihre Prüfung erforderlichen Angaben mitzuteilen.

Diese Angaben waren erfolgt. Ergänzend wies der LfD schließlich auch auf § 116 AO (Anzeigepflicht für jede öffentliche Stelle bei einem Anhaltspunkt für Steuerhinterziehung) hin, dessen Rechtsgedanke ebenfalls zu berücksichtigen ist.

Im Ergebnis bestanden keine Bedenken gegen die Erfüllung des Auskunftsersuchens des Finanzamts durch die Kreisverwaltung.

13.3.2 Ermittlung der steuerlichen Verhältnisse noch nicht bekannter Vermieter

Eine Kreisverwaltung bat den LfD um die datenschutzrechtliche Beurteilung des folgenden Sachverhalts: Das für die Region zuständige Finanzamt hatte die Wohngeldstelle der Kreisverwaltung aufgefordert, dem Finanzamt alle Vermieter mitzuteilen, die der Wohngeldstelle bekanntgeworden waren.

Dabei handelte es sich um den Versuch, unbekannte Steuerfälle zu ermitteln. Dies ist nach Auffassung der Finanzverwaltung nicht nur eine Aufgabe der Steuerfahndung, § 208 Abs. 1 Nr. 3 AO, sondern auch der anderen Stellen innerhalb des Finanzamts (gem. §§ 85, 88, 92 AO, unter Berufung auf BFH BStBl. 88, 113).

Vor diesem Hintergrund beurteilte der LfD die Angelegenheit wie folgt: Sammelauskunftsersuchen der vorliegenden Art sind nur unter einschränkenden Voraussetzungen zulässig. Entscheidend kam es nach Auffassung des LfD darauf an, ob aufgrund der Erfahrungen der Praxis eine erhöhte Wahrscheinlichkeit dafür bestand, daß Vermieter von Wohnungen an Wohngeldempfänger entsprechende Mieteinnahmen nicht versteuern (vgl. Urteil des BFH, BStBl. 1987, S. 484; vgl. auch BFH in BStBl. 88, 359, 362).

Es müßten also genügend Anhaltspunkte dafür bestehen, daß die Gruppe der an Wohngeldempfänger vermietenden Personen im Vergleich zur Gruppe der nicht an Wohngeldempfänger vermietenden Vermieter in besonderem Maße dazu neigt, Mieteinnahmen steuerlich nicht zu erklären.

Das Finanzamt wies darauf hin, daß praktische Erfahrungen eindeutig belegten, daß Mieteinnahmen insbesondere von Eigentümern kleinerer Häuser (Einfamilienhäuser mit Einliegerwohnung, Zweifamilienhäuser) häufig steuerlich nicht erklärt werden. Daraus ergibt sich jedoch kein Hinweis dafür, daß gerade die Vermieter, die an Wohngeldempfänger vermieten, vorrangig zu solchen Eigentümern von Einfamilienhäusern mit Einliegerwohnung oder von Zweifamilienhäusern gehören. Sie dürften eher überproportional Mehrfamilienhäuser besitzen. Auch bestehen keinerlei Anhaltspunkte dafür, daß sie besonders nachlässig in der Erfüllung ihrer steuerlichen Erklärungspflichten wären. Es ist schließlich auch nicht erkennbar, daß die Mietverhältnisse bezüglich dieser Gruppe in irgendeiner Weise so geartet wären, daß eine erhöhte Wahrscheinlichkeit der Steuerverkürzung seitens der jeweiligen Vermieter entstehen würde.

Danach dürfte der entscheidende Grund, die Anschriften der Vermieter, die an Wohngeldempfänger vermieten, zu erfragen, darin bestehen, daß diese behördlich so erfaßt sind, daß die Daten relativ unkompliziert an das Finanzamt übermittelt werden können. Dies allerdings konnte der LfD allein nicht als rechtfertigenden Grund anerkennen, bei dieser Gruppe der Vermieter mit Ermittlungen zu beginnen.

Der LfD wies als alternative Erkenntnisquelle auf folgende Möglichkeit hin: Es könnte eine Auswertung aus dem Melderegister angefordert werden, in der alle diejenigen Anschriften aufgeführt sind, unter denen mindestens drei erwachsene Personen mit unterschiedlichen Namen wohnen. In diesen Fällen ist regelmäßig damit zu rechnen, daß ein Mietverhältnis vorliegt. Dann könnte ein Abgleich mit den Steuererklärungsakten der jeweiligen Hauseigentümer durchgeführt werden, und es könnten entsprechende Befragungen der Steuerpflichtigen erfolgen.

Aus datenschutzrechtlicher Sicht liegt der wesentliche Vorteil dieses Verfahrens zunächst darin, daß es nicht mit der Übermittlung und damit Offenbarung von Sozialdaten verbunden ist. Ein weiterer Vorteil dieser Ermittlungsmethode wäre, daß nicht nur diejenigen Vermieter erfaßt würden, die an Wohngeldempfänger vermieten, sondern daß Mietverhältnisse unabhängig von der wirtschaftlichen Leistungsfähigkeit der Mieter erfaßt werden könnten. Zu den Gründen, warum der Erstbefragungsgrundsatz des § 93 Abs. 1 AO hier keine Rolle spielt, s. o. Tz. 13.3.1.

Daraufhin hat das Finanzamt auf die begehrte Auskunft durch die Wohngeldstelle verzichtet.

13.3.3 Personenverwechslungen aufgrund eines automatisierten Abgleichverfahrens bei der ZDFin

Ein Beschwerdeführer trug folgenden Sachverhalt vor: In seinem Steuerbescheid seien von dem ihm zu erstattenden Betrag 742,– DM mit dem Hinweis „Ausgleich durch Verrechnung" abgezogen worden. Als Begründung sei auf dem Bescheid angeführt worden:

„Aufrechnung mit fälligen Beträgen Kraftfahrzeugsteuer vom 3. März 1997 zu Steuernummer" (es folgt die Nummer eines Kfz-Kennzeichens). Da er kein Fahrzeug mit diesem Kennzeichen besaß, habe er vom Finanzamt Aufklärung erbeten. Es stellte sich schließlich folgendes heraus:

Das EDV-System der ZDFin kontrolliert anhand des Namens und des jeweiligen Geburtsdatums, ob noch Forderungen bestehen, bevor ein auszuzahlender Betrag angewiesen wird. Da im Fall des Beschwerdeführers ein Steuerpflichtiger mit dem gleichen Namen und dem gleichen Geburtsdatum – allerdings mit einem völlig anderen Wohnort in Rheinland-Pfalz – seine Kfz-Steuer in Höhe von 742,– DM nicht bezahlt hatte, war es hier zur Aufrechnung gekommen.

Der LfD bat die ZDFin um Prüfung, ob nicht ergänzende Feststellungen zur Identität der jeweils betroffenen Personen möglich wären, um Verwechslungsfälle der vorliegenden Art auszuschließen. Hierzu wäre aus seiner Sicht etwa geeignet, alle Personendatensätze mit identischen Namens- und Geburtsdaten, die bei der ZDFin gespeichert sind, mit einem besonderen Merker zu versehen, so daß es bei dem automatischen Abgleich möglich wäre, vor einer Umbuchung zunächst eine gesonderte Prüfung anzustellen, ob diese auch im Einzelfall zulässig ist.

Die ZDFin nahm dazu wie folgt Stellung: Daß trotz des Übereinstimmens von Namen und Geburtsdatum zwei verschiedene Steuerbürger beteiligt gewesen seien, sei ein extremer Ausnahmefall gewesen. Zwischenzeitlich sei das zuständige Finanzamt angewiesen worden, im vorliegenden Fall maschinell Vorsorge zu treffen, daß in Zukunft eine derartige Umbuchung verhindert wird.

Angesichts der extremen Seltenheit der Fälle unterschiedlicher Steuerpflichtiger mit übereinstimmenden Namen, Vornamen und Geburtsdaten sei jedoch zu berücksichtigen, daß Verfahrensänderungen keinen unverhältnismäßigen Aufwand verursachen dürften.

Die Erörterungen in diesem Zusammenhang sind noch nicht abgeschlossen.

13.3.4 Befugnisse der Steuerfahndung gegenüber den Kunden von Kreditinstituten

Der LfD hatte die Frage zu beurteilen, ob es zulässig sei, wenn Mitarbeiter der Steuerfahndung systematisch Informationen auswerten, die sie anläßlich der Durchsuchung von Kreditinstituten erlangt haben, ohne daß diese Informationen eigentlicher Anlaß der Durchsuchung gewesen sind.

Aus datenschutzrechtlicher Sicht vertrat er folgende Auffassung:

Die Aufgaben und Kompetenzen der Steuerfahndung sind in § 208 AO geregelt. Danach ist Aufgabe der Steuerfahndung,

- Steuerstraftaten und Steuerordnungswidrigkeiten zu erforschen (§ 208 Abs. 1 Nr. 1),
- die Besteuerungsgrundlagen in den Fällen von Steuerstraftaten und Steuerordnungswidrigkeiten zu ermitteln (§ 208 Abs. 1 Nr. 2) sowie
- unbekannte Steuerfälle aufzudecken und zu ermitteln (§ 208 Abs. 1 Nr. 3).

Die vorliegende Tätigkeit kann nur nach § 208 Abs. 1 Nr. 3 AO zulässig sein, denn die Handlungen nach Abs. 1 Nr. 1 und 2 setzen einen konkreten Anfangsverdacht gegen eine bestimmte Person voraus. Daran fehlt es jedoch in den hier angesprochenen Fällen.

Im Rahmen der Erforschung unbekannter Steuerfälle darf die Steuerfahndung gegen noch unbekannte Personen in noch unbekannten Steuerfällen immer dann tätig werden und auch in Rechte einzelner eingreifen (etwa mit Hilfe eines Sammelauskunftsersuchens an Kreditinstitute), wenn aufgrund allgemeiner Erfahrung die Möglichkeit objektiver Steuerverkürzung besteht (BFHE 148, 108 = BStBl. 88, 359). So hat es der BFH für zulässig gehalten, daß die Steuerfahndung ein Ersuchen an eine Zeitung richtet, um Auskunft über Name und Adresse der Auftraggeber einzelner Chiffreanzeigen über den Verkauf ausländischer Immobilien von beträchtlichem Wert zu erhalten. Das Bundesverfassungsgericht hat dieses Urteil des BFH bestätigt (BVerfG HFR 89, 440).

Der BFH hat auch zugelassen, daß die Steuerfahndung an ein Kreditinstitut ein Sammelersuchen um Auskunft über die Provisionszahlungen an alle in einer bestimmten Zeit für das Kreditinstitut tätig gewordenen Kreditvermittler gerichtet hat. Voraussetzung war allerdings, daß nach allgemeiner Erfahrung verhältnismäßig viele Kreditvermittler ihre Provisionen nicht versteuern und die Ausführung des Ersuchens keine unverhältnismäßige, unzumutbare Belastung für das Kreditinstitut bedeutet hat (BFH BStBl. 87, 484).

Das Finanzgericht Hamburg hat die allgemeine Erfahrung genügen lassen, daß Zahnärzte, die Goldgeschäfte mit Scheideanstalten machen, die Einkünfte daraus selten versteuert haben (EFG 87, 9, 10). Der BFH hat weiter entschieden, daß die Steuerfahndung aufgrund der Erfahrung, wonach kostspielige Segel- und Motorjachten oft steuerrechtlich nicht erfaßt würden, berechtigt sei, die in den Verkauf von Jachten eingeschalteten Makler zur Angabe von Namen und Anschriften von Jachteignern aufzufordern (BFH/NV 92, 791, 792). Allerdings sind nach der BFH-Rechtsprechung Fahndungsmaßnahmen ins Blaue hinein, auch Rasterfahndungen, unzulässig (BFH BStBl. 88, 359, 362; BStBl. 90, 198; 90, 1010; 91, 277). Diese Auffassung wird in der Literatur (insbesondere Tipke/Kruse, Anmerkung 5 f zu § 208) im wesentlichen unterstützt. Danach sind konkrete Anhaltspunkte im Einzelfall nicht erforderlich, damit die Steuerfahndung tätig werden kann. Sammelauskünfte können im Rahmen des Verhältnismäßigen grundsätzlich erforderliche, geeignete Kontrollmittel sein. Dabei sei nicht erforderlich, daß mit jedem von der Sammelauskunft betroffenen Fall als einem Steuerfall gerechnet werden könne. Es genüge, daß nach allgemeiner Steuerverkürzungserfahrung bestimmte Sachverhalte besonders verkürzungsträchtig oder kontrollbedürftig seien. Im Ergebnis ist so wohl auch das Zinsbesteuerungsurteil des Bundesverfassungsgerichts (BStBl. 91, 654, 664 ff.) zu verstehen. Zusammengefaßt reicht also ein generelles, auf Verwaltungserfahrung gegründetes Kontrollbedürfnis für Eingriffsmaßnahmen der Steuerfahndung aus.

Für das Verhältnis der Finanzverwaltung zu Banken enthält die Abgabenordnung seit dem 3. August 1988 in § 30 a eine besondere Regelung (durch die der sog. „Bankenerlaß" in eine gesetzliche Regelung umgewandelt wurde). Danach haben die Finanzbehörden bei der Ermittlung des Sachverhalts auf das Vertrauensverhältnis zwischen den Kreditinstituten und deren Kunden besonders Rücksicht zu nehmen. Für die Ausschreibung von Kontrollmitteilungen anläßlich von Außenprüfungen gelten besondere Beschränkungen (§ 30 a Abs. 3 AO). Diese sind unmittelbar von der Steuerfahndung zwar nicht zu beachten, da es sich nur um eine Regelung des Steuerermittlungsverfahrens, nicht des Steuerstrafverfahrens handelt. Soweit die Steuerfahndung aber im Rahmen der Steuerermittlung handelt (und dies tut sie in den Fällen des § 208 Abs. 1 Nr. 3 im Regelfall), ist sie zumindest analog anwendbar. Die „allgemeine Überwachung" zur Aufdeckung und Ermittlung unbekannter Steuerfälle soll verhindert werden (so unter Bezug auf § 208 Abs. 1 Nr. 3 AO ausdrücklich Tipke/Kruse, Anm. 5 zu § 30 a AO).

Für die Ausgangssituation sind danach zwei Fallgruppen zu unterscheiden:

a) Die Zufallsfunde betreffen Sachverhalte, die für sich genommen ein Sammelauskunftsersuchen gerechtfertigt hätten. Dann ist die Verwendung und Auswertung dieser Zufallsfunde durch die Steuerfahndung zulässig.

b) Die Zufallsfunde betreffen solche Sachverhalte nicht, sie sind vielmehr bloßes „Kontrollmaterial" wie die im Finanzbereich nach der KontrollmitteilungsVO (i. V. m. § 93 a AO) anfallenden Kontrollmitteilungen, die aus sich heraus nicht als besonders untersuchungswürdig anzusehen sind, bei denen das oben genannte Kriterium des „auf Verwaltungserfahrung gegründeten besonderen Kontrollbedürfnisses" nicht vorliegt. Dann wäre die Auswertung der Materialien (der Zufallsfunde) mit einer „Rasterfahndungsmaßnahme" bzw. einer Fahndung „ins Blaue hinein" zu vergleichen, sie wäre eine Maßnahme zur allgemeinen Überwachung, die von § 30 a Abs. 2 AO ausdrücklich ausgeschlossen ist. Sie wäre damit unzulässig.

Allein die Tatsache, daß die Steuerfahndung Zufallserkenntnisse gewonnen hat, kann also aus der Sicht des LfD nicht Anlaß dafür sein, diese Erkenntnisse zu weitergehenden steuerrechtlichen Prüfmaßnahmen zu verwenden.

13.3.5 Versand von Lohnsteuerkarten unter Nutzung des ePost-Dienstes

Eine Gemeinde wandte sich an den LfD mit der Bitte um Beurteilung, ob sie insbesondere für den Druck und den Versand von Lohnsteuerkarten den ePost-Dienst der Deutschen Post AG nutzen dürfe.

Zunächst war festzustellen, daß die auf der Lohnsteuerkarte angegebenen Daten dem Steuergeheimnis i. S. v. § 30 Abs. 1 AO unterliegen.

In Übereinstimmung mit den Referatsleitern für Abgabenordnung der Finanzministerien des Bundes und der Länder vertritt der LfD die Auffassung, daß diese Regelung die Amtsträger verpflichtet, das Steuergeheimnis zu wahren. Daraus folgt, daß die Finanzverwaltung (wozu auch die Lohnsteuerkartenstellen gehören) die Wahrung des Steuergeheimnisses nicht nur in rechtlicher, sondern auch in faktischer Hinsicht sicherstellen muß. Dies ist bei dem ePost-Verfahren der Deutschen Post AG nicht gewährleistet. Die Finanzverwaltung verliert die Herrschaft über die von ihr gelieferten Daten. Sie kann nicht kontrollieren, ob die im ePost-Dienst eingesetzten Personen die von der Finanzverwaltung gelieferten Daten tatsächlich nicht unbefugt speichern. Mit dem Einsatz des ePost-Dienstes wird zudem die Möglichkeit geschaffen, die Steuerdaten aller bisher nur dezentral erfaßter Bürger zentral bei einem einzigen Unternehmen außerhalb der Finanzverwaltung zu speichern. Schließlich muß aufgrund der wettbewerbsrechtlichen Situation in Europa damit gerechnet werden, daß bei einem Einsatz des ePost-Dienstverfahrens der Deutschen Post AG entsprechende Aufträge auch an andere Telekommunikationsunternehmen, die nicht mehr der Kontrolle durch deutsche Behörden und Gerichte unterlägen, vergeben werden müßten.

Die Referatsleiter für Abgabenordnung sprachen sich deshalb einstimmig gegen die Nutzung des ePost-Verfahrens der Deutschen Post AG durch die Finanzverwaltung aus. Aus den gleichen Gründen hat der LfD von einer Nutzung des ePost-Verfahrens für den Druck und die Zustellung von Lohnsteuerkarten abgeraten. Die Gemeinde ist diesem Rat gefolgt.

13.3.6 Zugriff der Finanzämter auf Melderegisterdaten

Das Finanzministerium bat um Stellungnahme zu dem Vorhaben, auf der Grundlage von § 11 MeldDÜVO allen Finanzämtern landesweit einen Zugriff auf die Meldedaten zu eröffnen. Der LfD hat daraufhin dem Ministerium mitgeteilt, er sei bei der Novellierung der Meldedaten-Übermittlungsverordnung davon ausgegangen, daß § 11 für die Finanzämter keine landesweite Abfragemöglichkeit eröffne. Nach der Novellierung des LDSG halte er jedoch derartige Abfragemöglichkeiten für zulässig, sofern die Voraussetzungen des neu geschaffenen § 7 LDSG (automatisiertes Übermittlungsverfahren) vorliegen. Der LfD bezweifelt nicht, daß die Voraussetzungen für einen Zugriff auf Meldedaten z. B. für bestimmte sachbearbeitende Personen in Vollstreckungsstellen gegeben sind.

Von dieser Einschätzung ausgehend haben Erörterungen mit dem begrüßenswerten Ergebnis stattgefunden, daß eine umfassende landesweite Zugriffsmöglichkeit nicht mehr gefordert wird. Vielmehr soll bei den 24 Finanzämtern ohne zentralisierte Zuständigkeiten die Zugriffsmöglichkeit auf Meldedaten aus dem jeweiligen Zuständigkeitsbereich (Landkreis) eines Finanzamtes beschränkt werden; für die übrigen Finanzämter mit kreisübergreifenden Zuständigkeiten soll zunächst geprüft werden, ob die Zugriffsberechtigung auf Meldedaten des übergeordneten Regierungsbezirks beschränkt werden kann. Falls dies nicht möglich sein sollte, hält es der LfD nach Abwägung zwischen der angestrebten Arbeitserleichterung und der möglichen Beeinträchtigung der schutzwürdigen Belange von Betroffenen aus datenschutzrechtlicher Sicht für vertretbar, daß für die Übergangszeit bis zur Realisierung eines neuen Einwohnerinformationssystems (EWOIS) diesen Finanzämtern eine landesweite Zugriffsmöglichkeit auf Meldedaten eingeräumt wird.

13.4 Datenschutz bei der gemeindlichen Abgabenerhebung

13.4.1 Berücksichtigung des Datenschutzes bei der Erhebung des „Fremdenverkehrsbeitrags A"

Zwei Ärzte, die in einem Badeort des Landes praktizieren, trugen dem LfD die Auffassung vor, die Erhebung des Gesamtumsatzes ihrer Praxis durch die Verbandsgemeindeverwaltung zum Zweck der Festsetzung des Fremdenverkehrsbeitrages sei unzulässig, da eine entsprechende Regelung in der gemeindlichen Satzung gegen höherrangiges Recht (das Steuergeheimnis) verstoße und unverhältnismäßig sei.

Die Gemeinde hatte eine gültige Satzung über die Erhebung eines Fremdenverkehrsbeitrages erlassen. In dieser ist bestimmt, daß der Beitragsschuldner eine schriftliche Erklärung über den Jahresumsatz im Sinne des Umsatzsteuergesetzes abzugeben hat.

Aus datenschutzrechtlicher Sicht hat der LfD den Sachverhalt wie folgt beurteilt:

Die o. g. Regelung begründet zwar einen beachtlichen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen und führt dazu, daß Daten, die beim Finanzamt dem Steuergeheimnis unterliegen, der Verbandsgemeindeverwaltung preisgegeben werden müssen. Dennoch ist diese Regelung auch aus datenschutzrechtlicher Sicht wirksam. Denn es liegt im Rahmen des Satzungsermessens der Gemeinden, die Erhebung des Fremdenverkehrsbeitrages auf der Grundlage des Gesamtumsatzes zu regeln. Auch das entsprechende Verfahren ist grundsätzlich zulässig. Entsprechend hat die obergerichtliche Rechtsprechung in der Vergangenheit wiederholt entschieden (z. B. OVG Koblenz, Urteil v. 22. September 1981, DÖV 82, 648; OVG Lüneburg, Urteil vom 13. November 1990, NVwZ-RR 92, 40).

Auch wenn es das informationelle Selbstbestimmungsrecht der Bürger schonendere Verfahren geben mag, um Fremdenverkehrsbeiträge festzusetzen, so ist bei der Abwägung zwischen Effektivität eines Verfahrens und Bürgerrechten dem Satzungsgeber ein breiter Spielraum der Beurteilung eingeräumt. Dieser Spielraum wurde vorliegend nicht überschritten. In Rheinland-Pfalz beruht die weit überwiegende Zahl der Fremdenverkehrsbeitragssatzungen auf diesem Modell.

Abschließend war zu betonen, daß die entsprechenden Daten bei der Verbandsgemeindeverwaltung dem Steuergeheimnis unterliegen und die Bediensteten, die diese Informationen zur Kenntnis erhalten, auch der Strafandrohung des § 355 StGB im Falle des Bruchs des Steuergeheimnisses unterworfen sind.

Vor diesem Hintergrund wiederholt der LfD allerdings seine Auffassung, daß die Berechnung und Festsetzung des Fremdenverkehrsbeitrages grundsätzlich ein Geschäft der laufenden Verwaltung der Gemeinden ist und insofern der Gemeinderat oder einer seiner Ausschüsse nicht regelmäßig die Umsatzlisten der Abgabenschuldner erhalten darf.

13.4.2 Weitergabe von Namen und Adressen der Steuerpflichtigen der „Grundsteuer A" an eine Jagdgenossenschaft

Eine Verbandsgemeinde fragte an, ob sie befugt sei, der in ihrem Bezirk gebildeten Jagdgenossenschaft eine Liste der Grundsteuerpflichtigen zu überlassen. Der LfD beurteilte den Sachverhalt wie folgt:

Die Jagdgenossenschaft ist befugt, eine Liste der Grundstückseigentümer des Bereiches zu erheben, der zur Jagdgenossenschaft gehört. Da die entsprechende Liste der Steuerpflichtigen zur „Grundsteuer A" die jeweils aktuellsten Namen und Anschriften der Grundstückseigentümer enthalten dürfte, ist sie auch zur Erhebung einer solchen Liste der Grundsteuerpflichtigen befugt (§ 12 Abs. 1 i. V. m. Abs. 4 Nr. 6 und Nr. 8 LDSG).

Dieser Erhebungsbefugnis entspricht eine Übermittlungsbefugnis des Steueramtes der Verbandsgemeinde. Sie ergibt sich aus § 31 Abs. 3 AO. Danach sind die für die Verwaltung der Grundsteuer zuständigen Behörden berechtigt, die nach § 30 AO geschützten Namen und Anschriften von Grundstückseigentümern, die bei der Verwaltung der Grundsteuer bekanntgeworden sind, zur Verwaltung anderer Abgaben sowie zur Erfüllung sonstiger öffentlicher Aufgaben zu verwenden oder den hierfür zuständigen juristischen Personen des öffentlichen Rechts auf Ersuchen mitzuteilen, soweit nicht überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen.

Solche überwiegend schutzwürdigen Interessen der jeweiligen Betroffenen waren im vorliegenden Zusammenhang nicht ersichtlich.

13.4.3 Gewerbesteuer: Beteiligung der Ortsgemeinden und Ortsbürgermeister

Eine Verbandsgemeinde trug dem LfD folgenden Sachverhalt mit der Bitte um Beurteilung vor:

Im Rahmen der Prüfung der ordnungsgemäßen Erhebung und Festsetzung von Abgaben verlange der Rechnungsprüfungsausschuß der Ortsgemeinde umfassend Einsichtnahme in die entsprechenden Gewerbesteuerakten; in diesem Zusammenhang fordere der Rechnungsprüfungsausschuß vom Ortsbürgermeister weitere Auskünfte an. Gemäß § 110 Abs. 3 GemO sei der Ortsbürgermeister auch verpflichtet, entsprechende Auskünfte zu erteilen. Daraus könne sich ein Anspruch der Ortsbürgermeister ergeben, umfassend über Einzelheiten der Abgabenerhebung informiert zu werden, um ihrerseits den Rechnungsprüfungsausschuß unterrichten zu können.

Der LfD hat hierzu wie folgt Stellung genommen:

a) Die Eigenschaft der Ortsgemeinde als Steuergläubigerin kann in gewissem Umfang die Wahrnehmung von Aufsichts- und Kontrollbefugnissen sowohl durch den Rechnungsprüfungsausschuß wie durch den Ortsbürgermeister und in bestimmten Fällen – wozu Niederschlagung und Erlaß gehören können – auch die Mitwirkung an Einzelfallentscheidungen rechtfertigen. Die Ausübung von Kontroll- und Aufsichtsbefugnissen hat sich an den Prinzipien dieser Rechstinstitute zu orientieren, wozu das Stichprobenprinzip und die Orientierung an sachangemessenen Schranken gehören. Auch der Umfang der damit einhergehenden Datenübermittlungen hat sich im Rahmen des Verhältnismäßigen (insbesondere also des zu Aufsichtszwecken Erforderlichen) zu halten. Rechnungsprüfungsausschuß und Ortsbürgermeister als Datenempfänger sind ihrerseits beim Umgang mit diesen Daten an das Steuergeheimnis gebunden und machen sich bei einer Verletzung gem. § 355 StGB strafbar.

Die Bediensteten in den Steuerämtern der Verbandsgemeinden unterliegen dem Steuergeheimnis nach § 30 AO; für die durch Landes- oder Bundesrecht festgelegten Steuern ergibt sich dies unmittelbar aus dieser Vorschrift; für kommunale Abgaben folgt dies aus der Verweisung in § 3 Abs. 1 Nr. 1 KAG. Das Steuergeheimnis gilt auch gegenüber anderen Amtsträgern der gleichen Funktionseinheit. Eine Offenbarung von Daten, die dem Steuergeheimnis unterliegen, ist danach nur zulässig, wenn sie einem Verwaltungsverfahren in Steuersachen dient oder wenn ein zwingendes öffentliches Interesse an der Offenbarung besteht (§ 30 Abs. 4 Nrn. 1 und 5 AO).

Daraus ergibt sich, daß zu Rechnungsprüfungszwecken von den Bediensteten der Verbandsgemeinde, die die Steuerangelegenheiten bearbeiten, an die prüfende Stelle Auskünfte im verhältnismäßigen Umfang zu erteilen sind. Dazu gehört auch die Vorlage der Akten der zu prüfenden Fälle. Da der Ortsbürgermeister als Teil der prüfenden Funktionseinheit der Ortsgemeinde anzusehen ist, können die entsprechenden Daten zunächst an ihn als Organ der Steuergläubigerin weitergeleitet werden, um sie dann an den Rechnungsprüfungsausschuß zu übermitteln, wenn der Verwaltungsvollzug insofern seine Beteiligung erforderlich macht. Nach Möglichkeit sollten Übermittlungen allerdings unmittelbar erfolgen.

b) Eine Befugnis, in diesem Zusammenhang an den Rat Daten zu übermitteln, setzt jeweils voraus, daß die konkrete Aufgabenerfüllung dieses Gemeindeorgans im Zusammenhang mit der Steuerfestsetzung und -erhebung die Offenbarung der in Rede stehenden Daten erfordert (§ 30 Abs. 4 Nr. 1 AO). Der Rat ist also in diese Aufsichts- und Kontrolltätigkeit nur dann einzubeziehen, wenn dies aufgrund seiner kommunalverfassungsrechtlichen Kompetenzen gerechtfertigt ist.

Unzulässig ist und bleibt es danach allerdings beispielsweise, Listen der Steuerzahlungen von Gewerbetreibenden zu allgemeinen kommunalpolitischen Zwecken zu erstellen und entsprechend zu nutzen.

13.4.4 Datenerhebung eines Eigenbetriebs Wasser- und Abwasserwerk zu Planungs- und Veranlagungszwecken

Aufgrund einer Eingabe ist dem LfD folgender Sachverhalt bekannt geworden:

Der Eigenbetrieb Wasser- und Abwasserwerk einer Verbandsgemeinde hat alle Grundstückseigentümer der Verbandsgemeinde unter Beifügung eines Fragebogens angeschrieben, um folgende Flächendaten zu erheben:

- Gebäudeflächen (einschließlich Garagen und Nebenanlagen)
- sonstige befestigte und angeschlossene Flächen.

Die Gesamtfläche der jeweiligen Grundstücke war bereits auf der Basis der der Verbandsgemeinde zur Verfügung stehenden Zweitkataster in die jeweiligen Fragebogen eingedruckt.

Aus datenschutzrechtlicher Sicht hat der LfD diese Datenerhebung wie folgt beurteilt:

Angesichts der Tatsache, daß die Abgabensatzung, nach der die erhobenen Daten Grundlage der Beitragsberechnung sein sollten, noch nicht erlassen worden war, sondern sich erst im Planungsstadium befunden hat, konnte eine Datenerhebung noch nicht auf diese künftige Rechtsgrundlage gestützt werden. Weder die §§ 85 ff. AO noch § 12 Abs. 1 LDSG rechtfertigen eine solche im Vorgriff auf eine zu erwartende Rechtsgrundlage erfolgende Datenerhebung und Speicherung.

Die Absicht, Informationsgrundlagen für die künftige Gestaltung der Abwasserabgabensatzung zu gewinnen, begründet den Planungszweck für die hier erhobenen Daten. Als Rechtsgrundlage für diese Datenerhebung und die anschließende Datennutzung kommt damit allein § 32 LDSG in Betracht, wonach für Zwecke der öffentlichen Planung personenbezogene Daten verarbeitet (und damit erhoben und genutzt) werden dürfen. Planungsdaten dürfen dann erhoben werden, wenn dafür ein besonderes öffentliches Interesse besteht, der Planungszweck auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann und überwiegende schutzwürdige Interessen der Betroffenen nicht entgegenstehen. Diese Voraussetzungen waren im vorliegenden Zusammenhang erfüllt.

Rechtsfolge ist zunächst, daß die Verbandsgemeindeverwaltung grundsätzlich die betroffenen Grundstückseigentümer auch mit dem hier in Rede stehenden Inhalt befragen durfte. Bei der Datenerhebung war allerdings § 12 Abs. 2 LDSG ergänzend heranzuziehen. Danach sind die betroffenen Bürger, da keine Auskunftspflicht bestanden hat (und § 32 LDSG auch keine solche Pflicht begründet), auf die Freiwilligkeit der Datenpreisgabe hinzuweisen.

Nach § 32 Abs. 2 LDSG durften die Daten zudem nur zu Planungszwecken verwendet, also nicht für die abgabenrechtliche Veranlagung der Betroffenen herangezogen werden. Nach Abschluß der Planung, also nach Erstellung einer entsprechenden abgabenrechtlichen Rechtsgrundlage (Satzung), mußten sie gelöscht werden.

Allerdings wäre auf der Basis der Freiwilligkeit auch eine Nutzung der Daten zu künftigen Abgabenzwecken zulässig gewesen. Dann hätte allerdings der Erhebungsbogen entsprechend ausgestaltet sein müssen. Die Verbandsgemeinde wurde hierauf hingewiesen.

14. Wirtschaft und Verkehr

14.1 Überprüfung der persönlichen Zuverlässigkeit bei der Beschäftigung von Wachpersonen

Wer das Bewachungsgewerbe betreibt, darf nur Personen beschäftigen, welche die für den Gewerbebetrieb erforderliche Zuverlässigkeit besitzen; andernfalls läuft der Bewachungsgewerbetreibende Gefahr, seine Erlaubnis zu verlieren (§ 34 a Abs. 1 Satz 4

i. V. m. Satz 3 Nr. 1 GewO). Er hat somit ein rechtliches Interesse daran, über eine gegebenenfalls vorliegende mangelnde Zuverlässigkeit und Ungeeignetheit der einzustellenden Personen Kenntnis zu erlangen. Dem stehen die Interessen der einzustellenden Person gegenüber.

Im Rahmen einer Anfrage des Gemeinde- und Städtebundes Rheinland-Pfalz hat der LfD dazu folgende Auffassung vertreten: Die Anzeige nach § 5 BewachVO dient einem doppelten Zweck. Zum einen versetzt sie die Erlaubnisbehörde in die Lage zu prüfen, ob die für den Gewerbebetrieb erforderliche Zuverlässigkeit i. S. d. § 34 a GewO weiterhin besteht, zum anderen soll sie gewährleisten, daß der Gewerbetreibende nur geeignete und zuverlässige Personen beschäftigt. Nach § 11 Abs. 1 GewO darf die zuständige öffentliche Stelle personenbezogene Daten nicht nur des Gewerbetreibenden selbst, sondern auch solcher Personen, auf die es für die Entscheidung ankommt – also beispielsweise der einzustellenden Wachperson –, erheben, soweit die Daten zur Beurteilung u. a. der Zuverlässigkeit bei der Durchführung gewerberechtlicher Vorschriften und Verfahren erforderlich sind.

Was die Überprüfung der Zuverlässigkeit der für die Beschäftigung als Wachmann in Aussicht genommenen Person anbelangt, ist hier auch die Datenerhebung (der anfragenden Behörde) bei Dritten gem. § 11 Abs. 2 Nr. 1 GewO zulässig. § 11 ist durch das Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften zur Regelung insbesondere solcher Fälle, in denen zur Beurteilung der gewerberechtlichen Zuverlässigkeit Daten erhoben werden müssen, in die Gewerbeordnung eingefügt worden. Des weiteren bleibt gem. § 11 Abs. 3 GewO die Einholung von Auskünften u. a. nach § 915 ZPO unberührt, und § 11 Abs. 4 GewO bestimmt, daß die nach den Absätzen 1 und 3 erhobenen Daten für Zwecke des Absatzes 1, also auch zur Beurteilung der Zuverlässigkeit von mit der Durchführung von Bewachungsaufgaben beschäftigten Personen, gespeichert oder genutzt werden dürfen.

Zur Übermittlungsbefugnis der befragten Behörde ist in der Gewerbeordnung eine bereichsspezifische Regelung nicht vorhanden. In Betracht kommt also die Anwendung des § 14 LDSG. Danach ist die Übermittlung personenbezogener Daten an öffentliche Stelle u. a. zulässig, wenn dies für Aufgaben des Empfängers erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 12 Abs. 4 LDSG zulassen würden. Die Notwendigkeit einer entsprechenden Datenübermittlung kann sich z. B. ergeben, wenn dies zur „Abwehr erheblicher Nachteile für das Gemeinwohl" erforderlich ist (§ 12 Abs. 4 Nr. 4 LDSG). Die zuständigen Stellen haben die durch § 34 a GewO begründeten gesetzlichen Aufgaben in erster Linie zum Schutz der Allgemeinheit wahrzunehmen, so daß unter diesem Gesichtspunkt eine Datenübermittlung zulässig sein könnte. Darüber hinaus sind nach Auffasung des LfD die zuständigen öffentlichen Stellen nach § 28 VwVfG stets verpflichtet, die Betroffenen anzuhören. Die Erfüllung des verfassungsrechtlichen Gebots der Gewährung rechtlichen Gehörs sollte als Mindestvoraussetzung für die zur Ausübung der informationellen Selbstbestimmung erforderliche Transparenz der Datenverarbeitung für den Betroffenen angesehen werden. Dieser kann dann etwa unzutreffende Erkenntnisse richtigstellen und somit auf eine Überprüfung der Auskunft hinwirken.

14.2 Der geplante Erlaß einer Verwaltungsvorschrift zur Durchführung des Aufstiegsfortbildungsförderungsgesetzes (sog. „Meister-BAföG")

Das Aufstiegsfortbildungsförderungsgesetz sieht eine Gewährung von Förderleistungen für Teilnehmerinnen und Teilnehmer beruflicher Aufstiegsfortbildung vor. Anträge auf Gewährung von Leistungen nach diesem Gesetz sind nach der hierzu erlassenen Landesverordnung vom 18. Juli 1996 (GVBl. 1996, S. 273) bei den zuständigen Ämtern für Ausbildungsförderung zu stellen.

Bei der Bezirksregierung Koblenz ist eine sogenannte Verbindungsstelle als verwaltungsinterne Vermittlungsstelle zwischen den Ämtern für Ausbildungsförderung und dem Rechenzentrum bei der Zentralen Daten- und Finanzverwaltung eingerichtet. Der Entwurf der Verwaltungsvorschrift zur Durchführung des Aufstiegsfortbildungsförderungsgesetzes sah u. a. folgende Aufgaben für diese Verbindungsstelle vor:

Entgegennahme der von den Ämtern für Ausbildungsförderung übersandten Daten; Weiterleitung der Daten nach Registrierung an das Rechenzentrum bei der Zentralen Daten- und Finanzverwaltung; Entgegennahme der vom Rechenzentrum der Zentralen Daten- und Finanzverwaltung erarbeiteten Bescheide, Zahlungsunterlagen und der verarbeiteten Daten mit Fehlerlisten; Übersendung der maschinell erstellten Bescheide, Bescheinigungen und der Zahlungslisten an die Ämter für Ausbildungsförderung; Übersendung der verarbeiteten Daten mit den Fehlerlisten an die Ämter für Ausbildungsförderung; darüber hinaus Erteilung der Kassenanordnungen an die Bundes- und Oberfinanzkasse sowie Erteilung der Annahmeanordnungen an die Oberfinanzkasse Koblenz aufgrund der maschinell erstellten Listen über die Rückforderungsbeträge.

Das Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau hat den LfD um Überprüfung unter datenschutzrechtlichen Gesichtspunkten gebeten.

Da im Antrag auf Förderung einer beruflichen Aufstiegsfortbildung eine Reihe sensibler personenbezogener Daten zu offenbaren sind, z. B. umfassende Angaben zum Einkommen und Vermögen sowie zu Schulden und Lasten, hat eine örtliche Fest-

stellung bei der Bezirksregierung Koblenz (Verbindungsstelle) stattgefunden. So werden dort vor Weiterleitung an das Rechenzentrum der Zentralen Daten- und Finanzverwaltung die von den Ämtern für Ausbildungsförderung übersandten Disketten mit den sensiblen Antragsdaten entgegengenommen und registriert.

Klärungsbedarf bestand insbesondere im Hinblick auf die in Ziffer 1.4 der Verwaltungsvorschrift vorgesehene Ausgestaltung der Verbindungsstelle als Vermittlungsstelle zwischen den Ämtern für Ausbildungsförderung und dem Rechenzentrum bei der Zentralen Daten- und Finanzverwaltung.

Zusammenfassend war festzustellen, daß die bei der Bezirksregierung eingerichtete Verbindungsstelle teilweise – lediglich – als technischer Erfüllungsgehilfe („Briefträger") agiert, andererseits aber auch als anordnende Stelle auftritt, nämlich die Kassen- und Annahmeanordnungen an die Bundes- und die Oberfinanzkasse erteilt. Hier liegt also eine Funktionsübertragung vor, für die es indessen keine spezielle Regelung auf Gesetzes- oder Verordnungsebene gibt, die bestimmt, daß eine Verbindungsstelle diese Aufgaben wahrzunehmen hat. Vielmehr ist in § 1 Abs. 1 der eingangs erwähnten Landesverordnung geregelt, daß zuständige Behörden zur Durchführung des Aufstiegsfortbildungsförderungsgesetzes die in den Kreisverwaltungen und den Stadtverwaltungen der kreisfreien Städte bestehenden Ämter für Ausbildungsförderung sind.

Auf diese Problemlage hat der LfD das zuständige Ministerium hingewiesen und um Stellungnahme gebeten. Zwischenzeitlich war die Verwaltungsvorschrift zur Durchführung des Aufstiegsfortbildungsförderungsgesetzes auch Thema in einer Sitzung der „Arbeitsgruppe Verwaltungsvorschriften und Standards". Es wurde festgestellt, daß „weder durch eine Verwaltungsvorschrift noch durch ein Rundschreiben die gegenwärtigen Mängel der Landesverordnung über die Zuständigkeit nach dem AFBG beseitigt werden können. Dieser Mangel besteht darin, daß die tatsächlichen Zuständigkeiten von den Regelungen in der Zuständigkeitsverordnung abweichen. Durch eine Änderung der Zuständigkeitsverordnung muß der Bezirksregierung, die z. Z. einen wesentlichen Beitrag zum Vollzug des AFBG leistet, eine Zuständigkeit eingeräumt werden." Damit sind die Bedenken des LfD ausgeräumt.

14.3 Untersagungsverfügung nach dem Gaststättengesetz

Eine Verbandsgemeindeverwaltung hat den LfD vor Zustellung der Verfügung, in der das Verbot zur Weiterbeschäftigung des Prokuristen einer Diskothek ausgesprochen wurde, um Stellungnahme hinsichtlich der vorgesehenen ausführlichen Darstellung der „kriminellen Karriere" des Betroffenen gegenüber der Betreibergesellschaft der Diskothek gebeten.

Nach § 31 Gaststättengesetz finden – mangels besonderer Bestimmungen zum Umgang mit personenbezogenen Daten in diesem Gesetz – die Regelungen der Gewerbeordnung Anwendung. Im vorliegenden Fall war § 11 GewO zu beachten. Nach § 11 Abs. 1 GewO darf die zuständige öffentliche Stelle personenbezogene Daten nicht nur des Gewerbetreibenden selbst, sondern auch solcher Personen, auf die es für die Entscheidung ankommt, erheben, soweit die Daten zur Beurteilung u. a. der Zuverlässigkeit erforderlich sind. Beispielhaft für solche Daten, die hier erforderlich sein können, nennt § 11 Abs. 1 Satz 2 Nr. 1 GewO abgeschlossene oder sonst anhängige Straf- oder Bußgeldverfahren. § 11 Abs. 4 GewO bestimmt, daß die nach den Absätzen 1 und 3 erhobenen Daten nur für Zwecke des Abs. 1, also u. a. zur Beurteilung der Zuverlässigkeit, gespeichert oder genutzt werden dürfen. Davon zu unterscheiden ist die weitere Rechtsfrage, was an eine nichtöffentliche Stelle übermittelt werden darf. Die Problematik liegt im vorliegenden Fall darin, daß § 11 Abs. 5 GewO als einschlägige Bestimmung nur die Datenübermittlung an öffentliche Stellen zuläßt. Damit wäre die Übermittlung an die Geschäftsführerin der Betreibergesellschaft der Diskothek unzulässig gewesen. Dies war jedoch nur als ein Zwischenergebnis anzusehen. Wenn nämlich die Daten aus dem polizeilichen Führungszeugnis für die Entscheidung in dem Verwaltungsverfahren genutzt werden dürfen, dann sollten sie im Laufe des Verfahrens grundsätzlich auch gegenüber der Geschäftsführerin der Betreibergesellschaft als Adressatin des Verwaltungsakts offengelegt werden.

Hier kommt als Rechtsgrundlage für die Datenübermittlung aus Sicht des LfD § 39 Abs. 1 VwVfG in Betracht. Nach dieser Vorschrift muß die Begründung eines Verwaltungsaktes erkennen lassen, von welchen tatsächlichen und rechtlichen Voraussetzungen und Überlegungen die Behörde bei ihrer Entscheidung ausgegangen ist. Die Betroffenen müssen die für ihren konkreten Fall für die Behörde maßgeblichen Gründe erfahren, da die Begründungspflicht ein wesentliches Erfordernis des rechtsstaatlichen Verfahrens ist. Zugleich sind aber auch die mit einer Datenübermittlung verbundenen Informationseingriffe so gering wie möglich zu halten. Nach Auffassung des LfD war es im vorliegenden Fall angemessen, das Beschäftigungsverbot damit zu begründen, daß die über den Prokuristen eingeholte Auskunft Eintragungen enthält, die dessen persönliche Zuverlässigkeit in Frage stellen. Rechtliche Bedenken hatte der LfD hinsichtlich der vorgesehenen detaillierten Hinweise, z. B. auf die Art der begangenen Delikte.

14.4 Übermittlung von Firmendaten der Industrie- und Handelskammer an eine Kreisverwaltung

Im Zusammenhang mit dem Förderprogramm der Landesregierung „Arbeit statt Sozialhilfe" wurde seitens einer IHK die Frage an den LfD herangetragen, ob es zulässig sei, zwecks zu verbessernder Vermittlung von Sozialhilfeempfängern auch Firmendaten an eine beteiligte Kreisverwaltung zu übermitteln.

Die IHK ist als Körperschaft des öffentlichen Rechts eine öffentliche Stelle im Sinne von § 2 LDSG. Gemäß der Regelung in § 9 Abs. 6 IHKG gilt für die Datenübermittlung nach Abs. 1 an öffentliche Stellen das LDSG. Zunächst war darauf hinzuweisen, 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 § 5 Abs. 1 Nr. 1 LDSG 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. Die Übermittlung personenbezogener Daten an öffentliche Stellen ist nach § 14 LDSG zulässig, wenn dies entweder für Aufgaben des Empfängers oder für Aufgaben der übermittelnden Stelle erforderlich ist und wenn die Voraussetzungen vorliegen, die ausnahmsweise eine Zweckänderung erlauben. Die Voraussetzungen dieser Ausnahmen sind insgesamt in elf Fallgruppen in den §§ 12 Abs. 4 und 13 Abs. 2 LDSG geregelt. Die Notwendigkeit einer entsprechenden Datenübermittlung kann sich insbesondere in jenen Fällen ergeben, in denen eine Überprüfung der Angaben Betroffener notwendig erscheint oder dies wegen eines überwiegenden Interesses der Allgemeinheit oder von dritten Personen erforderlich ist. Eine Möglichkeit, auf dieser Grundlage die bei der IHK vorliegenden Firmendaten an die Kreisverwaltung zu übermitteln, sah der LfD nicht.

In diesem Zusammenhang war indessen zu beachten, daß § 9 Abs. 4 Satz 1 IHKG für den nichtöffentlichen Bereich eine Regelung enthält, wonach die Industrie- und Handelskammern Firma, Anschrift und Wirtschaftszweig ihrer kammerzugehörigen Unternehmen zur Förderung von Geschäftsabschlüssen und zu anderen dem Wirtschaftsverkehr dienenden Zwecken übermitteln dürfen. Ferner ist mit Satz 2 bezüglich der übrigen in Absatz 1 genannten Daten (Telefonnummer, angebotene Waren und Dienstleistungen, Betriebsgrößenklasse sowie Name und Alter der Betriebsinhaber) die Möglichkeit geschaffen worden, auch diese Daten an nichtöffentliche Stellen zu übermitteln, sofern der Kammerangehörige nicht widersprochen hat. Um die oben dargestellte Lücke bei der Übermittlung an öffentliche Stellen zu schließen, war es nach Auffassung des LfD zulässig, im vorliegenden Fall die spezialgesetzliche Regelung in § 9 Abs. 4 IHKG entsprechend anzuwenden. Wenn hier nämlich für den nichtöffentlichen Bereich die beschriebenen personenbezogenen Daten zur Verfügung gestellt werden dürfen, muß dies erst recht für die Übermittlung an öffentliche Stellen gelten.

14.5 Verwaltungsvorschrift der Landesregierung zur Bekämpfung der Korruption in der öffentlichen Verwaltung

In der Staatszeitung vom 4. November 1996 stand zu lesen, daß „die Landesregierung mit einer Verwaltungsvorschrift alle praktikablen Möglichkeiten zur Korruptionsbekämpfung in der öffentlichen Verwaltung ausschöpfen will. (...) Kern der Regelung im öffentlichen Auftragswesen ist ein zentrales Verzeichnis von unzuverlässigen Bewerbern um öffentliche Aufträge. (...) Eine solche ‚Schwarze Liste' ist nach Auffassung vieler Staatsanwälte und Rechnungsprüfer das einzige wirksame Mittel zur Bekämpfung von Korruption auch auf der Bieterseite. Die Indizierung von Unternehmen soll vorbeugenden Charakter haben."

Die Grundlage für den Ausschluß vom Vergabeverfahren sind die Verdingungsordnungen. Diese basieren auf § 55 LHO. Die Einzelregelungen finden sich in § 7 Nr. 5 Buchst. c VOL/A und § 8 Nr. 5 Abs. 1 Buchst. c VOB/A. Eine entsprechende Regelung enthält Art. 29 Buchst. d der EG-Dienstleistungsrichtlinie vom 18. Juni 1992, die mangels Umsetzung in nationales Recht mittlerweile unmittelbar gilt.

Eine Verbesserung von Maßnahmen in der Korruptionsbekämpfung ist zweifellos ein berechtigtes Anliegen. Es gilt zu verhindern, daß betroffene Firmen sich ungehindert weiter am Wettbewerb um öffentliche Aufträge beteiligen können. Die in der Verwaltungsvorschrift vorgesehenen Angaben über das betroffene Unternehmen umfassen die Datenfelder Name, Anschrift, Gewerbezweig, Branche, ggf. Handelsregisternummer, besondere Informationen über eine Konzernstruktur, Art und Weise der Verfehlung sowie Nachweis der Verfehlung.

Aufgrund der Bestandteile der Meldung war davon auszugehen, daß bei der Melde- und Informationsstelle (Finanzministerium) auch personenbezogene Daten natürlicher Personen gespeichert und übermittelt werden oder abgerufen werden können. Ferner war auch zu klären, ob mit der Regelung unter Punkt 17.5 der Verwaltungsvorschrift, wonach „die auftragsvergebenden Dienststellen die Informationen über erfaßte Unternehmen unmittelbar bei der Melde- und Informationsstelle abfragen können", womöglich ein automatisiertes Übermittlungsverfahren im Sinne von § 7 LDSG eingerichtet wurde.

Diesbezüglich hat der LfD das Ministerium der Finanzen um Stellungnahme gebeten. Darin wurde ausgeführt, daß gegenwärtig das Verzeichnis unzuverlässiger Bewerber datenschutzrechtlich nicht relevant sei. Im gewerblichen Geschäftsverkehr träten dem Staat ganz überwiegend Unternehmen gegenüber, die als juristische Personen (AG, GmbH usw.) organisiert seien und nur in seltenen Fällen Einzelunternehmen. Nach den bisherigen Erfahrungen sei nicht damit zu rechnen, daß Angaben über Einzelunternehmen in das Verzeichnis aufzunehmen sind. Auch ein automatisiertes Übermittlungsverfahren nach § 7 LDSG sei nicht vorgesehen. Nach allem würden keine personenbezogenen Daten anfallen.

Für den Fall, daß sich im Laufe der Entwicklung die Notwendigkeit ergibt, personenbezogene Daten zu speichern, wird sich das Finanzministerium am LDSG orientieren und keine Speicherung vornehmen, solange das Verzeichnis nicht das Verfahren der Anmeldung zum Datenschutzregister durchlaufen hat.

14.6 Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes

Der Entwurf soll im wesentlichen die Richtlinie des Rates der Europäischen Union vom 29. Juli 1991 über den Führerschein umsetzen (2. EG-Führerscheinrichtlinie 91/439/EWG; ABl. EG Nr. L 237, 1) und enthält daneben weitere, von der Richtlinie unabhängige Neuregelungen u. a. im Bereich des Fahrerlaubnis- und Fahrzeugzulassungsrechts. Außerdem werden hinsichtlich des Fahrzeugregisters Ergebnisse und Folgerungen umgesetzt, die im ZEVIS-Erfahrungsbericht der Bundesregierung enthalten sind (vgl. Bundestagsdrucksache 12/3251).

Aus der Sicht des Datenschutzes liegt das Hauptproblem in der vorgesehenen Einrichtung eines zentralen Fahrerlaubnisregisters. Gegenwärtig gibt es in Deutschland zentral beim Kraftfahrtbundesamt das Verkehrszentralregister, das sog. Negativdaten zur Fahrerlaubnis wie Entziehung, Versagung und Sperrfristen enthält; des weiteren sind etwa 660 örtliche Fahrerlaubnisregister vorhanden. Die erteilten Fahrerlaubnisse werden heute – ausgenommen die der Fahranfänger für den Führerschein auf Probe – ausschließlich örtlich gespeichert, wobei aufgrund von Wohnsitzänderungen Daten von einem Inhaber an mehreren örtlichen Stellen erfaßt sein können. Nach Ansicht der Bundesregierung ist die Einrichtung eines zentralen Fahrerlaubnisregisters erforderlich. Es soll ein personenbezogenes Register mit etwa 50 Mio. erfaßten Bürgerinnen und Bürgern geschaffen werden. Zwar schreibe die EG-Führerscheinrichtlinie nicht ausdrücklich das zentrale Fahrerlaubnisregister vor. Artikel 12 Abs. 3 der Richtlinie enthalte jedoch die Verpflichtung zu einem effektiven gegenseitigen Informationsaustausch über die bestehenden Fahrerlaubnisse und ausgestellten Führerscheine. In einer Protokollerklärung des Rates werde dies nochmals ausdrücklich hervorgehoben.

Unter Beteiligung der Datenschutzbeauftragten des Bundes und der Länder ist der Gesetzentwurf mehrfach überarbeitet worden. Dabei wurden aus der Sicht des Datenschutzes wichtige Fortschritte erzielt. Im Hinblick auf die beabsichtigten Regelungen in den ersten Entwürfen hat die Gefahr bestanden, daß es zur Einführung eines neuen bundesweiten „Melderegisters" von Führerscheininhabern gekommen wäre. Denn bei jedem Wohnungswechsel sollte ein Informationsaustausch zwischen Einwohnermeldebehörde und Führerscheinstelle erfolgen, die dann das neue Führerscheinregister aktualisiert hätte. Nach dem gegenwärtigen Stand des Entwurfes werden lediglich die unveränderbaren Personalien und die Führerscheindaten der Betroffenen erfaßt; es wird also kein Rückgriff auf die aktuellen Anschriften ermöglicht.

Im übrigen war eine parallele Speicherung der Daten sowohl in dem neuen zentralen Register als auch in den bestehenden örtlichen Führerscheinregistern vorgesehen. Bezüglich der Erforderlichkeit dieser beabsichtigten Doppelspeicherung haben die Datenschutzbeauftragten Bedenken erhoben mit dem Ergebnis, daß nach dem aktuellen Entwurf die örtlichen Fahrerlaubnisregister nur noch bis spätestens zum 31. Dezember 2005 geführt werden dürfen. Allerdings hat der Bundesrat in seiner Stellungnahme gefordert, diese Frist bis zum Jahre 2009 zu verlängern.

Zu den weiteren datenschutzrechtlichen Verbesserungen gehören auch die unentgeltliche Selbstauskunft für Betroffene sowie die Zweckbindung von Abrufprotokolldaten aus dem Verkehrszentralregister und dem zentralen Fahrerlaubnisregister mit der Einschränkung der Nutzung durch die Strafverfolgungsbehörden auf den Einzelfall zur Verhinderung oder Verfolgung schwerwiegender Straftaten gegen Leib, Leben und Freiheit einer Person.

14.7 Neukonzeption des automatisierten Ordnungswidrigkeitenverfahrens

Die nunmehr vom DIZ betreute Neukonzeption des DV-Verfahrens konnte im Berichtszeitraum noch nicht abgeschlossen werden. Was die Anregungen des LfD im 15. Tb., Tz. 14.8 anbelangt, hat das Ministerium des Innern und für Sport zwischenzeitlich mitgeteilt, daß für das Datenmodell der Neukonzeption des Ordnungswidrigkeitenverfahrens die Festlegung getroffen wird, beim Verwarnungsgeldangebot und bei der Anhörung im Bußgeldverfahren Angaben über einen sog. „Privatzeugen" nicht aufzunehmen. In den Fällen der Privatanzeigen wird die Angabe „Beweis: Zeuge" oder „Beweis: Zeuge vorhanden" für ausreichend gehalten. Beim Zusammentreffen von dienstlichem und privatem Zeugen ist beabsichtigt, den privaten Zeugen mit „. . . und weitere Zeugen" anzugeben. Ferner hat sich das Ministerium der Auffassung des LfD angeschlossen, daß bei den Massenverfahren der Kennzeichenanzeigen die Angaben des Betroffenen zum Führerschein in der Anhörung nicht erforderlich sind. Es führt aus: „Diese Daten werden für den Zweck, für den die übrigen Daten erhoben werden, beispielsweise die Ahndung einer Geschwindigkeitsüberschreitung, nicht benötigt." Die Aufnahme eines Merkmals „Fahrerlaubnis ja/nein" wurde hier für ausreichend gehalten.

Aufgrund dieser weitgehenden Annäherung der Auffassungen hat der LfD seine Bedenken gegen die vollständige Zeugenangabe im Bußgeldbescheid zurückgestellt und wird das Datenmodell der Neukonzeption des DV-Verfahrens zur Bearbeitung von Verkehrsordnungswidrigkeiten datenschutzrechtlich nicht beanstanden.

14.8 Halteranfragen im automatisierten Ordnungswidrigkeitenverfahren

Im Bereich des automatisierten Ordnungswidrigkeitenverfahrens war auf ein datenschutzrechtliches Problem aufmerksam zu machen. Es betrifft den Fall der gebührenpflichtigen Verwarnung bei einem Parkverstoß, wobei die Betroffenen das angebotene Verwarnungsgeld mittels des am Fahrzeug angebrachten Überweisungsträgers alsbald einzahlen. Da bei Parkverstößen nach der Rechtsprechung der Grundsatz besteht, daß der Betroffene ohne vermeidbare Verzögerung schriftlich zu der Angelegenheit angehört werden muß, und eine Zusendung des Anhörbogens erst nach der Halterfeststellung beim KBA erfolgen kann, wird nach etwa drei Tagen mittels Datenträgeraustausch eine Halteranfrage an das KBA geschickt und die Rückantwort mit den personenbezogenen Daten des Fahrzeughalters verarbeitet. Wenn nun in der Zwischenzeit der Eingang des Verwarnungsgeldes festgestellt worden ist, sind die Halterdaten nicht mehr erforderlich. In diesem Zusammenhang hat der LfD gegenüber dem DIZ angeregt, beim Einspielen der Bänder mit den Halterdaten programmtechnisch eine Plausibilitätsprüfung dergestalt zu integrieren, daß im Falle des zwischenzeitlich registrierten Zahlungseingangs die systemseitige Übernahme der entsprechenden Halterdaten unterbleibt. Das DIZ hat diesen Vorschlag umgehend aufgenommen und im automatisierten Ordnungswidrigkeitenverfahren sichergestellt, daß keine Halterdaten in das System übernommen werden, wenn der Vorgang durch Zahlung erledigt ist.

Damit wurde eine datenschutzfreundliche und zugleich mit relativ geringem Programmieraufwand verbundene Lösung verwirklicht.

14.9 Antragsvordruck zur Erteilung einer Parkberechtigung

Ein Petent hat den LfD um Prüfung eines seitens einer Stadtverwaltung entwickelten Antragsvordrucks gebeten. Es wurde gerügt, daß bei der Beantragung einer Parkberechtigung die Frage beantwortet werden müsse, ob die antragstellende Person im Besitz einer Fahrerlaubnis ist und für welche Klassen sie wann von welcher Behörde erteilt wurde. Entscheidend – so der Petent – sei hier jedoch, wer Halter des Fahrzeugs ist, wobei dieser keineswegs im Besitz einer Fahrerlaubnis sein müsse, sondern sich beispielsweise von einem Familienangehörigen oder sonstigen Personen mit einer Fahrerlaubnis fahren lassen könne. Es würden Daten erhoben, die im Rahmen der Beantragung einer Parkberechtigung keine Rolle spielten.

Die Straßenverkehrsbehörde hat in ihrer Stellungnahme u. a. folgendes ausgeführt: „Im Zuge der Einführung der Parkraumbewirtschaftung wurden vom Stadtrat Berechtigungskriterien festgelegt und beschlossen, daß die antragstellende Person als Halter des Fahrzeugs eine Fahrerlaubnis besitzen muß. Nach der Verwaltungsvorschrift zu § 45 StVO muß das Kraftfahrzeug, für das eine Sonderparkberechtigung gewährt werden soll, auf den Anwohner als Halter zugelassen sein oder nachweislich vom Antragsteller dauernd genutzt werden." Hier würden solche Personen ausscheiden, die nicht im Besitz einer Fahrerlaubnis seien, da sie nicht zum Führen des Kraftfahrzeugs berechtigt seien. Vorübergehend habe die Notwendigkeit bestanden, Kenntnis darüber zu erhalten, ob die antragstellende natürliche Person auch die zum Führen des (auf den beantragten Parkplatz abzustellenden) Kraftfahrzeugs erforderliche Fahrerlaubnis besitzt. Inzwischen bestehe für diese Vorgehensweise kein Anlaß mehr, so daß im Antragsformular bezüglich der Fahrerlaubnis nur noch folgende Angabe zu beantworten sei: „Ich besitze eine Fahrerlaubnis, die zum Führen des beantragten Kraftfahrzeuges berechtigt." Damit war nach Auffassung des LfD die Erhebung personenbezogener Daten durch die Straßenverkehrsbehörde auf das zur Aufgabenerledigung erforderliche Minimum zurückgeführt worden; denn die Fragen nach der Fahrerlaubnisklasse, dem Zeitpunkt der Erteilung sowie der ausstellenden Behörde sind entfallen. In diesem Zusammenhang war darauf hinzuweisen, daß es sich bei der Ausstellung eines Anwohner-Parkausweises um einen begünstigenden Verwaltungsakt handelt, der eine Sonderparkberechtigung begründet und als Nachweis dafür dient, daß der Inhaber zu dem begünstigten Personenkreis gehört und auf den dafür gekennzeichneten Flächen parken darf. Nach der Regelung in § 6 Abs. 1 Nr. 14 StVG i. V. m. § 45 Abs. 1 b Nr. 2 StVO kann die Straßenverkehrsbehörde Parkvorrechte schaffen. Ob und inwieweit für Anwohner reservierte Parkflächen zur Verfügung gestellt werden, steht im Ermessen der zuständigen Straßenverkehrsbehörde. Dieses Gestaltungsermessen umfaßt auch die Befugnis, den begünstigten Personenkreis näher festzulegen. Dabei ist es ein sachliches Differenzierungskriterium, wenn hinsichtlich der antragstellenden Personen darauf abgestellt wird, ob diese im Besitz einer Fahrerlaubnis sind. Denn die Parkraumnot betrifft in erster Linie diejenigen Menschen, die in dem jeweiligen Gebiet ihren Lebensmittelpunkt haben sowie ein Fahrzeug und die zugehörige Fahrerlaubnis besitzen.

Nach allem war aus der Sicht des Datenschutzes die Datenerhebung in bezug auf das Vorhandensein einer Fahrerlaubnis für das entsprechende Fahrzeug nicht zu beanstanden.

14.10 Änderung der Fahrzeugscheine durch die Meldebehörde bei Umzug innerhalb des Zulassungsbezirks

Zum Hintergrund: Bei einem Wohnungswechsel bestehen Meldepflichten sowohl gegenüber der Meldebehörde als auch gegenüber der Kfz-Zulassungsstelle. Dies bedeutet, daß die Betroffenen oftmals zwei örtlich auseinanderliegende Dienststellen aufsuchen und dort u. U. mit langen Wartezeiten rechnen müssen. Ihnen könnte ein Weg erspart werden, wenn die Meldebehörde zusammen mit der notwendigen Änderung des Melderegisters und des Personalausweises gleichzeitig auch die Anschrift im Fahrzeugschein ändert.

Hinsichtlich dieses Vorschlags, der dem LfD zur Stellungnahme zugeleitet wurde, war zunächst zu klären, welchen Rechtscharakter die Wahrnehmung von Aufgaben der Zulassungsstelle durch die Meldebehörde hat. So nehmen bei der Vorlage des Fahrzeugscheins die Meldebehörden Daten zur Kenntnis, die zur Erfüllung ihrer Aufgaben nicht erforderlich sind, nämlich alle Eintragungen außer den Adreßdaten. Es handelt sich hierbei jedoch nicht um den Fall einer (partiellen) Aufgabendelegation, sondern lediglich um reine Mithilfe bei der staatlichen Aufgabenerfüllung. Im Zusammenhang mit der Adreßänderung im Fahrzeugschein werden die Zulassungsdaten dementsprechend auch nicht i. S. v. § 12 Abs. 1 LDSG erhoben. Die Meldebehörde tritt hier sozusagen als „Werkzeug" der Zulassungsstelle auf, verarbeitet mithin auch keine Daten im Auftrag. Ihre Tätigkeit ist vielmehr unter den Begriff der technischen Erfüllungshilfe einzuordnen, wobei die Meldung an die Zulassungsstelle zur Änderung des örtlichen Fahrzeugregisters eine Datenübermittlung nach § 14 LDSG darstellt. Da es den Betroffenen freigestellt sein wird, die Adreßänderung im Fahrzeugschein weiterhin durch die Zulassungsstelle vornehmen oder seitens der Meldebehörde durchführen zu lassen, hat der LfD nach allem die Datenübermittlung für zulässig gehalten.

14.11 Automatische Gebührenerhebung auf Autobahnen – der Feldversuch ist abgeschlossen

Über den Feldversuch auf einem Autobahnteilstück der A 555 zwischen Bonn und Köln hat der LfD im 15. Tb., Tz. 14.6, ausführlich berichtet. Der Versuch wurde Ende 1995 abgeschlossen, die Ergebnisse und die Schlußfolgerungen seitens des Bundesministeriums für Verkehr dargestellt. Die Kernaussage lautet, daß die Anforderungen des Datenschutzes erfüllt werden können, wenn für die Gebührenerhebung ein anonymes Zahlungsverfahren eingesetzt wird, die Vorgänge der Erhebung und Kontrolle für die Nutzer transparent gemacht werden und wenn durch Kontrollen sichergestellt werden kann, daß kein Zahlungswilliger und kein Nutzer, der nicht gebührenpflichtig ist, als Falsch- oder Nichtzahler registriert wird. Probleme im Bereich der Kontrolle (z. B. sichere Fahrzeugerkennung, manipulationssichere Erhebung, Übermittlung und Verarbeitung der Nutzungsdaten) – wahrscheinlich auch verkehrspolitische Überlegungen – haben dazu geführt, daß die Einführung der „Autobahnmaut" für Pkw zurückgestellt wurde.

Durch die frühzeitige Beteiligung der Datenschutzbeauftragten des Bundes und der Länder war es möglich, datenschutzrechtliche Gesichtspunkte im Hinblick auf die Grundstruktur des Verfahrens zur automatisierten Gebührenerhebung auf Autobahnen einzubringen und mit den Beteiligten – teilweise vor Ort – zu diskutieren. Dabei hat sich gezeigt, daß die Datenschutzanforderungen durch eine entsprechende Technikgestaltung erfüllbar sind. Hier wurde auch deutlich, daß der Datenschutz dazu beitragen kann, fehlerhafte Entscheidungen zu vermeiden.

15. Landwirtschaft, Weinbau und Forsten

15.1 Flurbereinigungsverfahren: „Sprechende Nummern" auf den Begrenzungspflöcken

Ein Beschwerdeführer war von einem Flurbereinigungsverfahren betroffen. In dessen Verlauf wurden auf der Feldflur die vorläufigen Besitzstände markiert. Dies erfolgte durch Einschlagen kleiner Pflöcke (kurzer Dachlatten) an den Eckpunkten der jeweiligen neuen Grundstücksgrenzen. Auf den Pflöcken war in etwa 4 cm großer Schrift für jeden lesbar eine laufende Nummer angegeben, die den neuen Besitzer bezeichnen sollte. Diese Nummer bestand aus fünf Ziffern. Die ersten drei Ziffern kennzeichneten den jeweiligen Eigentümer. Die beiden letzten Ziffern gaben die Besitzverhältnisse an: Bei Alleineigentum des Ehemannes 01; bei Alleineigentum der Ehefrau 02, bei gemeinsamem Eigentum der Ehegatten 04. Der Beschwerdeführer war der Auffassung, hier handele es sich um persönliche Daten, die Außenstehende nichts angingen. Die Eigentumsangaben auf den Pflöcken waren nach seiner Auffassung nicht erforderlich.

Es ergab sich, daß bei drei von den neun Kulturämtern des Landes noch Ordnungsnummern zur Kennzeichnung bei der nach dem Furbereinigungsgesetz vorgeschriebenen örtlichen Anzeige der neuen Flurstücksgrenzen verwendet wurden. Hierfür hätten organisatorische Vorteile gesprochen. Es sei auch den Eigentümern möglich gewesen, frühzeitig zu erkennen, was sie als Zuteilung im Bodenordnungsverfahren erhalten sollten.

Grundsätzlich ist es aber nach Auffassung des zuständigen Ministeriums auch möglich, die neuen Flurstücke örtich nur durch die nicht personenbeziehbaren Flur- und Flurstücksbezeichnungen auf den Pflöcken kenntlich zu machen, wie es bereits bei sechs Kulturämtern praktiziert wurde. Diese Verfahrensweise wurde aufgrund der vom LfD vorgetragenen Bedenken inzwischen einheitlich eingeführt.

15.2 Errichtung einer Tierhalterdatei bei einer Bezirksregierung

Eine Bezirksregierung wollte in ihrer Eigenschaft als Bezirkspolizeibehörde eine Tierhalterdatei ständig zum Zweck der vorbeugenden Gefahrenabwehr einrichten. Sie bat den LfD um eine datenschutzrechtliche Beurteilung dieses Vorhabens.

Der LfD wies auf folgende Gesichtspunkte hin:

Grundsätzlich ist die Aufgabe der Tierseuchenbekämpfung von den Kreisverwaltungen wahrzunehmen. Die Bezirksregierung als Bezirkspolizeibehörde kann nur dann in einer Vielzahl gleichartiger Fälle Aufgaben der nachgeordneten oder ihrer Aufsicht unterstehenden Behörden in diesem Zusammenhang wahrnehmen, wenn Art und Umfang einer Gefahr dies erfordern (§ 1 Abs. 4 Landestierseuchengesetz). Dem LfD standen nicht genug Informationen zur Verfügung, um dies konkret beurteilen zu können. Vom zuständigen Referat der Bezirksregierung wurde auf die Bekämpfung der Maul- und Klauenseuche hingewiesen. Es wurde allerdings nicht dargelegt, daß die Bekämpfung dieser Seuche nach der gegenwärtigen Sachlage das Eingreifen der Bezirkspolizeibehörde und das Handeln auf überregionaler, kreisübergreifender Ebene erfordert hätte.

Weiterhin müßte die Speicherung der fraglichen Daten zur rechtmäßigen Erfüllung der Aufgaben der Tierseuchenbekämpfung erforderlich sein (§ 12 Abs. 1 LDSG). Die Bezirksregierung hatte als zu erfüllende Aufgabe genannt, vorbeugende Maßnahmen zu treffen, um im Fall der Verbreitung einer Tierseuche konkrete schnelle Maßnahmen zur Bekämpfung durchführen zu können. Die Datenspeicherung als vorbeugende Maßnahme für den Gefahrenfall ist auch aus datenschutzrechtlicher Sicht unter Anwendung des Erforderlichkeitsgrundsatzes nicht grundsätzlich ausgeschlossen. Allerdings muß zwischen dem Nutzen der gespeicherten Daten zur Aufgabenerfüllung im Fall der Durchführung der konkreten Gefahrenabwehrmaßnahmen und der Intensität des ständigen Eingriffs in das informationelle Selbstbestimmungsrecht der Personen, deren Daten vorsorglich gespeichert werden, ein angemessenes Verhältnis bestehen. In diesem Zusammenhang bestanden grundsätzliche Zweifel. Konkret blieb die Frage offen, ob die Speicherung der Zahl der durchgeführten Untersuchungen durch Tierärzte bei den jeweiligen erfaßten Tierhaltern wirklich im Fall der Durchführung von Tierseuchenbekämpfungsmaßnahmen erforderlich war.

Konkret war ergänzend zu prüfen, ob die Zweckbindung der Daten bei den Stellen, von denen diese übermittelt werden sollten, zulässigerweise zum Zweck der vorbeugenden Tierseuchenbekämpfung durchbrochen werden durfte. Gegen die Nutzung der Daten der Tierseuchenkassen hat der LfD in diesem Zusammenhang Bedenken erhoben. Diese Daten werden unter Hinweis auf genau und abschließend genannte Zwecke bei den Betroffenen erhoben.

Als letztes wies der LfD darauf hin, daß eine Erhebung der fraglichen Daten bei Statistikstellen gegen das Statistikgeheimnis verstoßen würde und grundsätzlich ausgeschlossen ist.

Insgesamt kam der LfD zu dem Ergebnis, daß nach den ihm vorliegenden Informationen die Erstellung einer entsprechenden Tierhalterdatei auf der Ebene der Bezirksregierung derzeitig nicht zulässig war.

Die Bezirksregierung sah von einer entsprechenden Datenspeicherung ab.

15.3 Betriebsdatenerhebung im Rahmen der Entsorgung von Reststoffen aus der Weinbereitung

Im Rahmen des Bringsystems für weinbauliche Abwässer forderte das Abwasserwerk einer Verbandsgemeinde von einem anliefernden Winzer Nachweise über die Entsorgung von Reststoffen aus der Weinbereitung. Der Winzer sollte nicht nur angeben, wieviel Wein er erzeugt hatte, sondern auch eine Kopie der Weinerzeugungsmeldung vorlegen.

Dagegen wandte sich der Winzer mit dem Argument, diese Weinerzeugungsmeldung lasse eine Vielzahl von Betriebsdaten erkennen, die für die wirtschaftliche Leistungsfähigkeit eines Betriebes bedeutsam seien. So würden nicht nur die erzeugten Weine nach Rebsorten, sondern auch die Qualitätsstufen dort gesondert aufgeführt.

Aus datenschutzrechtlicher Sicht stellte sich die Frage, ob die Datenerhebung zum Zweck der Durchführung des Bringsystems für weinbauliche Abwässer erforderlich war. Es ergab sich, daß das Abwasserwerk folgende Informationen benötigte:

- Angabe der Ertragsrebfläche; diese war erforderlich, um das Flächenverhältnis von teilnehmenden zu nicht teilnehmenden Flächen bestimmen zu können;
- Verkaufsmengen von Trauben und Traubenmost: Diese Informationen konnten zur Reduzierung der Maßstabshöhe für die Berechnung des Beitrages führen.

Die Erhebung dieser Daten war also zulässig. Ebenso war es zulässig, daß das Abwasserwerk bezüglich dieser Angaben einen gewissen Nachweis gefordert hat.

Da die Traubenernte- und Weinerzeugungsmeldung jedoch Angaben über die genannten erforderlichen Daten hinaus enthält, hat der LfD angeregt, den Teilnehmern am Bringsystem freizustellen, die jeweils vorzulegende Kopie der Traubenerntemeldung bezüglich der Angaben zu Rebsorte und Qualitätsstufe zu schwärzen bzw. diese Rubriken bei der Kopie abzudecken.

Mit diesem Verfahren hat sich das Abwasserwerk einverstanden erklärt. Dementsprechend hat es seine Formulare um folgenden Zusatz ergänzt: „Angaben zu Rebsorten und Qualitätsstufen auf der Weinerzeugungsmeldung können auf der Kopie geschwärzt bzw. beim Kopieren abgedeckt werden."

15.4 Datenschutz bei der Versendung von landwirtschaftlichen Antragsformularen

In einer Eingabe wurde beklagt, daß auf den Adreßetiketten, die eine Kreisverwaltung auf den Umschlägen mit landwirtschaftlichen Antragsformularen verwandte, neben dem Namen und der Anschrift des jeweiligen Landwirts auch die volle landwirtschaftliche Betriebsnummer aufgebracht war.

Ein betroffener Landwirt trug vor, mit Hilfe dieser Betriebsnummer könne jedermann bei der Kreisverwaltung innerbetriebliche Angelegenheiten erfragen.

Die vom LfD um Stellungnahme gebetene Kreisverwaltung teilte mit, daß die in Rede stehenden Adressenaufkleber vom Statistischen Landesamt zur Verfügung gestellt würden. Die Kreisverwaltung verwende sie unverändert. Diese Verfahrensweise sei landeseinheitlich geregelt. Aus Sicht der Kreisverwaltung sei der gemeinsame Ausdruck von Betriebsnummer und Anschrift im Adressenfeld nicht erforderlich.

Das zuständige Ministerium hat daraufhin mitgeteilt, die Adreßaufkleber würden aus den Daten der landwirtschaftlichen Betriebsdatenbank erstellt werden. Die aufgedruckte Unternehmensnummer stelle eine fortlaufende Numerierung innerhalb der Sitzgemeinde des Unternehmens dar. Die Kuvertierung der Antragsunterlagen erfolge manuell durch die Kreisverwaltung. Einige der Antragsformulare seien bereits mit unternehmensspezifischen Daten ausgefüllt. Um sicherzustellen, daß die teilausgefüllten Antragsformulare in die richtigen Umschläge gelangten, werde ein Vergleich der Unternehmensnummer durch den Mitarbeiter der Kreisverwaltung durchgeführt: Er vergleiche die Unternehmensnummer auf dem Adreßetikett des Umschlags mit der auf dem Antragsformular aufgebrachten Nummer. Dies diene sowohl der Sicherheit des Landwirts als auch der Verwaltung.

Da der Umschlag durch die Post unmittelbar dem Empfänger zugeleitet werde und Dritte üblicherweise keine Kenntnis davon erhielten, sei diese Verfahrensweise aus der Sicht des Ministeriums mit datenschutzrechtlichen Regelungen vereinbar. Die Kreisverwaltung hat ergänzend mitgeteilt, daß allein aufgrund der Unternehmensnummer keinerlei Auskünfte erteilt würden.

Nach diesem Vortrag hat der LfD die Nutzung der Unternehmensnummer auf dem Adressenetikett für erforderlich und angemessen und damit auch datenschutzrechtlich zulässig gehalten.

15.5 Datenübermittlungen an die Landwirtschaftskammer Rheinland-Pfalz

Die Landwirtschaftskammer Rheinland-Pfalz erstellt im Rahmen der Fortschreibung der Flächennutzungspläne bzw. der Landschaftspläne einen landwirtschaftlichen Fachbeitrag. Damit soll den Planungsbüros Material für ihre gutachterlichen Stellungnahmen zur Verfügung gestellt werden, und es sollen den Verbandsgemeinden Hilfen für das planungsrechtliche Abwägungsverfahren gegeben werden.

Zu diesem Zweck erbat die Landwirtschaftskammer von den Kreisverwaltungen Namen und Anschriften aller landwirtschaftlichen Betriebe mit Angaben der Größe und Nutzungen der landwirtschaftlichen oder forstwirtschaftlichen Flächen, Namen der Betriebe, die Extensivierungsprogramme des Landes Rheinland-Pfalz in Anspruch nehmen sowie Lage und Größe der Parzellen, die im Rahmen der Extensivierungsprogramme bewirtschaftet werden. Die Anschriften und Namen sollten dazu dienen, evtl. vor Ort Befragungen durchzuführen.

Der LfD beurteilte dieses Anliegen wie folgt:

Die von der Landwirtschaftskammer erbetenen Angaben könnten ausschließlich aus der Betriebsdatenbank der Kreisverwaltungen entnommen werden. Datenschutzrechtlich war also zu beurteilen, ob die Daten der landwirtschaftlichen Betriebsdatenbank für die hier genannten Zwecke der Landwirtschaftskammer übermittelt und genutzt werden dürften.

Die allgemeinen Regelungen des LDSG sind in diesem Zusammenhang nicht anzuwenden, da für die landwirtschaftliche Betriebsdatenbank eine vorrangige bereichsspezifische Regelung, insbesondere zur Zweckbindung der dort gespeicherten Daten, existiert. Diese Betriebsdatenbank ist errichtet worden, um die Fördermaßnahmen in den Sektoren der pflanzlichen und der tierischen Produktion nach den entsprechenden EG-Regelungen durchzuführen.

Die dort genannten Voraussetzungen lagen nicht vor. Der LfD hat in Übereinstimmung mit dem zuständigen Ministerium die begehrten Datenübermittlungen für nicht zulässig gehalten.

Von den entsprechenden Datenübermittlungen wurde Abstand genommen.

15.6 Nutzung von Daten der EG-Weinbaukartei zu Zwecken gemeindlicher Abgabeerhebungen

Eine Verbandsgemeinde erhebt Schmutzwasserabgaben auf bewirtschaftete Rebflächen. Zu diesem Zweck versendet sie Erhebungsbögen an die Winzer, die bereits eine Angabe über deren gesamte Rebfläche enthalten. Die Winzer sollen dann von dieser Gesamtrebfläche geordnet nach unterschiedlichen Kriterien die Flächen abziehen, die nicht bewirtschaftet werden.

Die Ausgangsinformation über die Gesamtrebfläche stammt aus den Daten der Weinbaukartei, die der Verbandsgemeinde zum Zweck der Beitragserhebung in anderen Zusammenhängen (Abgaben zum Deutschen Weinfonds und nach dem Absatzförderungsgesetz, Abgabe an die Wiederaufbaukasse) zur Verfügung stehen.

Ein Beschwerdeführer wandte sich dagegen, daß die Gesamtrebflächenangaben aus der Weinbaukartei zu Zwecken der Abgabenerhebung im vorliegenden Zusammenhang genutzt wurden.

Der LfD hat dies wie folgt beurteilt:

Die Einrichtung der Weinbaukartei ist durch Verordmung (EWG) Nr. 2392/86 des Rates zur Einführung der gemeinschaftlichen Weinbaukartei vom 24. Juli 1986 (ABl. EG Nr. L 208 S. 1) vorgesehen. Artikel 3 Abs. 1 2. Spiegelstrich dieser Verordnung regelt folgendes:

„Die Mitgliedstaaten tragen dafür Sorge, daß die Weinbaukartei ausschließlich zur Durchführung der weinrechtlichen Vorschriften, für statistische Zwecke oder strukturelle Maßnahmen verwendet wird. Die Mitgliedstaaten können aber, soweit es ihre innerstaatlichen Rechtsvorschriften zulassen, vorsehen, daß die Kartei auch zu anderen Zwecken verwendet werden kann, insbesondere zu strafrechtlichen oder steuerlichen Zwecken."

Bei der Auslegung dieser Vorschrift ist zu berücksichtigen, daß der Vorschlag des Rates ursprünglich keine Erweiterung der Zweckbestimmung der Daten vorgesehen hat. Die genannte Erweiterung kam auf Initiative Frankreichs zustande, das seine Weinkontrolldaten traditionell auch zu steuerlichen Zwecken nutzt. Deutschland hat im Verordnungsgebungsverfahren kein Interesse an einer solchen Erweiterung geäußert.

Außerdem ist festzustellen, daß nach dem Wortlaut und nach der Entstehungsgeschichte dieser EG-Vorschrift ausdrückliche nationale bereichsspezifische Zweckerweiterungsregelungen für eine zweckerweiternde Nutzung der Weinbaukartei erforderlich sind.

Solche ergänzenden ausdrücklichen bereichsspezifischen nationalen Vorschriften bestehen nicht, um die Weinbaukarteidaten zum Zweck der Schmutzwasserabgabenerhebung nutzen zu dürfen. Das LDSG kommt wegen den vorrangigen speziellen Regelungen der EG-Verordnung nicht zur Anwendung.

Vor diesem Hintergrund hat der LfD der Verbandsgemeindeverwaltung mitgeteilt, daß eine Nutzung der Daten, wie sie im vorliegenden Fall erfolgt ist, aus datenschutzrechtlicher Sicht unzulässig ist.

Die Verbandsgemeinde hat sich dieser Auffassung schließlich angeschlossen.

16. Statistik

16.1 Mikrozensus

In jedem Jahr gehen zum Mikrozensus zahlreiche Anfragen ein (vgl. die Darstellung im 15. Tb., Tz. 16.1). Die enge Zusammenarbeit mit dem Statistischen Landesamt hat sich im Berichtszeitraum bewährt. Die für den Mikrozensus 1996 eingesetzten Erhebungsunterlagen zeichnen sich im Vergleich zu den Befragungsbögen des Mikrozensus 1995 erfreulicherweise durch eine größere Klarheit und Transparenz aus. So ist nunmehr für die schriftliche Befragung der deutliche Hinweis auf die Freiwilligkeit dadurch sichergestellt, daß am linken Rand der betreffenden Frage die Kennzeichnung durch das (senkrecht) ausgeschriebene Wort „freiwillig" erfolgt. Weiterhin ist diese Kennzeichnung deutlich sichtbar in grüner Farbe unterlegt.

Begrüßenswert ist ebenfalls, daß bei allen Fragen mit freiwillliger Auskunftserteilung eine eigene Anwortkategorie „keine Angabe" aufgenommen wurde. Auch für die mündliche Befragung sind im Erhebungsbogen der interviewenden Person im Zusammenhang mit der Freiwilligkeit entsprechende Vorkehrungen getroffen worden.

Fernerhin fiel angenehm auf, daß im Interviewer-Handbuch zur Durchführung des Mikrozensus 1996 nunmehr unter Punkt 4.2 besonderer Wert auf die Erläuterung zur Freiwilligkeit der Auskunftserteilung gelegt wird. Lediglich die Ausgestaltung des Hinweises im Ankündigungsschreiben zur Haushaltsbefragung auf die Möglichkeit, den Fragebogen selbst auszufüllen, war

nach Auffassung des LfD nicht sehr gelungen. Hier wäre ein expliziter Hinweis auf die verschiedenen Arten der Auskunftserteilung wünschenswert gewesen. Im Text des Ankündigungsschreibens war der Hinweis optisch nicht abgehoben und nur in einem Halbsatz untergebracht, so daß er leicht zu überlesen war.

Insgesamt war jedoch festzustellen, daß die seitens des LfD in seinem 15. Tb. dargestellte Problematik vom Statistischen Landesamt aufgenommen und die angeregten Verbesserungen bei der Ausgestaltung der Haushaltsbefragung Mikrozensus 1996 größtenteils umgesetzt wurden.

In Abstimmung mit dem LfD hat das Statitische Landesamt hinsichtlich des Mikrozensus 1997 den Text des Ankündigungsschreibens entsprechend umgestaltet und einen expliziten Hinweis auf die verschiedenen Arten der Auskunftserteilung aufgenommen.

16.2 Entwurf eines Statistikregistergesetzes

Nach der Verordnung des Rates vom 22. Juli 1993 über die innergemeinschaftliche Koordinierung des Aufbaus von Unternehmensregistern für statistische Verwendungszwecke – VO Nr. 2186/93 – (ABl. EG Nr. L 196 S. 1) sind die Mitgliedstaaten der Europäischen Union verpflichtet, Unternehmensregister für statistische Verwendungszwecke (Statistikregister) aufzubauen und zu führen.

Der Entwurf eines Statistikregistergesetzes soll den Vorgaben der EG-Unternehmensregisterverordnung Rechnung tragen. Es ist vorgesehen, daß die Bundesanstalt für Arbeit, die Finanzbehörden, die Industrie- und Handelskammern und die örtlichen Gewerbeämter aus ihrem Datenbestand Angaben über Unternehmen an die Statistikämter zum Aufbau und zur Führung eines Unternehmensregisters übermitteln. Für den Aufbau und die Führung des Statistikregisters werden neben den Namen und Adressen von Unternehmen und ihren Betrieben insbesondere Angaben über Umsatz, Zahl der Beschäftigten, Rechtsform, Beginn und Ende der wirtschaftlichen Tätigkeit sowie der Wirtschaftszweig aufgenommen und jährlich aktualisiert. Der zugrunde gelegte Unternehmensbegriff ist hierbei sehr weit und umfaßt juristische Personen ebenso wie natürliche Personen aller Wirtschaftszweige und Berufe, soweit sie zum Bruttosozialprodukt infolge ihrer selbständigen wirtschaftlichen Tätigkeit beitragen. Mithin werden im Unternehmensregister Angehörige der freien Berufe ebenso erfaßt wie Handwerker und Einzelhändler.

Ursprünglich war geplant, eine Unternehmenskennummer einzuführen, um die aus unterschiedlichen Quellen stammenden Angaben im Unternehmensregister zusammenzuführen. Aus der Sicht des Datenschutzes wurden Bedenken bezüglich dieses einheitlichen Kennzeichens vorgetragen, das zu einer Art Personenkennzeichen für Selbständige und Angehörige freier Berufe führen könnte. Die Diskussion in diesem Zusammenhang ist noch nicht abgeschlossen. Ein weiteres Problem scheint indessen gelöst: Nach der Neufassung von § 3 Abs. 2 des o. g. Gesetzentwurfs übermitteln die Statistischen Ämter bestimmte Betriebsdaten aus dem Statistikregister jährlich an die Bundesanstalt für Arbeit, soweit diese Angaben im Statistikregister gegenüber der von der Bundesanstalt für Arbeit übermittelten Angaben abweichen. Diesbezüglich geäußerte datenschutzrechtliche Bedenken wurden berücksichtigt, indem nunmehr wegen des Grundsatzes der Trennung von Statistik und Verwaltung die abweichende Angabe ausschließlich für statistische Zwecke und nur in den abgeschotteten Bereich der Bundesanstalt übermittelt wird. Die Arbeiten am Entwurf für ein Statistikregistergesetz sind noch nicht abgeschlossen.

16.3 Nutzung von Melderegistern für künftigen Zensus?

Die Europäische Kommission arbeitet an einem Projekt „Volkszählung 2001". Es soll unionsweit eine Zählung der Bevölkerungen und Wohnungen durchgeführt werden. Die diesbezüglichen Vorstellungen zum Erhebungsprogramm gehen teilweise über den Rahmen der Volkszählung in Deutschland im Jahre 1987 hinaus, beispielsweise bei der Frage nach Verwandtschaftsverhältnissen innerhalb eines Haushalt sowie der Erfassung des Geburtsdatums mit Tag, Monat und Jahr. Aufgrund zu erwartender Akzeptanzprobleme bei der Bevölkerung – auch die Frage der Finanzierbarkeit spielt hier eine Rolle – im Hinblick auf eine Volkszählung (Vollerhebung) hat die Bundesregierung gegen das Vorhaben auf der Ebene der Europäischen Union Vorbehalte geltend gemacht. Zur Umsetzung der geplanten europäischen Statistikanforderungen wird daran gedacht, die Daten durch Auswertung von Verwaltungsregistern zu gewinnen. Insbesondere kommen hier die Einwohnermelderegister in Betracht, aus denen sich datenmäßig bereits Vor- und Familienname, Geschlecht, Tag und Ort der Geburt, Familienstand, Staatsangehörigkeit und Wohnungsstand ergeben.

Aus der Sicht des Datenschutzes bestehen erhebliche Bedenken gegen eine solche Vorgehensweise; denn bei statistischen Erhebungen ist nach verfassungsgerichtlicher Rechtsprechung der Grundsatz der Trennung von Statistik und Verwaltung zu gewährleisten. So hat das Bundesverfassungsgericht im Volkszählungsurteil die Auffassung vertreten, daß die damals vorgesehene Übernahme sämtlicher Daten aus bereits vorhandenen Dateien der Verwaltung keine zulässige Alternative zur Totalzählung ist. „Die Nutzung von Daten aus verschiedenen Registern und Dateien würde voraussetzen, daß technische, organisatorische und rechtliche Maßnahmen getroffen werden, die es erst erlauben, diese Daten, bezogen auf bestimmte Personen oder Institutionen,

zusammenzuführen. Eine solche Maßnahme wäre z. B. die Einführung eines einheitlichen, für alle Register und Dateien geltenden Personenkennzeichens oder dessen Substituts. Dies wäre aber gerade ein entscheidender Schritt, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren" (BVerfGE 65, 1, 57).

In der Diskussion befindet sich auch die Überlegung, das Melderegister für Zwecke der Statistik um weitere Merkmale zu ergänzen (z. B. Angaben zu Bildungsabschlüssen, zur Berufstätigkeit sowie zum Pendlerverhalten). Verwaltungsregister müssen indessen nach Auffassung der Datenschutzbeauftragten auf diejenigen Daten beschränkt bleiben, die für die rechtmäßige Erfüllung der Aufgaben der Verwaltung erforderlich sind. Eine statistikbezogene Erweiterung des Katalogs der gesetzlich festgelegten Meldedaten wäre danach unzulässig.

Sollten sich die Pläne für eine unionsweite Volkszählung weiter konkretisieren, wird aus datenschutzrechtlicher Sicht auf die Gefahren einer „Register-Volkszählung" als Ersatz für eine Primärerhebung eindringlich hinzuweisen sein.

17. Personaldatenverarbeitung

17.1 Personalverwaltungssysteme

Das Ministerium des Innern und für Sport ist seit etwa zwei Jahren damit beschäftigt, ein neues automatisiertes Personalverwaltungssystem einzuführen. Dabei handelt es sich um ein bei den Regierungspräsidien in Hessen eingeführtes System. In diesem Zusammenhang haben mehrere intensive Erörterungen stattgefunden. Schwerpunkte waren die Zugriffsprotokollierungen, die Löschungsfristen der Datenfelder „Beurteilungen" und „Nebentätigkeiten" und die Einrichtung von differenzierten Zugriffsprofilen.

Da dieses System noch intensiv mit der Personalvertretung abgestimmt werden soll, wird mit weiteren ein bis zwei Jahren bis zur Realisierung gerechnet.

Die Katasterverwaltung hat deshalb eine andere, neuere hessische Entwicklung namens „FARO" zum Beginn der Neuorganisation ab April 1997 übernommen. Auch hier haben zu den gleichen Punkten Beratungsgespräche stattgefunden. Datenschutzfragen zur Telearbeit werden unten, Tz. 21.7, erörtert.

17.2 Bekanntgabe der Stundenreduzierungen von Lehrern an den Schulelternbeirat

Der Personalrat einer Schule wandte sich mit der Frage an den LfD, ob es zulässig sei, daß der Schulleiter den Schulelternbeirat konkret über die jeweiligen Lehrdeputatskürzungen verschiedener Lehrer unterrichtet. Dabei habe der Schulleiter mitgeteilt, daß eine bestimmte Lehrerin ein Attest bis zum 1. Mai vorgelegt habe, daß sie evtl. aber auch länger fehlen werde sowie daß ein bestimmter Lehrer zukünftig aus gesundheitlichen Gründen weniger unterrichten werde.

Der LfD hat dies wie folgt beurteilt: Die Angabe, wie lange eine Lehrkraft voraussichtlich dem Dienst fernbleiben wird, ist zum einen ein personenbezogenes Datum, das dem Personaldatenschutz unterliegt. Zum andern aber hat diese Angabe unmittelbaren Bezug zur Amtsausübung der Lehrkraft; Schüler und Eltern – dementsprechend auch die Elternvertreter – sind von derartigen Informationen unmittelbar betroffen. Die Rechtslage trägt dem Rechnung: Lehrerdaten dürfen genutzt werden, wenn dies zur Erfüllung schulischer Aufgaben erforderlich ist (§ 54 a Abs. 1 Satz 2 SchulG). Es ist Aufgabe der Schule, die Eltern an der Gestaltung der Erziehungs- und Unterrichtsarbeit der Schule zu beteiligen. Das Vertrauensverhältnis zwischen der Schule und dem Elternhaus ist zu festigen und zu vertiefen (§ 33 Abs. 1 SchulG; ausführlicher zur schulrechtlichen Lage s. o. die Ausführungen unter 8.1.6). Vor diesem Hintergrund ist es aus der Sicht des LfD erforderlich, die Elternvertretungen über Dauer und Grund von Abwesenheitszeiten der Lehrkräfte zu unterrichten.

Bezüglich der betroffenen Lehrerin bedeutete die Information, daß unter Umständen mit einem längeren Fehlen über den 1. Mai hinaus zu rechnen sei, daß insofern Unsicherheit über die Dauer der Erkrankung bestand. Auch mit diesem Inhalt ist nicht erkennbar, daß überflüssige und überschießende Informationen, deren Nutzung dann auch unzulässig gewesen wäre, betroffen waren. Die Unsicherheit, ob die Lehrerin nach dem 1. Mai wieder zur Verfügung stehen wird, durfte zulässigerweise den Betroffenen zur Kenntnis gegeben werden.

Die Information bezüglich des Lehrers, daß dieser aus gesundheitlichen Gründen künftig weniger unterrichten werde, könnte möglicherweise als zu weitgehend angesehen werden. Der Grund, warum das Lehrdeputat gekürzt wurde, ist für die betroffenen Eltern und Kinder nicht unmittelbar bedeutsam. Auch diesbezüglich ist das Geheimhaltungsinteresse des betroffenen Lehrers aber nicht so stark zu gewichten, daß das o. g. gesetzliche Ziel, das Vertrauensverhältnis zwischen der Schule und dem Elternhaus zu festigen und zu vertiefen, dahinter zurückstehen müßte. Jedenfalls dann, wenn die Mitteilung über den Grund von Abwesenheitszeiten so global wie im vorliegenden Fall erfolgt, bestehen dagegen keine datenschutzrechtlichen Bedenken.

Ein Verstoß gegen datenschutzrechtliche Vorschriften war deshalb aus der Sicht des LfD nicht gegeben.

17.3 Personaldaten im Internet

Die Frage, ob und in welchem Umfang Beamtendaten bzw. Daten von Funktionsträgern des öffentlichen Dienstes auch im Internet veröffentlicht werden dürfen, hat den LfD im Berichtszeitraum wiederholt beschäftigt.

Er geht dabei von folgenden Gesichtspunkten aus:

Name, Dienstbezeichnung und Funktionsbeschreibung eines öffentlich Bediensteten sind Informationen, die grundsätzlich nicht dem informationellen Selbstbestimmungsrecht des Betroffenen selbst unterliegen. Dies sind nämlich Informationen, die einen solch engen Bezug zur amtlichen Tätigkeit bzw. zum Handeln des Staates gegenüber den Bürgern haben, daß sie nicht primär der Individualsphäre des Bediensteten, sondern der Sphäre des Staates zuzuordnen sind. Der Betroffene hat insofern nicht das Recht, nur nach eigenem Gutdünken über die Verbreitung dieser Daten zu bestimmen (vgl. 13. Tb., Tz. 17.3).

Andererseits ist der Dienstherr nicht frei im Umgang mit diesen Daten. Er hat vielmehr die beamtenrechtliche Fürsorgepflicht (die vergleichbar auch gegenüber Angestellten gilt) zu beachten. Dies ist allerdings nicht primär ein Datenschutzgesichtspunkt, sondern ein Gesichtspunkt des Beamten- bzw. Arbeitsrechts. Soweit die Veröffentlichung der Amtsdaten im Internet betroffen ist, hat der LfD keine Gründe der Fürsorgepflicht gesehen, die dem entgegenstehen würden. Entsprechende Daten sind in einer Vielzahl anderer Publikationen ebenfalls öffentlich zugänglich. Die neue Qualität des Internets begründet insofern keine erheblichen zusätzlichen Gefährdungstatbestände.

Diese Gesichtspunkte gelten allerdings nur bezüglich der genannten Informationen. Soweit auch die Veröffentlichung eines Bildes betroffen ist, soweit das Geburtsdatum, die Privatadresse oder das Privattelefon in Rede stehen, kann nicht mehr davon gesprochen werden, daß der Aspekt des Handelns für ein staatliches Organ im Vordergrund steht. Diese Daten gehören vielmehr primär der persönlichen Sphäre der Bediensteten an. Sie unterliegen deshalb auch ihrem informationellen Selbstbestimmungsrecht. Mit anderen Worten: Eine Veröffentlichung wäre nur zulässig, wenn die Betroffenen eingewilligt hätten; eine gesetzliche Vorschrift, die diese Einwilligung entbehrlich machen würde, existiert in diesem Zusammenhang nicht. Zu Fragen des technisch-organisatorischen Datenschutzes bei Internet-Anschlüssen s. u. Tz. 21.6.

17.4 Weitergabe der Daten Schwangerer an den Personalrat/Betriebsrat

Nach § 80 Abs.1 BetrVG gehört es zu den grundlegenden Aufgaben des Betriebsrates, die Durchführung der zugunsten der Arbeitnehmer geltenden Normen, zu denen auch die Vorschriften über den Mutterschutz gehören, zu überwachen. Um diese allgemeine Überwachungspflicht effektiv wahrnehmen zu können, steht dem Betriebsrat gegenüber dem Arbeitgeber ein Informationsanspruch zu (vgl. § 80 Abs. 2 BetrVG). Dieser Informationsanspruch gilt jedoch nicht uneingeschränkt, sondern nur insoweit, als die Mitarbeitervertretung Auskünfte von seiten des Arbeitgebers benötigt, um aus einem bestimmten Anlaß eine konkrete Aufgabe erfüllen zu können. Ein diesbezüglicher Anspruch setzt demnach voraus, daß der Betriebsrat eine Aufgabe zu erfüllen hat, die es erfordert, ihn über einen bestimmten Sachverhalt zu unterrichten. Ein allgemeines Informationsrecht steht dem Betriebsrat dagegen nicht zu, da er nicht die Funktion eines allgemeinen Kontrollorgans besitzt (so ausdrücklich für einen vergleichbaren Sachverhalt BVerwG NJW 1991, 373 für die inhaltsgleiche Vorschrift des § 68 Abs. 2 S. 1 LPersVG a. F.).

Darüber hinaus ist zu beachten, daß eine ohne vorherige Zustimmung erfolgte Weitergabe persönlicher Daten aus der Privat- und Intimssphäre – wozu auch das Bestehen einer Schwangerschaft gehört – eine Beeinträchtigung der Belange der Betroffenen bedeutet, so daß an das Informationsbegehren strenge Anforderungen zu stellen sind (in diesem Sinne auch: BVerwG NJW 1991, 373).

Aus diesem Grunde hat der Betriebsrat keinen Anspruch auf eine laufende Unterrichtung über schwangere Mitarbeiterinnen, die ihre Einwilligung zu seiner Unterrichtung nicht erteilt haben.

Der Betriebsrat ist somit darauf beschränkt, in anderer Weise, z. B. durch regelmäßige Mitteilungen an die weiblichen Beschäftigten, dafür zu sorgen, daß die Mutterschutzbestimmungen in Anspruch genommen und beachtet werden.

In diesem Sinn hat der LfD gegenüber anfragenden Dienststellen Stellung genommen.

17.5 Verwaltungsvorschrift zur Erstellung der Frauenförderpläne

Der LfD hatte zum Entwurf einer VV Stellung zu nehmen, die die Erstellung der Frauenförderpläne und der damit zusammenhängenden Berichte regeln soll. Die Frauenförderpläne sollen danach aus einem Datenteil, einem Prognoseteil sowie einem Maßnahmeteil bestehen.

Als Anlage zum VV-Entwurf waren 14 Erhebungsbögen beigefügt. Diese Bögen sollten Teil des Datenteils der Frauenförderpläne werden.

Diese Erhebungsbögen enthalten zwar in Einzelfällen möglicherweise personenbeziehbare Daten, insbesondere wenn in den einzelnen Spalten Angaben über nur eine Person gemacht werden. Die erhobenen Angaben sind jedoch insgesamt grundsätzlich dienststellenintern wohl bekannt. Sensible Informationen sind in keinem Fall betroffen.

Datenschutzrechtliche Fragen ergaben sich allerdings im Zusammenhang mit dem sog. „Maßnahmeteil". Wenn in den Frauenförderplänen einzelne Maßnahmen genannt werden, so könnten diese möglicherweise personenbeziehbare Informationen enthalten. Wenn in diesem Zusammenhang personenbezogene oder personenbeziehbare Daten mit sensibleren Informationen Teil des Maßnahmeteils werden sollten, so wären datenschutzrechtliche Anforderungen an die Nutzung dieses Maßnahmeteils zu beachten.

Der gesamte Frauenförderplan mit Datenteil und Maßnahmeteil soll dienststellenintern veröffentlicht werden. Der LfD geht davon aus, daß die Frauenförderpläne insoweit grundsätzlich nur dem dienstinternen Gebrauch (unter Einschluß der Meldung an die jeweiligen Aufsichtsinstanzen) dienen. Dann bestehen auch unter dem Aspekt der Personenbeziehbarkeit keine grundsätzlichen Bedenken gegen die hier erfolgende Datenverarbeitung. Der LfD hat aber empfohlen, die VV um einen Hinweis darauf zu ergänzen, daß die Informationen, die im Frauenförderplan enthalten sind, nur dem dienstlichen Gebrauch dienen, den Beschränkungen des § 70 LBG bzw. des § 203 Abs. 2 StGB unterliegen und nicht als allgemein veröffentlichte Daten anzusehen sind.

Das Ministerium ist dieser Anregung im wesentlichen nachgekommen.

17.6 Nebentätigkeitsmeldungen

Die Einführung neuer Formulare zur Befragung der Landesbediensteten, ob und in welchem Umfang sie Nebentätigkeiten ausüben, hat insbesondere unter Lehrern zu Unruhe und zur Frage an den LfD geführt, ob diese Formulare und die zugrundeliegenden Rechtsvorschriften (Landesbeamtengesetz, NebentätigkeitsVO) mit dem Datenschutz vereinbar seien.

Den Fragestellern war sicherlich darin zuzustimmen, daß die Erhebung von Informationen über Nebentätigkeiten auch deren außerdienstliches Verhalten betrifft und insofern eine Einschränkung ihres informationellen Selbstbestimmungsrechtes mit sich bringt.

Diese Einschränkung ist jedoch aufgrund des Gesetzes (§§ 71 a bis 77 LBG i. V. m. der NebentätigkeitsVO) gesetzlich gerechtfertigt:

- Die Übernahme einer Pflegschaft bei Angehörigen ist gem. § 71 a Abs. 1 Satz 2 zweiter Halbsatz LBG anzeigepflichtig.
- Die Verwaltung fremden Vermögens, wenn sie entgeltlich erfolgt, ist eine gem. § 71 a Abs. 3 LBG genehmigungspflichtige Nebentätigkeit.
- Vorstandspositionen in Vereinen etc. sind dann (aber auch nur dann) anzeigepflichtige Nebentätigkeiten, wenn sie entgeltlich wahrgenommen werden (§ 74 Nr. 1 LBG).

Jeder öffentlich Bedienstete ist verpflichtet, entsprechend dem Grundsatz der Gesetzmäßigkeit seines Handelns die gesetzlich auferlegten Pflichten zu erfüllen. Wenn er der Auffassung ist, gesetzliche Pflichten würden gegen höherrangiges Recht verstoßen (hier käme nur das Grundgesetz in Betracht), bleibt es ihm unbenommen, eine Verfassungsbeschwerde beim Bundesverfassungsgericht einzureichen.

Nach Auffassung des LfD verstoßen die genannten Regelungen des Nebentätigkeitsrechts aber nicht gegen Verfassungsrecht, auch nicht gegen das Grundrecht auf informationelle Selbstbestimmung. Die genehmigungs- und anzeigepflichtigen Tatbestände haben sämtlich einen deutlichen Sozialbezug und können im Einzelfall Auswirkungen auf die Amtsausübung des öffentlich Bediensteten haben, sei es unter dem Gesichtspunkt der außerdienstlichen Belastung, sei es unter dem der möglichen Befangenheit bei einzelnen dienstlichen Handlungen. Datenschutzüberlegungen sind immer in Verhältnis zu anderen Staatszielen zu setzen. Es hat jeweils konkret eine Abwägung zu erfolgen, wenn die unterschiedlichen Ziele kollidieren. Diese Abwägung hat der Gesetzgeber im Bereich der Nebentätigkeiten in nachvollziehbarer und nicht zu beanstandender Weise getroffen.

17.7 Personaldatenübermittlung durch die ZBV zu gemeindlichen Vollstreckungszwecken

Der nunmehr im Ruhestand befindliche Beschwerdeführer war als angestellter Lehrer im Dienst des Landes tätig gewesen. Seine Rente erhält er nicht vom Land, sondern von einer anderen Stelle.

Im Rahmen eines Vollstreckungsverfahrens wegen eines Ausbaubeitragsbescheides hat die Gemeindekasse bei der OFD – ZBV – angefragt, von welcher Stelle der Beschwerdeführer seine Rente beziehe. Die OFD hat dies der Gemeindekasse mitgeteilt. Der Beschwerdeführer wandte sich auch deshalb gegen die Datenübermittlung, weil er Widerspruch gegen die Vollstreckungsmaßnahmen und gegen den zugrundeliegenden Bescheid eingelegt hatte.

Der Prüfung der hier in Rede stehenden Datenübermittlung war § 31 LDSG zugrunde zulegen. Für Beamte wäre § 102 d Abs. 2 LBG i. V. m. § 102 Abs. 1 vorrangig anzuwenden. Für den Beschwerdeführer als Angestellten im Ruhestand gilt jedoch die beamtenrechtliche Vorschrift dann nicht, wenn und soweit § 31 LDSG eine Regelung enthält.

Im vorliegenden Fall war § 31 Abs. 2 LDSG anzuwenden. Diese Bestimmung betrifft nach ihrem Wortlaut zwar nur Übermittlungen an andere als öffentliche Stellen, sie regelt also ausdrücklich nur Übermittlungen an private Stellen. Wenn Datenübermittlungen aber an private Stellen zulässig sind, sind sie – unter den gleichen Voraussetzungen – erst recht auch an öffentliche Stellen als Datenempfänger zulässig.

Hier kam die Regelung in Betracht, wonach die Übermittlung personenbezogener Beschäftigtendaten (auch von Ruhestandsbeschäftigten) zulässig ist, soweit die empfangende Stelle ein rechtliches Interesse darlegt und überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen (§ 31 Abs. 2 Nr. 5 LDSG). Das Vollstreckungsinteresse der Gemeindekasse ist als rechtliches Interesse zu qualifizieren: Seine Durchsetzung ist mit Hilfe rechtlich geregelter Verfahren möglich.

Das Interesse des Betroffenen, den Vollstreckungsmaßnahmen zu entgehen, war nicht als überwiegend schutzwürdig anzusehen. Seine schutzwürdigen Interessen konnte er vielmehr im Vollstreckungsverfahren mit den dort rechtlich vorgesehenen Möglichkeiten (Rechtsbehelfen) zur Geltung bringen. Diese Möglichkeiten hatte er zudem bereits im Verfahren gegen den vollstreckbaren Bescheid. Seine Einlassung, vor Bescheidung seines Widerspruchs sei die Inanspruchnahme gerichtlicher Hilfe nicht möglich, war nicht nachvollziehbar. Die Datenübermittlung war zulässig, der Beschwerdeführer mußte entsprechend beschieden werden.

17.8 Bescheinigungen über die Notwendigkeit der ärztlichen Behandlung während der Arbeitszeit

Eine Stadtverwaltung hatte ein Formular entwickelt, in dem der behandelnde Arzt bescheinigen sollte, warum es notwendig war, während der Arbeitszeit den Arzt aufzusuchen. Bedienstete stellten die Frage, ob die Aufbewahrung dieser Bescheinigungen und deren Nutzung für spätere Kontrollen durch das Personalamt zulässig sei.

Der LfD stellte hierzu fest: Die Wahrnehmung von Aufsichts- und Kontrollbefugnissen stellt auch im Rahmen der Personaldatenverarbeitung keine Zweckänderung dar (§ 13 Abs. 3 LDSG ist auf die Vorgänge, die in § 31 Abs. 1 LDSG geregelt sind, anwendbar). Damit wäre es grundsätzlich zulässig, die in Rede stehenden Bescheinigungen auch zum Zwecke der Kontrolle zu nutzen.

Davon zu unterscheiden ist aber, ob diese Bescheinigungen nicht kurzfristig zu vernichten bzw. den Betroffenen zurückzugeben sind. Für die Löschung von Personaldaten gilt – soweit nicht § 102 f LBG anzuwenden ist – § 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 Erforderlichkeit 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 (§ 19 Abs. 2 Nr. 2 LDSG).

Vor diesem Hintergrund ist es nicht ausgeschlossen, im Interesse auch einer Kontrolle des jeweils abzeichnenden Vorgesetzten, die Aufbewahrung der Bescheinigungen für eine bestimmte Zeit vorzuschreiben. Die entsprechende Frist müßte allerdings generell festgelegt werden und sich im Rahmen der Verhältnismäßigkeit halten. Im Rahmen der Personaldatenverarbeitung hat der LfD den Schluß des laufenden Kalenderjahres für einen vertretbaren Vernichtungszeitpunkt gehalten.

Im Rahmen der Verhältnismäßigkeitsprüfung wäre dann allerdings auch zu erwägen, ob es nicht ausreichen würde, entsprechend der beihilferechtlichen Regelung eine Pflicht der Bediensteten zu begründen, die ärztlichen Bescheinigungen zum Zweck der nachträglichen Kontrolle noch für eine zu bestimmende Frist bei sich aufzubewahren.

Wenn eine solche allgemeine Regelung nicht besteht, ist auf der Grundlage des Erforderlichkeitsgrundsatzes davon auszugehen, daß die Bestätigung durch den Vorgesetzten, eine entsprechende Bescheinigung habe vorgelegen, grundsätzlich die weitere Aufbewahrung entbehrlich macht.

Die Stadtverwaltung wurde in diesem Sinn unterrichtet.

17.9 Zulässige Datenerhebungen durch den Arbeitgeber bei Kuranträgen

Eine öffentliche Stelle des Landes, die ausschließlich Angestellte beschäftigt, verlangte, daß bei der Kurbeantragung der Personalabteilung eine ärztliche Bescheinigung mit Diagnose vorgelegt werden sollte.

Die Datenverarbeitung dieser Stelle bei Dienst- und Arbeitsverhältnissen war nach § 31 LDSG zu beurteilen. Danach dürfen personenbezogene Daten von Beschäftigten nur erhoben werden, soweit dies zur Abwicklung des Dienst- oder Arbeitsverhältnisses erforderlich ist oder eine Rechtsvorschrift dies erlaubt.

Wenn ein Bediensteter eine Kur ohne Anrechnung auf den Urlaub antreten wollte, waren folgende Unterlagen (insbesondere in Anwendung der geltenden tarifvertraglichen Regelungen) vorzulegen:

- Befürwortung durch den Amtsarzt;
- Bewilligungsbescheid des gesetzlichen Rentenversicherungsträgers oder einer Krankenkasse im Rahmen der Krankenhilfe oder Genesendenfürsorge oder des Versorgungsamts bei einem Schwerbeschädigten.

Es war und ist nicht erforderlich, daß die ärztliche Bescheinigung Angaben zur Krankheit des Bediensteten sowie zu Besserungsmöglichkeiten durch Kur enthält. Diese Angaben könnten nur den Sinn haben, dem Arbeitgeber eine Überprüfung der ärztlichen Bescheinigung auf Richtigkeit zu ermöglichen. Eine solche Überprüfung wäre im Regelfall, wenn kein besonderer Anlaß besteht, nicht geboten. Damit war die Erhebung dieser Informationen datenschutzrechtlich unzulässig.

In diesem Sinn wurde die öffentliche Stelle unterrichtet, die entsprechend verfahren wird.

17.10 Auslagerung des Beihilfeverfahrens auf Privatunternehmen

Ein Beamter wandte sich dagegen, daß sein Dienstherr (eine Gemeinde) bei der Bayerischen Versicherungskammer eine sogenannte „Beihilfeversicherung" abgeschlossen hatte und seine Beihilfeanträge deshalb von der Pfälzischen Pensionsanstalt in Bad Dürkheim bearbeitet würden, die insoweit als Geschäftsstelle der Bayerischen Versicherungskammer tätig wurde.

Ausweislich der Versicherungsbedingungen handelte es sich im vorliegenden Fall um eine Beihilferückdeckungsversicherung, da der Gegenstand des Versicherungsschutzes sich auf die Verpflichtung des Versicherungsnehmers (Kommune als Dienstherr) zur Gewährung von Beihilfen zu den in Krankheits-, Geburts- und Todesfällen erwachsenen Aufwendungen beschränkte (vgl. § 1 Abs. 1 AVB/BV).

Nach den Versicherungsbedingungen war es möglich, daß die PPA als Geschäftsstelle der Bayerischen Beamtenkrankenkasse in der Pfalz Beihilfeleistungen unmittelbar im Namen des Dienstherrn „Kommune" an den Beamten erbrachte.

In der Praxis wurden die Beihilfeanträge durch die Beschäftigten unmittelbar an die PPA gesandt, wodurch für den Dienstherrn der Vorteil entstand, keine Beihilfeakten selbst führen zu müssen. Ein Nebeneffekt dieses Verfahrens war die Erfüllung der Verpflichtungen aus § 102 a Sätze 2 und 3 LBG, wonach Beihilfeakten von den übrigen Personalunterlagen getrennt aufzubewahren sind und in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden sollen.

Die PPA übersandte den Beamten unter Rückgabe der eingereichten Belege eine Mitteilung über die Berechnung. Auf dem von der PPA vorgelegten Muster fehlte allerdings der Hinweis, daß es sich um eine namens und im Auftrag der Kommune erstellte Abrechnung handele. Bei den Beihilfeberechtigten konnte der Eindruck entstehen, mit der Änderung des Verfahrens sei auch eine Rechtsänderung verbunden. Bei der PPA werden künftig aber entsprechend geänderte Formulare eingesetzt werden.

Danach handelt es sich bei der Tätigkeit der PPA überwiegend um technische Erfüllungshilfe, nicht dagegen um die Übertragung einer gesamten Aufgabe zur eigenverantwortlichen Erledigung durch die PPA, die nur im Wege der Delegation oder des Mandats und damit auf der Grundlage einer gesetzlichen Regelung zulässig wäre. Der Umfang der im 14. Tb. genannten Fälle einer Entscheidung durch die beauftragte Stelle konnte von der PPA zwar nicht beziffert werden, aber es handele sich um wenige Fälle. In dem Massenverfahren „Beihilfeberechnung" können diese Einzelfälle hingenommen werden, da nach Widerspruch die Letztentscheidung bei der Kommune verbleibt.

Die technische Erfüllungshilfe bedingt, daß datenschutzrechtlich zu ihrer Durchführung ein Auftragsverhältnis im Sinne des § 4 LDSG begründet wird. Dies ist im Bereich des Beihilfeverfahrens erfolgt. Gesichtspunkte, die gegen die Zulässigkeit der Auftragserteilung sprechen, waren nicht ersichtlich.

Selbstverständlich ist, daß der Auftragnehmer (die PPA) die im Rahmen der Auftragsdatenverarbeitung erhaltenen Daten nur zum Zweck der Auftragserfüllung verwenden darf. Andere Zwecke, etwa auch die der Werbung für andere Tätigkeitsfelder der PPA, dürfen mit diesen Daten nicht verfolgt werden. Allein die Verwendung eines Briefkopfes der PPA mit der Angabe sonstiger Tätigkeitsfelder erfüllt diesen Begriff der zweckändernden Verwendung zu Werbungszwecken allerdings nicht.

Der LfD hat seine Auffassung, wonach die hier vorliegende Datenverarbeitung zulässig war, dem Beschwerdeführer mitgeteilt.

17.11 Anforderungen an Mitarbeiterbefragungen

Der LfD wurde in mehreren Fällen gefragt, unter welchen Voraussetzungen behördliche Organisations- bzw. Arbeitsplatzuntersuchungen zulässig sind, in deren Verlauf die Mitarbeiter auch über ihre subjektive Einschätzung zu ihrem Wohlbefinden, zu Vorgesetzten und zu sonstigen dienstlichen Belangen befragt werden sollten.

Der LfD ging dabei von folgenden Grundsätzen aus:

a) Organisations- und Arbeitsplatzuntersuchungen dürfen schon wegen des haushaltsrechtlichen Grundsatzes der Sparsamkeit und Wirtschaftlichkeit nicht verhindert werden. Nach § 31 Abs. 1 LDSG ist es zulässig, Daten Bediensteter zu erheben, wenn dies zur Durchführung organisatorischer Maßnahmen erforderlich ist. Die genannten Untersuchungen dienen dem Zweck, Organisationsverbesserungen durchzuführen.

b) Die Mitwirkungspflicht der Beamten an solchen Befragungen ergibt sich aus der beamtenrechtlichen Gehorsamspflicht; die Mitwirkungspflicht der Arbeitnehmer ist als individualrechtliche Nebenpflicht aus dem Arbeitsvertrag anzusehen (vgl. LAG Frankfurt vom 26. Januar 1989, CR 1990, 274).

c) Soweit subjektive Einschätzungen einzelner Beschäftigter erfragt werden, gelten grundsätzlich die gleichen Gesichtspunkte. Solche Fragen haben sich jedoch in besonderer Weise unter Berücksichtigung des Übermaßverbots am Erforderlichkeitsgrundsatz zu orientieren; sie können leicht das unantastbare Zentrum der informationellen Selbstbestimmung tangieren; zudem dürfte bei personenbezogener Befragung dann die Gefahr unehrlicher Antworten bestehen, wodurch die Eignung (als Teil des Verhältnismäßigkeitsprinzips) einer solchen Untersuchung zweifelhaft würde, wenn diese Fragen von den Betroffenen als unverhältnismäßiger Eingriff in ihre Persönlichkeitssphäre empfunden würde.

17.12 Herausgabe von Personalakten an die Staatsanwaltschaft

Ein Beschwerdeführer trug vor, in seiner Eigenschaft als Polizeibeamter werde gegen ihn sowie gegen zwei weitere Kollegen ein Strafverfahren wegen des Verdachtes der Körperverletzung im Amt durchgeführt.

Bei der Einsicht in die Verfahrensakte habe er festgestellt, daß die Staatsanwaltschaft die Personalakten der drei Beamten zur Durchführung weiterer Ermittlungen angefordert habe. Diese seien auch an die Staatsanwaltschaft übersandt worden und befänden sich dort immer noch bei den Verfahrensakten. Er wandte sich gegen die Überlassung der gesamten Personalakte an die Staatsanwaltschaft, insbesondere deshalb, weil er der Auffassung war, daß dies zur Prüfung des Strafvorwurfes keinesfalls erforderlich sei.

Die Staatsanwaltschaft war gegenteiliger Auffassung. Seitens des Polizeipräsidiums konnte aufgrund des Anforderungsschreibens der Staatsanwaltschaft keine Beschränkung auf Teile der Akte vorgenommen werden, da nicht erkennbar war, welche Ermittlungen seitens der Staatsanwaltschaft nach Übersendung der Akten beabsichtigt waren.

Gemäß § 102 Abs. 1 Satz 2 LBG dürfen Personalakten nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden, es sei denn, der Beamte willigt in die anderweitige Verwendung ein, eine gesetzliche Vorschrift sieht die Übermittlung zu anderen Zwecken vor oder die Voraussetzungen des § 102 d Abs. 2 Satz 1 LBG sind gegeben.

Danach ist § 102 d LBG keine abschließende Vorschrift für die Datenübermittlung aus Personalakten. Andere gesetzliche Vorschriften vermögen ebenfalls solche Übermittlungen zu rechtfertigen. Als eine solche andere gesetzliche Vorschrift ist im vorliegenden Zusammenhang § 161 StPO anzusehen. Danach kann die Staatsanwaltschaft zum Zweck der Erforschung des Sachverhalts beim Verdacht einer Straftat von allen öffentlichen Behörden Auskunft verlangen. Die Behörden sind verpflichtet, dem Ersuchen der Staatsanwaltschaft zu genügen.

§ 161 StPO ist insofern eine gegenüber § 102 d LBG vorrangige Vorschrift. Sie besitzt auch gegenüber § 14 Abs. 2 LDSG Vorrang, woraus sich ergibt, daß die aktenübersendende Stelle keine Überprüfungsbefugnis bezüglich der Erforderlichkeit der Aktenvorlage zu Strafverfolgungszwecken hat.

Allerdings steht das Verlangen nach Vorlage der gesamten Personalakten durch die Staatsanwaltschaft unter dem verfassungsrechtlichen Vorbehalt, daß es mit Blick auf die Rechte des betroffenen Beamten an der Vertraulichkeit der Personalakten (und damit in bezug auf sein Grundrecht auf informationelle Selbstbestimmung) verhältnismäßig sein muß.

Eine Beurteilung dieser Frage würde die Kenntnis sowohl der Strafverfahrensakten wie der Personalakte voraussetzen. Eine entsprechende konkrete Prüfung konnte der LfD im hier zugrundeliegenden Fall noch nicht vornehmen, da das Strafverfahren nach wie vor noch nicht abgeschlossen ist. Der LfD wird nach Abschluß des Strafverfahrens eine konkrete Prüfung durchführen.

17.13 Die Verbreitung von Beförderungs- und Versetzungslisten innerhalb einer großen Behörde

Ein Polizeibeamter legte eine umfangreiche Personalliste vor, in der 52 Bewerber um Beförderungsstellen mit Geburtsdatum, Eintrittsdatum, Prüfungsdatum und -note, Daten der letzten drei Beförderungen und der Note der jeweils letzten Beurteilung aufgeführt waren. Er erklärte, diese Liste kursiere in seiner Behörde, und er wolle wissen, ob dies rechtmäßig sei.

Es stellte sich heraus, daß im Zusammenhang mit dem hier betroffenen Beförderungsverfahren eine Vielzahl verwaltungsgerichtlicher Klagen anhängig geworden war. Die Bezirksregierung hatte die Bewerberliste im Zusammenhang mit den Konkurrentenklagen auf Anordnung des Verwaltungsgerichts diesem überlassen. Eine Weitergabe der Liste durch die Bezirksregierung an die Antragsteller oder die Beigeladenen der entsprechenden Verwaltungsstreitverfahren war nicht erfolgt.

Der LfD ließ sich die entsprechenden Anforderungsschreiben des Verwaltungsgerichts in Kopie vorlegen. Danach hatte das Verwaltungsgericht sich „die Besetzungsakte" bzw. „die vollständigen einschlägigen Akten und Verwaltungsvorgänge im Original" vorlegen lassen. Die fragliche Personalliste befand sich in den Stellenbesetzungsakten, die im Zusammenhang mit der Besetzung der streitbefangenen Stellen entstanden waren.

Die Bezirksregierung hatte in diesem Zusammenhang keine Möglichkeit, die Vorlage zu verweigern. Die Verwendung der Akten beim Verwaltungsgericht unterlag und unterliegt nicht der Kontrollkompetenz des LfD. Die Gerichte sind, soweit sie rechtsprechende Tätigkeit ausüben und in diesem Zusammenhang Daten verarbeiten, ausdrücklich aus der Zuständigkeit des LfD ausgenommen (§ 24 Abs. 2 LDSG). Unabhängig davon war darauf hinzuweisen, daß gem. § 100 VwGO die Beteiligten einen Einsichtsanspruch in die Gerichtsakten und die dem Gericht vorgelegten Akten besitzen. Sie konnten sich durch die Geschäftsstelle des Gerichts auf ihre Kosten Ausfertigungen, Auszüge und Abschriften erteilen lassen.

Soweit die an dem Rechtsstreit Beteiligten Unterlagen, die personenbezogene Daten Dritter enthalten, genutzt haben, hatte dies allerdings ebenfalls im Rahmen der gesetzlichen Vorschriften zu erfolgen. Die Nutzung durfte insbesondere nicht zu einer Verletzung des allgemeinen Persönlichkeitsrechts der Betroffenen führen. Diesbezüglich existiert aber, wenn es sich bei den nutzenden Personen um Private handelt, die die Daten nicht geschäftsmäßig verarbeiten, keine staatliche Aufsicht. Etwaige Ansprüche mußten vielmehr auf dem Zivilrechtsweg unmittelbar gegen die Betroffenen geltend gemacht werden.

Der LfD konnte den Betroffenen nicht weitergehend unterstützen.

17.14 Veröffentlichung von Personaldaten aus einem Dienstordnungsverfahren

Der Beschwerdeführer war vor seiner Ruhestandsversetzung als Erster Kreisbeigeordneter eines Landkreises im Dienst. Zu seinem Geschäftsbereich gehörte u. a. der Abfallwirtschaftsbetrieb. Im Zusammenhang mit der Erweiterung einer Deponie war es zu beträchtlichen Mehrforderungen der beteiligten Baufirmen gekommen. Daraufhin entspann sich in den zuständigen Gremien des Landkreises, aber auch in der Öffentlichkeit eine Diskussion über die Verantwortung für diese finanziellen Belastungen. Im Zuge dieser sich wesentlich auch in der Tagespresse abspielenden Diskussionen erklärte der Beschwerdeführer öffentlich, er wolle eine Selbstanzeige gegen sich erstatten, um im Rahmen eines Dienstordnungsverfahrens den Vorwürfen, er habe bei dem Management des Deponiebaus Fehler begangen, zuvorzukommen. Diese Selbstanzeige erfolgte jedoch nicht, da durch eine zeitnahe Verfügung des Landrates gegen den Beschwerdeführer dienstordnungsrechtliche Vorermittlungen eingeleitet wurden.

Nach einiger Zeit legte die Vorermittlungsführerin das wesentliche Ergebnis der Vorermittlungen dem Landrat vor. Der Beschwerdeführer verweigerte sein Einverständnis zur Bekanntgabe des Ergebnisses der Vorermittlungen an Stellen außerhalb der Personalverwaltung.

In den „Kreisinformationen" wurden daraufhin unter der Überschrift „Vorermittlungsbericht liegt vor, erster Kreisbeigeordneter belastet – Landrat entlastet" folgende Informationen veröffentlicht:

„Der Vorermittlungsbericht konkretisiert, belegt und erhärtet den Verdacht gegen den Beigeordneten und den damaligen Abfallwirtschafts-Amtsleiter, für die Sach- und Finanzprobleme beim Bau der Deponie dienstrechtlich verantwortlich zu sein. . . . Nach Eingang der rechtlich verbrieften abschließenden Stellungnahme zum Vorermittlungsbericht durch die Betroffenen wird der Landrat seine weiteren Entscheidungen nach dem Dienstordnungsgesetz treffen."

Die Kreisverwaltung hat darauf hingewiesen, daß die öffentliche Diskussion der Vorgänge auch durch Zutun des Beschwerdeführers selbst entstanden sei; darüber hinausgehende Erkenntnisse aus den Vorermittlungen seien seitens des Dienstvorgesetzten nicht nach außen gegeben worden. Eine Übermittlung von „Personal-Aktendaten" im Sinne des § 102 Abs. 1 Satz 2 LBG habe nicht vorgelegen.

Der LfD hat die Angelegenheit wie folgt beurteilt:

Zunächst war davon auszugehen, daß die öffentliche Diskussion über die erheblichen Mehraufwendungen beim Bau der Deponie ohne Zutun der Kreisverwaltung entstanden war. Die Frage nach der politischen Verantwortung für diese Mehraufwendungen, die in der Öffentlichkeit gestellt wurde, zeigte, wie groß das öffentliche Interesse an den dienstlichen Vorgängen im Zusammenhang mit dieser Deponieerweiterung war und welche Bedeutung dieser Diskussion für die Kreisverwaltung insgesamt zukam.

Die Information der Öffentlichkeit darüber, daß ein Dienstordnungsverfahren gegen den Beschwerdeführer durchgeführt wurde, war angesichts dieses Sachverhalts zulässig.

Die Information der Öffentlichkeit über das Ergebnis des Vorermittlungsberichtes vor Abgabe einer Stellungnahme der Betroffenen selbst gegenüber dem Landrat war allerdings unzulässig. Dies verstieß gegen den Grundsatz der Vertraulichkeit von Personalangelegenheiten. Aus datenschutzrechtlicher Sicht wäre es zwar zulässig gewesen, in einem Fall wie dem vorliegenden die Öffentlichkeit über den Erlaß einer Dienstordnungsverfügung oder über die Einleitung des förmlichen Dienstordnungsverfahrens zu unterrichten, auch wenn es sich bei diesen Entscheidungen um Vorgänge handelt, die dem Grundsatz der Vertraulichkeit der Personalangelegenheiten unterliegen. Insoweit hätte aber das öffentliche Interesse daran, über die angemessene Ahndung von öffentlich bekanntgewordenen Dienstverfehlungen informiert zu werden (§ 4 Abs. 1 und 2 Landespressegesetz), Vorrang gehabt. Dies gilt insbesondere dann, wenn durch fehlerhaftes Verwaltungshandeln ein Schaden in der hier in Rede stehenden Höhe entstanden ist.

Vor einer solchen Entscheidung des Dienstvorgesetzten allerdings, die in Kenntnis der Stellungnahme des Betroffenen selbst ergehen muß (§ 26 Abs. 4 DOG), verstößt eine Veröffentlichung von internen Überlegungen, die noch nicht zu einer abschließenden Überzeugungsbildung des Dienstvorgesetzten selbst geführt haben, gegen überwiegende schutzwürdige Belange des Betroffenen.

In diesem Sinne hat der LfD den Beschwerdeführer sowie den Landrat unterrichtet.

17.15 Die Aufnahme von Pfändungsverfügungen in die Personalakte

Der LfD hatte anläßlich einer Eingabe zu beurteilen, ob es zulässig ist, daß die personalaktenführende Dienststelle Informationen über die Gehaltspfändung (Kopie der Drittschuldnererklärung der ZBV) in die Grundakte aufnimmt, obwohl der Vollstreckungsgläubiger bescheinigt hatte, daß der zugrundeliegende Titel zurückgenommen worden war.

Der LfD hat dies wie folgt beurteilt: Mit der Dienstbehörde stimmte er darin überein, daß Informationen über Pfändungen unabhängig von der Höhe der gepfändeten Beträge der personalaktenführenden Stelle zugeleitet werden dürfen. Insoweit hat bereits die Datenschutzkommission seinerzeit mit der ZBV Einvernehmen erzielt. Die Pfändungs- und Einziehungsverfügungen dürfen demnach also nicht nur bei der ZBV zu den Besoldungsunterlagen genommen werden; eine Kopie der Drittschuldnererklärung kann an die Personaldienststelle des Betroffenen übersandt werden. Hintergrund war, daß der Personaldienststelle die Prüfung ermöglicht werden soll, ob sich der Bedienstete in ernsthaften finanziellen Schwierigkeiten befindet. Dies ist dienstlich unter den Gesichtspunkten bedeutsam, ob der Beamte insbesondere bei der Ausübung kassenwirksamer Tätigkeiten möglicherweise unzuverlässig geworden ist und ob ein Dienstvergehen wegen übermäßigen Schuldenmachens vorliegt. Damit soll auch allgemein die Prüfung ermöglicht werden, ob sich der Bedienstete nicht außerhalb des Dienstes in einer Weise verhalten hat, die dem Ansehen des Dienstherrn abträglich sein könnte.

Diese Gesichtspunkte begründen also eine Prüfungspflicht des Dienstherrn, ob ein Dienstordnungsverfahren einzuleiten ist oder ob sonstige dienstliche Konsequenzen geboten sind.

Die Durchführung der o. g. Prüfungen begründet auch die Notwendigkeit der Aufbewahrung der entsprechenden Unterlagen bis zu deren Abschluß (§ 31 Abs. 1 LDSG).

Es kann dahinstehen, ob diese Prüfungen im Rahmen eines Dienstordnungsverfahrens im Wege von Vorermittlungen zu erfolgen haben oder ob Verwaltungsermittlungen gegen einen bestimmten Bediensteten zulässig sind. Die Auffassung, daß Verwaltungsermittlungen gegen einen bestimmten namentlich bekannten Beamten unzulässig sind, wird allerdings mit zutreffenden Gründen von Bartel, RiA 85, 254, vertreten.

Die Frage, in welchen Akten der Dienstbehörde die diesen Prüfungszwecken dienenden Unterlagen wie lange aufzubewahren sind, war wie folgt zu beantworten:

Die Unterlagen sind dann, wenn Verwaltungsermittlungen geführt werden, zunächst in eine Sachakte zu nehmen. Wenn dienstordnungsrechtliche Vorermittlungen geführt werden, ist ein Dienstordnungsheft anzulegen. Die dafür geltenden Aufbewahrungsbestimmungen enthält das Dienstordnungsgesetz. Wenn nur allgemeine dienstliche Konsequenzen geprüft werden, kann die Aufnahme in die Personalakten erfolgen.

Nach Abschluß der Verwaltungsermittlungen ist eine Entscheidung darüber zu treffen, ob das Dienstordnungsverfahren eingeleitet wird. Wenn das Dienstordnungsverfahren eingeleitet wird, sind die Aktenvorgänge zu einem Dienstordnungsheft zu nehmen und entsprechend den Vorgaben des Dienstordnungsgesetzes aufzubewahren.

Ansonsten sind die Vorgänge gem. § 102 e Abs. 1 Nr. 1 LBG sofort, wenn sich die Rechtswidrigkeit des Pfändungsvorgangs ergeben hat, ansonsten gem. § 102 e Abs. 1 Nr. 2 LBG nach zwei Jahren auf Antrag des Beamten zu vernichten.

17.16 Datenerhebungen durch die ZBV im Hinblick auf Kindergeld und Ortszuschlag

Ein Angestellter trug folgenden Sachverhalt vor: Er selbst habe eine Aufforderung der ZBV erhalten, den Fragebogen zur Überprüfung der Anspruchsvoraussetzungen für die Zahlung des Kindergeldes und/bzw. kinderbezogenen Anteils im Ortszuschlag oder Sozialzuschlages für über 18 Jahre alte Kinder für das Jahr 1996 und zur Weiterzahlung ab dem 1. Januar 1997 auszufüllen.

Er war der Auffassung, diese Aufforderung an ihn persönlich sei unrechtmäßig erfolgt, da er für seine Tochter weder Kindergeld noch kinderbezogenen Ortszuschlag erhalte. Auch als Zählkind hätte seine Tochter in seinem Fall keine Auswirkung auf seine Besoldung.

Die ZBV teilte diese Auffassung. Der Beschwerdeführer sei irrtümlich angesprochen worden, weil der automatisiert gespeicherte Datenbestand der ZBV automatisiert ausgewertet worden sei. Dabei seien alle diejenigen Bezügeempfänger unter Übersendung eines Fragebogens zur Überprüfung der Anspruchsvoraussetzungen für die Zahlung des Kindergeldes und/bzw. kinderbezogenen Anteils im Ortszuschlag oder Sozialzuschlages für über 18 Jahre alte Kinder angeschrieben worden, bei denen Kinder diesen Alters im Datensatz gespeichert worden sind.

Dies habe dazu geführt, daß auch solche Bezügeempfänger zur Datenpreisgabe aufgefordert wurden, für deren Kinder kein Kindergeld gezahlt wird und deren Kinder auch nicht als „Zählkinder" in Betracht kommen. Der LfD stellte fest, daß die Aufforderung zur Datenpreisgabe in Fällen, in denen dies zur Aufgabenerfüllung nicht erforderlich war, datenschutzrechtlich unzulässig war. Es waren alle Vorkehrungen zu treffen, die technisch und organisatorisch möglich sind, um dies auszuschließen. Der LfD hat die OFD Koblenz – ZBV – aufgefordert, ihr Auswertungsverfahren künftig entsprechend umzugestalten.

Ob diesem Anliegen technische oder sonstige Hinderungsgründe entgegenstehen, wird derzeit noch geprüft.

Grundsätzlich vertritt der LfD allerdings die Auffassung, daß die Nutzung der Datenbestände der ZBV unter Einschluß der Angaben zu Kindern auch zum Zweck der Durchführung des Kindergeldverfahrens zulässig ist. Die Daten der ZBV werden auch zu dem Zweck gespeichert, die steuerrechtlichen Pflichten des Arbeitgebers zu erfüllen. Durch die Kopplung des Kindergeldverfahrens mit dem einkommensteuerrechtlichen Verfahren ist die Nutzung der Kindergelddaten wie die der sonstigen zu steuerlichen Zwecken gespeicherten Personaldaten zu beurteilen.

Der Beschwerdeführer trug weiter vor, auch die vergleichbare Befragung seiner Ehefrau sei rechtswidrig gewesen. Diese beziehe zwar Kindergeld und Ortszuschlag für ihre Tochter. Es bestehe aber kein ausreichender Anlaß, die verlangten Erklärungen zu fordern, da sie einen Bescheid erhalten habe, wonach bis zu einem bestimmten Termin Kindergeld gewährt werde. Überprüfungen der Rechtmäßigkeit von Zahlungen innerhalb dieses Zeitraumes dürften nur aus begründetem Anlaß erfolgen, der hier nicht vorliege.

Diese Auffassung hat der LfD nicht geteilt. Aus seiner Sicht bestand ein begründeter Anlaß für das Verlangen von Auskünften.

Ein solcher Anlaß besteht nämlich nicht nur dann, wenn der Kindergeldantrag geprüft und beschieden wird. Im Zeitpunkt der Bescheidung des Kindergeldantrages, der auf die Zukunft gerichtet ist, wird jeweils eine Prognose über das zu erwartende Einkommen des jeweiligen Kindes abgegeben. Jeweils nach Ablauf des steuerrechtlich und damit auch kindergeldrechtlich relevanten Zeitraumes (Kalenderjahres) besteht Anlaß zu überprüfen, ob sich die ursprünglich gestellte Prognose über das Einkommen des Kindes als zutreffend erwiesen hat. Insoweit ist die Kindergeldstelle berechtigt, den Bezügeempfänger zu Auskünften aufzufordern.

Auch die Verwendung des von der OFD – ZBV – eingesetzten Formblattes in diesem Zusammenhang begegnet aus datenschutzrechtlicher Sicht keinen Bedenken.

Nach dem nunmehr geltenden Kindergeldrecht können nämlich nicht nur Einkünfte aus nichtselbständiger oder selbständiger Arbeit relevant sein, sondern ebenso Einkünfte aus Kapitalvermögen, aus Gewerbebetrieb oder sonstige Einkünfte. Damit ist allein der Nachweis, daß sich das Kind in Ausbildung befindet, für die Frage der Einkommenserzielung nicht ausreichend.

17.17 Datenschutz bei dienstlichen Telefonanlagen

Folgende Fragen zum Datenschutz bei dienstlichen Telefonanlagen hatte der LfD zu beantworten:

a) Darf der Einzelverbindungsnachweis der Telekom zur Gebührenverwaltung dienstlicher Telefonanschlüsse genutzt werden?

Der Einzelgebührennachweis der Telekom enthält Informationen über Zeitpunkt, Zeitdauer sowie Rufnummer des angerufenen Gesprächpartners, verkürzt um die letzten drei Ziffern.

Soweit die dienstlichen Telefonate davon betroffen sind, bestehen keine datenschutzrechtlichen Bedenken gegen die Nutzung dieses Einzelverbindungsnachweises zur Kontrolle und zu Abrechnungszwecken.

Soweit es gestattet ist, von dienstlichen Apparaten aus Privatgespräche zu führen, wären in einer solchen Auflistung allerdings auch Privatgespräche enthalten. Damit auch unter dieser Voraussetzung eine Nutzung durch die Dienststelle datenschutzverträglich wäre, müßten Vorkehrungen getroffen werden, damit die Privatgesprächsdaten grundsätzlich nur zweckentsprechend (d. h. im Regelfall also nur zu Abrechnungszwecken) genutzt werden. Dies ist allerdings durch technische und organisatorische Maßnahmen durchaus erreichbar. So könnte eine denkbare Verfahrensweise sein, daß jeder Anschlußinhaber den Einzelgebührennachweis unmittelbar von der Posteingangsstelle erhält, ohne daß eine andere Person oder Stelle diesen Gebührennachweis vorher bearbeitet hat. Der Anschlußnutzer könnte dann die Verbindungsdaten der Privatgespräche bis auf die jeweils angefallenen Gebühren schwärzen. Daraus ließe sich ohne Probleme errechnen, in welchem Umfang Ersatz für Privatgespräche zu leisten ist. Die dienstlichen Gespräche wären ungeschwärzt zu lassen. Der so bearbeitete Gebührennachweisbogen könnte dann auf dem üblichen Weg über die Abrechnungsstelle geleitet werden.

Sicher ließen sich auch andere Verfahrensweisen mit einer gleichen oder ähnlichen Wirkung entwickeln.

Zur Frage der Mitbestimmung in diesem Zusammenhang hat der LfD ausgeführt, daß aus seiner Sicht die Nutzung des Einzelverbindungsnachweises der Telekom als ein Verfahren anzusehen sei, das geeignet ist, Daten von Beschäftigten zu verarbeiten oder zu nutzen (§ 80 Abs. 1 Nr. 2 Landespersonalvertretungsgesetz). Bei der Einführung eines solchen Verfahrens habe deshalb der Personalrat mitzubestimmen.

Bei der zulässigen Führung von Privatgesprächen haben die Mitarbeiter selbstverständlich ein Recht darauf, darüber unterrichtet zu werden, auf welchem Wege ihre Privatgespräche erfaßt und abgerechnet werden.

Die Aufbewahrungsdauer der Einzelverbindungsnachweise richtet sich nach den in der hierzu abgeschlossenen Dienstvereinbarung getroffenen Fristen. Wenn keine Dienstvereinbarung abgeschlossen wird, ist eine entsprechende Frist in einer Dienstanweisung zu formulieren. Sowohl Abrechnungszwecke wie Dokumentationszweck dürften keine längere Aufbewahrungsdauer als etwa ein Jahr nach Entstehen der Nachweise rechtfertigen.

b) Darf die Anzeige des Anrufertelefons im Display regelmäßig erfolgen?

Die Anzeige des Anrufertelefons im Display ist davon abhängig, ob das Telefonnetz digitalisiert ist. Es ist nicht erforderlich, daß das beteiligte Telefon selbst einen ISDN-Anschluß nutzt. Die Nutzung dieses Merkmals durch öffentliche Stellen des Landes ist zulässig.

c) Was darf in amtsinterne Telefonverzeichnisse aufgenommen werden?

Wenn in diesen Verzeichnissen nur Name, Amtsbezeichnung und Anschlußnummer enthalten sind, ist die Erstellung und Nutzung eines solchen Verzeichnisses nicht abhängig von der Zustimmung der Mitarbeiter. Derartige Informationen sind primär tätigkeitsbezogen; bei öffentlich Bediensteten sind diese Informationen vom informationellen Selbstbestimmungsrecht grundsätzlich nicht umfaßt. Es liegt deshalb im Ermessen der Dienstbehörde, ob und in welchem Umfang sie solche Daten nutzt und übermittelt (vgl. 13. Tb. Tz. 17.3).

Ein Mitbestimmungsrecht des Personalrats über die Festlegung des Verteilers ergibt sich in diesem Zusammenhang aus dem Landespersonalvertretungsgesetz nicht. Nach den vorstehend genannten Überlegungen dürfte allerdings deutlich sein, daß die Frage, ob in diesem Zusammenhang ein Mitbestimmungsrecht existiert, keinen datenschutzrechtlichen Gehalt besitzt.

17.18 Auskunftspflicht der Personalverwaltung gegenüber dem Petitionsausschuß des Landtags

Auf Bitten des Bürgerbeauftragten nahm der LfD zur Frage, ob eine Behörde verpflichtet sei, dem Bürgerbeauftragten bzw. dem Petitionsausschuß Personalakten ihrer Mitarbeiter zu überlassen, wie folgt Stellung:

Die Behörde dürfte dann Personaldaten ihrer Mitarbeiter an das Parlament (den Bürgerbeauftragten oder den Petitionsausschuß) übermitteln, wenn die betroffenen Bediensteten eingewilligt hätten oder wenn eine gesetzliche Vorschrift dies rechtfertigen würde. Dies ergibt sich aus § 102 Abs. 1 Satz 2 LBG. Dort heißt es, daß Personalaktendaten nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden dürfen, es sei denn, der Beamte willigt in die anderweitige Verwendung ein, eine gesetzliche Vorschrift sieht die Übermittlung zu anderen Zwecken vor oder die Voraussetzungen des § 102 d Abs. 2 Satz 1 sind gegeben. Nach § 102 d Abs. 2 Satz 1 dürfen dann Auskünfte auch ohne Einwilligung des Beamten erteilt werden, wenn die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz höherrangiger Interessen des Dritten die Auskunftserteilung erfordert. Inhalt und Empfänger der Auskunft sind in diesen Fällen dem Beamten schriftlich mitzuteilen.

Der LfD wies darauf hin, daß er für die Beurteilung der Frage, ob der Petitionsausschuß bzw. der Bürgerbeauftragte sich für die Übermittlung dieser Informationen im vorliegenden Zusammenhang auf eine gesetzliche Vorschrift berufen konnte bzw. ob im konkreten Fall die Kenntnisnahme durch den Bürgerbeauftragten oder den Petitionsausschuß erforderlich war, um eine erhebliche Beeinträchtigung des Gemeinwohls abzuwehren oder höherrangige Interessen des Parlaments zu schützen, nicht zuständig sei. Insoweit liege die Zuständigkeit für die datenschutzrechtliche Beurteilung beim Ältestenrat des Landtages (§ 2 Abs. 2 LDSG i. V. m. § 12 der Datenschutzordnung des Landtags vom 31. Oktober 1995, GVBl. S. 467, BS 1101-7). Die Beratungsbefugnis müsse dem Umfang der Kontrollbefugnis entsprechen, damit unterschiedliche Beurteilungen vermieden werden.

17.19 Entwurf eines Landesgesetzes zur Neuregelung des Disziplinarrechts

Das Ministerium des Innern und für Sport hat den Entwurf eines völlig neu strukturierten Disziplinargesetzes vorgelegt. Dieser Entwurf enthält besondere Regelungen über die Datenerhebung beim Betroffenen, die Beweiserhebung, die Datenerhebung bei privaten Dritten im Wege der Zeugenvernehmung, die Herausgabepflicht des betroffenen Beamten in bezug auf amtliche Unterlagen, die Beschlagnahme und Durchsuchung, die Untersuchung des Beamten in einem Krankenhaus gegen seinen Willen, allgemeine Regelungen über die Beweiserhebung sowie Regelungen über die Übermittlung personenbezogener Daten durch andere öffentliche Stellen an die Disziplinarorgane; auch die Übermittlung von Informationen über das durchgeführte Disziplinarverfahren zwischen öffentlichen Dienststellen wird besonders geregelt. Schließlich enthält der Entwurf eine ergänzende allgemeine Erhebungsregelung; dort heißt es (inhaltlich übereinstimmend mit § 26 Abs. 1 Satz 1 DOG), daß nach der Einleitung des Disziplinarverfahrens die erforderlichen Ermittlungen durchzuführen sind.

Insgesamt soll also das LDSG mit seinen Erhebungs- und Übermittlungsregelungen in wesentlichen Teilen durch die genannten Vorschriften des Gesetzentwurfs ersetzt werden. Allerdings hat der LfD auf einige aus seiner Sicht bestehende Defizite hingewiesen. Die Diskussion mit dem Ministerium hierzu ist derzeit noch nicht abgeschlossen.

18. Datenschutz im kommunalen Bereich

18.1 Änderung der Kommunalwahlordnung

Mit dem Zweiten Landesgesetz zur Änderung kommunalrechtlicher Vorschriften wurde das Kommunalwahlrecht für Unionsbürger eingeführt. Die Kommunalwahlordnung war der neuen Rechtslage anzupassen. Durch eine Ergänzung von § 10 KWO sollte zugelassen werden, daß die Staatsangehörigkeit in das amtliche Wählerverzeichnis aufgenommen wird. Die Aufnahme dieses Merkmals – so die Begründung – verfolge vorrangig den Zweck, der Gemeindeverwaltung bei der Vorbereitung der Kommunalwahlen die Arbeitsabläufe zu erleichtern. Außerdem werde damit dem gesteigerten Anspruch der Unionsbürger auf Informationen entsprochen.

Der LfD sprach sich in seiner Stellungnahme zu dem Entwurf gegen die Aufnahme der Staatsangehörigkeit in das Wählerverzeichnis aus. Die für die Ergänzung genannten Gründe hielt er nicht für überzeugend. Er wies auf zusätzliche Gefährdungen von Ausländern hin, die auf gezielten Auswertungen des Wählerverzeichnisses beruhen könnten. Diese Gefährdungen hätten schließlich den Gesetzgeber veranlaßt, Gruppenauskünfte aus dem Melderegister, die das Datum Staatsangehörigkeit enthielten, nur mit Zustimmung des Ministeriums als der obersten Aufsichtsbehörde zuzulassen (§ 34 Abs. 3 MG).

Den Bedenken des LfD wurde Rechnung getragen; die Vorschrift über die Aufstellung und Form des Wählerverzeichnisses (§ 10) blieb unverändert.

18.2 Bildung von Wahlvorständen

Eine Stadt hatte Bürgerinnen und Bürger, deren Adressen im Stichprobenverfahren aus dem Melderegister entnommen worden waren, angeschrieben und gebeten, sich für eine ehrenamtliche Tätigkeit im Wahlvorstand anläßlich der Wahl des Bürgermeisters zur Verfügung zu stellen. Das Einverständnis zur Bestellung oder Hinderungsgründe sollten „auf jeden Fall" unter Verwendung eines dem Schreiben beigefügten Vordrucks mitgeteilt werden. In dem Vordruck wurden außer der Adresse das Geburtsdatum, private und berufliche Telefonanschlüsse, der höchste Bildungsabschluß und bisherige Tätigkeiten als Wahlhelfer erfragt. Für den Fall, daß ein Ablehnungsgrund nach § 19 GemO besteht, wurde um Mitteilung der Gründe gebeten.

Die Verwaltung räumte in der vom LfD angeforderten Stellungnahme ein, daß es sich um eine Datenerhebung auf freiwilliger Grundlage handelte und sicherte die genaue Beachtung der Hinweispflichten bei künftigen Befragungen dieser Art zu. Nach dem höchsten Bildungsabschluß sei deshalb gefragt worden, weil sich bei früheren Wahlen häufig gezeigt habe, daß die zu Mitgliedern des Wahlvorstandes bestellten Personen ihrer Aufgabe nicht gewachsen waren. Wenn dies erst am Wahltag festgestellt werde, sei es oftmals schwierig, noch geeignete Ersatzleute zu bestellen. Der Bildungsabschluß werde also als ein Kriterium zur Vorauswahl herangezogen.

Der LfD konnte sich dieser Argumentation nicht verschließen. Wenn die datenschutzrechtlichen Anforderungen an eine freiwillige Datenerhebung erfüllt sind, hält er es auch für zulässig, nach dem Bildungsabschluß zu fragen.

18.3 Tagesordnung von öffentlichen Gemeinderatssitzungen

In einer Eingabe an den LfD wurde beklagt, daß mit der Tagesordnung einer Sitzung des Ortsgemeinderats auch öffentlich bekanntgemacht wurde, welche Einwohner durch Vorkaufsrechtsangelegenheiten betroffen sind. Die betroffene Verwaltung vertrat die Auffassung, daß eine Behandlung derartiger Angelegenheiten in nichtöffentlicher Sitzung nach der Natur des Beratungsgegenstands grundsätzlich nicht erforderlich, also auch nicht gerechtfertigt sei. Für die in öffentlicher Sitzung zu behandelnde Tagesordnung bestehe die Veröffentlichungspflicht nach § 34 Abs. 6 GemO.

Der LfD vertrat hingegen die Auffassung, daß Vorgänge dieser Art in nichtöffentlicher Sitzung des Gemeinderats zu behandeln sind. Die öffentliche Bekanntmachung der Tagesordnung nichtöffentlicher Sitzungen soll sich nach Nummer 5 der VV zu § 34 GemO auf allgemeine Bezeichnungen der Beratungsgegenstände beschränken (z. B. Personalsachen, Grundstückssachen, Abgabensachen). Danach wäre die Veröffentlichung einer Tagesordnung mit den Anschriften von Personen, die von Vorkaufsrechtsangelegenheiten betroffen sind, nicht zulässig gewesen.

Das Ministerium des Innern und für Sport bestätigte diese Rechtsauffassung unter Hinweis auf einschlägige Entscheidungen des VG Mainz, des OVG Rheinland-Pfalz und des Bundesverwaltungsgerichts. Es wies darauf hin, daß bei der Beratung über die Ausübung des Vorkaufsrechts durch die Gemeinde in der Regel auch Einzelheiten des Kaufvertrages, insbesondere Kaufpreis, Abreden zwischen den Parteien des Kaufvertrages und Zahlungsmodalitäten zu erörtern sind. Des weiteren sei davon auszugehen, daß auch die vom Käufer beabsichtigte Nutzung Gegenstand der Beratung sein werde, weil die Gemeinde prüfen müsse, ob sie von dem Vorkaufsrecht Gebrauch machen solle, um ihre Planvorstellungen verwirklichen zu können. Eine öffentliche Beratung wäre grundsätzlich geeignet, Persönlichkeitsrechte des Eigentümers zu berühren. Darüber hinaus könnte auch die Diskussion über gemeindliche Planungsabsichten in öffentlicher Sitzung den Interessen der Gemeinde widersprechen. In aller Regel sei daher vom Vorliegen besonderer Gründe zur Beratung und Beschlußfassung über die Ausübung des gemeindlichen Vorkaufsrechts in nichtöffentlicher Sitzung auszugehen.

18.4 Unterrichtungsrechte des Gemeinderates

Die Weiterentwicklung und Stärkung der Unterrichtungs- und Kontrollrechte des Gemeinderates (§ 33 GemO) hat nicht zur Beseitigung dieses schon aus der Zeit vor der Novellierung der Gemeindeordnung bekannten Konfliktbereichs geführt. Im Gegenteil: Mehr denn je wird der LfD um die datenschutzrechtliche Beurteilung von Informationsvorgängen ersucht, deren Zulässigkeit zwischen der Gemeindevertretung und der Gemeindeverwaltung umstritten ist.

Ein Beispiel: Eine Ortsgemeinde betreibt den Bau eines Golfplatzes. Sie erstellte einen Bebauungsplan „Golfplatz" und beschloß, den Plan auszulegen und die Träger öffentlicher Belange anzuhören.

Eine Ratsfraktion beantragte hierzu nähere Informationen. Im einzelnen wollte sie wissen:

- Wer ist Eigentümer der einzelnen im Bereich des Bebauungsplans gelegenen Grundstücke?
- Welche Grundstücke hat die Ortsgemeinde seit dem 1. Januar 1991 erworben, von welchem Eigentümer und zu welchem Preis?
- Welche der seit dem 1. Januar 1991 erworbenen Grundstücke stehen als Tauschland zur Verfügung, wenn Eigentümer von Grundstücken, die vom Bebauungsplan betroffen sind, nicht verkaufen oder verpachten wollen.
- Welche Grundstücke hat die Gemeinde als Mitpächter eines Golfclubs gepachtet?
- Welchen genauen Inhalt haben die Pachtverträge?

Gegen die Bekanntgabe der Eigentümer der betroffenen Grundstücke sind keine datenschutzrechtlichen Bedenken zu erheben. Ein Umlegungsbeschluß ist in der Gemeinde ortsüblich bekanntzumachen. Bereits dadurch werden in gewissem Umfang personenbeziehbare Informationen bekanntgegeben: Durch die Bezeichnung der vom Umlegungsverfahren betroffenen Grundstücke erhält jedermann Kenntnis von deren Einbeziehung in das Umlegungsverfahren. Zwar sind die Namen der Eigentümer nicht Teil dieser Bekanntmachung; da bei der Auskunftserteilung aus dem Liegenschaftskataster und aus dem Grundbuch indessen nur an das berechtigte Interesse anfragender Personen angeknüpft wird, dürfte es für Interessenten grundsätzlich nicht ausgeschlossen sein, auch die Namen der betroffenen Grundstückseigentümer zu erfahren. Die schutzwürdigen Interessen Betroffener sind insoweit nicht sehr hoch anzusetzen; das Informationsinteresse des Gemeinderats geht deshalb vor.

Die übrigen Fragen beziehen sich auf Vertragsverhältnisse oder auf Verwaltungsverfahren. Daß das Informationsrecht des Gemeinderats nicht alle von der Gemeinde abgeschlossenen Verträge umfaßt, folgt schon daraus, daß die Auskunftspflicht nach § 33 Abs. 2 GemO nur Verträge mit ganz bestimmten Vertragspartnern umfaßt. Informationen aus Verwaltungsverfahren sind durch das Verwaltungsgeheimnis nach § 30 VwVfG geschützt.

Da die Fraktion ihr Unterrichtungsverlangen nicht näher begründete, mußte bei der nach § 33 Abs. 5 GemO gebotenen Abwägung mit den schutzwürdigen Interessen Betroffener davon ausgegangen werden, daß die Informationen für die allgemeine politische Arbeit in den Gemeindegremien verwendet werden sollten. Im Rahmen einer solchen Betrachtung überwiegen die schutzwürdigen Interessen der Betroffenen. Keine Bedenken bestehen dagegen, daß die Auskünfte in nichtpersonenbezogener Form erteilt werden, der Gemeinderat also beispielsweise über durchschnittlich gezahlte Grundstückspreise informiert wird. Nicht in diese rechtliche Beurteilung einbezogen ist die Zulässigkeit der Akteneinsicht nach § 33 Abs. 3 Satz 2 ff. GemO. Voraussetzung wäre die Begründung des Einsichtverlangens, denn nur in Kenntnis der Gründe kann beurteilt werden, ob „überwiegende" schutzwürdige Interessen entgegenstehen.

18.5 Öffentliche Berichterstattung über Ratssitzungen

Der Bürgermeister einer Ortsgemeinde veröffentlichte im Mitteilungsblatt der Verbandsgemeinde einen Auszug aus der Niederschrift über eine öffentliche Sitzung des Ortsgemeinderats. Gegenstand der Berichterstattung war die Beratung und Beschlußfassung über die Zahlung eines Räumungskostenvorschusses an den Gerichtsvollzieher für die zwangsweise Räumung einer Mietwohnung. Die Mieter wurden namentlich benannt.

Der Beratungsgegenstand hätte seiner Natur nach in nichtöffentlicher Sitzung des Ortsgemeinderats behandelt werden müssen (§ 35 Abs. 1 Satz 1 GemO). Dies war insbesondere deshalb geboten, weil es sich um einen für die persönliche Sphäre der betroffenen Mieter äußerst sensiblen Sachverhalt handelt, bei dessen Behandlung nicht nur die Nichtöffentlichkeit zu gewährleisten war, sondern der darüber hinaus, wäre er nichtöffentlich behandelt worden, der Schweigepflicht der Sitzungsteilnehmer (§ 20 GemO) unterlegen hätte. Die Veröffentlichung im Mitteilungsblatt erfolgte unter fehlerhafter Würdigung von § 41 GemO. Nach dieser Vorschrift dürfen nur die Ergebnisse der öffentlichen und nichtöffentlichen Sitzungen bekanntgemacht werden, wobei zu beachten ist, daß Angelegenheiten, die nach § 20 GemO der Schweigepflicht unterliegen, nicht veröffentlicht werden dürfen.

Die Verfahrensweise wurde als Verstoß gegen datenschutzrechtliche Vorschriften beanstandet.

18.6 Schweigepflicht von Ehrenbeamten

Der Bürgermeister einer Ortsgemeinde äußerte sich in einem Leserbrief zur Ansiedlung von Industrie- und Gewerbebetrieben. Dabei stellte er mit Personenbezug Sachverhalte dar, die ihm aus dienstlicher Veranlassung bekannt geworden waren, so beispielsweise, daß namentlich genannte Kritiker des Projekts in der betroffenen Gemeinde nur mit Nebenwohnsitz gemeldet seien, daß sie in einem persönlichen Gespräch für eine Verschiebung der Grenzen des Gewerbegebiets eingetreten seien und daß sich ein anderer namentlich genannter Kritiker des Projekts früher selbst um einen Ansiedlungsplatz bemüht habe.

In seiner Entgegnung zur rechtlichen Bewertung dieser Vorgehensweise gegenüber dem LfD wies er darauf hin, die in dem Leserbrief Genannten hätten sich wiederholt öffentlich zu dem Projekt geäußert, ihre Vorbehalte seien also allgemein bekannt gewesen. Die Sachverhaltsdarstellungen in dem Leserbrief seien offenkundig gewesen oder hätten ihrer Bedeutung nach keiner Geheimhaltung bedurft.

In der abschließenden datenschutzrechtlichen Bewertung war der Bürgermeister darauf hinzuweisen, daß es auch die von den Bürgern öffentlich vorgetragene Meinung nicht rechtfertigt, davon auszugehen, daß die in seinem Leserbrief dargestellten Sachverhalte im Verbreitungsgebiet einer Tageszeitung offenkundig sind. Es wurde ihm vorgehalten, daß er die ihm nach § 20 GemO obliegende Verschwiegenheitspflicht verletzt hatte. Von einer zulässigen Durchbrechung der Verschwiegenheitspflicht hätte nur dann ausgegangen werden können, wenn der Leserbrief dazu gedient hätte, in der gleichen Weise vorgebrachte unwahre Tatsachenbehauptungen der Betroffenen richtigzustellen. Dies war aber nicht der Fall.

18.7 Datenschutz und Familienforschung

Standesbeamte berufen sich bei der Verweigerung von Auskünften oder der Einsicht in Personenstandsbücher häufig auf den Datenschutz. Betroffen sind durch diese Verweigerung insbesondere Personen, die Familienforschung betreiben, also Auskünfte aus Personenstandsbüchern oder Einsicht erbitten, um nähere Informationen über ihre Vorfahren zu erlangen. Aber auch die übrige historische Forschung sieht sich durch die Übermittlungs- und Einsichtsrestriktionen des Personenstandsgesetzes behindert. Vor Jahren berichtete die Presse über die Ablehnung des Antrags auf Einsichtnahme in die Aufzeichnungen über den Räuberhauptmann Johannes Bückler, besser bekannt unter dem Namen Schinderhannes, der im Jahre 1803 in Mainz hingerichtet worden war. „Wie Schinderhannes unter die Datenschützer fiel" lautete die Überschrift eines vielbeachteten Beitrags in der Presse, in dem über diesen Fall eines „eindeutig überzogenen Datenschutzes" berichtet wurde. Abgesehen davon, daß die gesetzliche Vorschrift (§ 61 PStG), auf die sich der Standesbeamte – zu Recht – berief, aus einer Zeit stammt, in der noch kein Datenschutzbeauftragter Kontrollverantwortung hatte: Der Vorwurf der Forschungsbehinderung an den Datenschutz ist auch noch aus einem anderen Grunde falsch. Der Datenschutz spielt nämlich nur dann eine Rolle, wenn die Personen, auf die sich

Eintragungen in Personenstandsbüchern beziehen, noch leben oder wenn durch die Auskunftserteilung oder Einsichtgewährung schutzwürdige Belange lebender Nachkommen beeinträchtigt werden können. Datenschutz beruht auf dem Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG; dieses Recht kann, wie leicht einsichtig ist, von Verstorbenen nicht mehr ausgeübt werden. Soweit es um Eintragungen über nicht mehr lebende Personen geht, schützt § 61 PStG deren Ansehen als den über den Tod hinauswirkenden Teil der Menschenwürde (Art. 1 Abs. 1 GG). Dies wird von Standesbeamten häufig noch verkannt, und so werden Auskunftsersuchen mit dem pauschalen Hinweis auf den angeblich entgegenstehenden Datenschutz abgelehnt.

Die fehlerhafte Berichterstattung über den „Datenschutz für Schinderhannes" hatte übrigens ihr Gutes: Die Durchführungsverordnung zum Personenstandsgesetz (BS 211-2) wurde im Jahre 1981 so verändert, daß abweichend von § 61 PStG für die vor dem 1. Januar 1876 geführten Zivilstandsregister ein Einsichtsrecht begründet ist, wenn ein berechtigtes Interesse glaubhaft gemacht wird. Da Forschungsinteressen als berechtigte Interessen zu qualifizieren sind, besteht in jedem Falle ein Zugangsrecht zu Aufzeichnungen, die bis zu diesem Zeitpunkt entstanden. Für die Zeit danach gilt nach § 61 PStG, daß Einsicht in die Personenstandsbücher, Durchsicht dieser Bücher und die Erteilung von Personenstandsurkunden – außer von Behörden – nur von Personen verlangt werden kann, auf die sich der Eintrag bezieht, sowie von deren Ehegatten, Vorfahren und Abkömmlingen. Andere Personen haben diese Rechte nur dann, wenn sie ein rechtliches Interesse glaubhaft machen. Nach der Rechtsprechung gehören zu den Abkömmlingen nur die Verwandten in gerader Linie, und Forschungsinteressen können nicht als rechtliche Interessen anerkannt werden. Damit wird man den Standesbeamten keine falsche Auslegung der gesetzlichen Bestimmungen vorwerfen können, wenn sie Auskünfte oder Einsicht bei Nachkommen in der Seitenlinie oder bei fehlendem rechtlichen Interesse verweigern. Auf den Datenschutz können sie sich aber nur in den seltenen Fällen berufen, in denen die Persönlichkeitsrechte lebender Personen betroffen sind.

18.8 Unterrichtung von Nachlaßgerichten durch die Standesämter

Nach § 11 des Landesgesetzes über die freiwillige Gerichtsbarkeit haben die Standesbeamten den Nachlaßgerichten alle Todesfälle mitzuteilen, die ihnen nach § 32 PStG angezeigt werden. Dieser Mitteilungspflicht entsprechen die Standesbeamten aufgrund einer Weisung des Ministeriums des Innern und für Sport durch Übersendung einer Durchschrift der „Anzeige über Sterbefall an Finanzamt" (§ 9 Abs. 1 ErbStDV). Eine Prüfung des Inhalts dieses Vordruckes ergab, daß nicht alle im Besteuerungsverfahren notwendigen Angaben auch für die Aufgabenwahrnehmung der Nachlaßgerichte erforderlich sind. Das Ministerium der Justiz räumte ein, daß Angaben zum Beruf des Verstorbenen oder von dessen Angehörigen entbehrlich sind; soweit eine Nachlaßsicherung nicht in Betracht kommt – insbesondere dann, wenn ein überlebender Ehegatte und/oder Kinder vorhanden sind, die das Erbe in Besitz haben –, sind auch Angaben über das vorhandene Vermögen verzichtbar.

Das Ministerium des Innern und für Sport wird auf diese Einschränkungen der Datenübermittlung an die Nachlaßgerichte beim Neuerlaß einer Verwaltungsvorschrift zur Durchführung personenstandsrechtlicher Vorschriften hinweisen.

18.9 Die Ehefrau des Ortsbürgermeisters – ein Datenschutzproblem!

Nicht nur in der großen Politik, auch auf der örtlichen Ebene werden Auseinandersetzungen gelegentlich mit Datenschutzargumenten geführt. Hinweise auf tatsächliche oder vermeintliche Verstöße gegen Datenschutzvorschriften kommen nicht selten von politischen Gegnern. Bei allem Bemühen, einer Instrumentalisierung des Datenschutzes entgegenzuwirken, hat der LfD selbstverständlich auch in solchen Fällen die Pflicht zur sachlichen Prüfung und zur Stellungnahme. Eine Eingabe kann nicht deshalb zurückgewiesen werden, weil sie vermutlich zuvörderst dem Zweck dient, dem politischen Gegner etwas anzuhängen.

Eine Fraktion im Ortsgemeinderat einer kleinen Gemeinde beschwerte sich beim LfD über den Ortsbürgermeister, der seine Ehefrau unentgeltlich in der Verwaltung beschäftige. Damit auch jeder Bürger von dem segensreichen Wirken erfahre, habe dies der Bürgermeister wie folgt öffentlich bekanntgemacht: „Meine Frau wird weiterhin jeden Montag in der Zeit von 9 bis 10 Uhr Wertstoffsäcke ausgeben und Ihnen bei verschiedenen Angelegenheiten behilflich sein. Weiterhin ist sie am Dienstag und Donnerstag von 17.30 Uhr bis 18.30 Uhr mit mir im Büro."

Die Fraktion teilte weiter mit, die Bürgermeistersgattin verfüge über alle Schlüssel zum Rathaus und könne „insbesondere zu Zeiten, in denen sie alleine in der Verwaltung anwesend ist, ungehindert und ohne Mühe alle Akten der Gemeinde wie Bauanträge, Personenstandsangelegenheiten, Grundstücksgeschäfte usw. einsehen". Auch bei den Sprechstunden des Ortsbürgermeisters sei sie anwesend, habe dann Akteneinsicht und könne die Gespräche der Bürgerinnen und Bürger mithören. Die Fraktion meinte, daß dies alles mit Datenverarbeitungsvorgängen (Datenerhebung, -nutzung, -übermittlung) verbunden sei, die, weil kein Beschäftigungsverhältnis bestehe, rechtswidrig seien.

Diese Argumentation ist nicht von der Hand zu weisen: Mit der Ausübung der beschriebenen Tätigkeiten sind Informationsvorgänge verbunden, die datenschutzrelevant sind. Datenschutzrechtlich ist von Bedeutung, daß kein Beschäftigungsverhältnis existiert, die Ehefrau des Bürgermeisters also keinen dienstrechtlichen oder strafrechtlichen Verschwiegenheitspflichten, die an

ein Beschäftigungsverhältnis anknüpfen, unterliegt und der Bürgermeister auch keine dienstrechtlichen Weisungsbefugnisse hat. Die materiellen Datenschutzbestimmungen des LDSG richten sich an die datenverarbeitenden Stellen; sie setzen voraus, daß sie durch Weisungsgebundene vollzogen werden.

Eine umfassende datenschutzrechtliche Würdigung gebietet es indessen, in Betracht zu ziehen, daß die freiwillige unentgeltliche Mitarbeit in der gemeindlichen Arbeit auch andere rechtliche Grundlagen haben könnte. Zu denken ist an die Ausübung eines Ehrenamtes oder von ehrenamtlichen Tätigkeiten – die aber wohl vorliegend nicht in Betracht kommen –, vielleicht aber auch an ein Auftragsverhältnis besonderer Art. Sofern im Rahmen eines solchen Rechtsverhältnisses eine Weisungsgebundenheit bestünde, ließen sich die damit einhergehenden datenschutzrechtlichen Probleme durch die Begründung eines datenschutzrechtlichen Auftragsverhältnisses i. S. v. § 4 LDSG und eine Verpflichtung nach dem Verpflichtungsgesetz lösen.

Wegen der grundsätzlichen Bedeutung der Sache fragte der LfD beim Ministerium des Innern und für Sport als der obersten Aufsichtsbehörde an, auf welcher Rechtsgrundlage und in welcher Rechtsform eine freiwillige unentgeltliche Mitarbeit in der gemeindlichen Arbeit ohne Verletzung datenschutzrechtlicher Bestimmungen möglich ist. Das Ministerium äußerte sich wie folgt:

„Nach den mitgeteilten Umständen kommt eine unentgeltliche Mitarbeit der Ehefrau des Ortsbürgermeisters als Schreibkraft nur durch Wahrnehmung eines Ehrenamtes oder einer ehrenamtlichen Tätigkeit in Betracht.

In welcher der beiden Formen eine solche Tätigkeit ausgeübt wird, hängt nach § 18 Abs. 1 und 2 GemO allein davon ab, ob die Tätigkeit nur vorübergehend, dann ehrenamtliche Tätigkeit, oder auf längere Zeit, dann Ehrenamt, ausgeübt werden soll. Zu einer ehrenamtlichen Tätigkeit werden die Einwohner vom Ortsbürgermeister bestellt, während zu einem Ehrenamt nur Bürger durch den Ortsgemeinderat gewählt werden, soweit durch Gesetz nicht etwas anderes bestimmt ist (vgl. § 18 Abs. 3 Satz 1 GemO).

Die Bestellung und Wiederbestellung zu einer ehrenamtlichen Tätigkeit sowie die Wahl zu einem Ehrenamt ist weiterhin beschränkt auf die Wahrnehmung gemeindlicher Aufgaben. Für die Wahrnehmung von Verwaltungsaufgaben in Ortsgemeinden gelten dabei folgende Grundsätze:

- Die Verbandsgemeindeverwaltung führt gem. § 68 Abs. 1 GemO im Namen und im Auftrag der Ortsgemeinde deren Verwaltungsgeschäfte. Die Beschäftigung von hauptamtlichen Bediensteten durch die Ortsgemeinde zur Erledigung von Verwaltungsgeschäften, die der Verbandsgemeindeverwaltung nach der vorgenannten Vorschrift vorbehalten sind, ist nicht zulässig.
- Nicht zu den Verwaltungsgeschäften zählt der Schriftverkehr des Ortsbürgermeisters als Organ seiner Gemeinde. Gegen die Beschäftigung einer hauptamtlichen Schreibkraft im erforderlichen Umfang bestehen insoweit keine Bedenken (vg. Tz. 7.1 und 7.2 der VV zu § 68 GemO).
- Eine andere Bewertung ergibt sich auch nicht aus einer ehrenamtlichen Wahrnehmung der Aufgaben.

Für die vorliegende Eingabe folgt daraus, daß nur die Fertigung des Schriftverkehrs des Ortsbürgermeisters als Organ der Ortsgemeinde, die nicht Verwaltungsgeschäfte sind, von der Ehefrau ehrenamtlich oder als Ehrenamt wahrgenommen werden können. Die vorliegend durch Aushang genannten weiteren Tätigkeiten fallen offensichtlich nicht unter die gemeindlichen Aufgaben. Sie dürfen auch ehrenamtlich oder aufgrund anderer Rechtsverhältnisse nicht wahrgenommen werden."

Danach war es also unzulässig, daß die Ehefrau des Ortsbürgermeisters zur Wahrnehmung von Aufgaben, die nicht nur in der Fertigung des Schriftverkehrs des Ortsbürgermeisters – außerhalb der Verwaltungsgeschäfte – bestanden, herangezogen wurde. Auch diese Schreibarbeiten waren unzulässig, wenn sie nicht im Rahmen einer ehrenamtlichen Tätigkeit wahrgenommen wurden. Gegen datenschutzrechtliche Bestimmungen wurde insoweit verstoßen, als es der Ortsbürgermeister seiner Frau ermöglichte, unzulässige Tätigkeiten auszuüben und dabei personenbezogene Daten von Bürgerinnen und Bürgern zur Kenntnis zu nehmen.

18.10 Bürgerbefragung

Es entspricht bestem Demokratieverständnis, wenn die politischen Repräsentanten einer Gemeinde wichtige – und kostenträchtige – Entscheidungen sorgsam vorbereiten. Und so ist auch unter Datenschutzgesichtspunkten nicht das geringste dagegen einzuwenden, daß ein Ortsbürgermeister die Einwohner befragt, ob sie mit dem Neubau eines Gemeinde- und Vereinshauses einverstanden sind, wenn er diese Befragung in der gesetzlich vorgeschriebenen Weise durchführt.

Ein Ortsbürgermeister in einer kleinen pfälzischen Gemeinde hatte sich zu den datenschutzrechtlichen Aspekten der von ihm inszenierten Befragungsaktion zum Neubau eines Gemeinde- und Vereinshauses erkennbar nicht die geringsten Gedanken gemacht. In einem Anschreiben an die Einwohnerinnen und Einwohner wies er darauf hin, daß für jede in Frage kommende

Person ein separater Zettel auszufüllen ist. Der „Zettel" enthielt die Erklärung: „Ich habe das Erläuterungsschreiben zu dieser Angelegenheit erhalten und gebe dazu folgende verbindliche Erklärung ab: – ich bin für den Neubau eines Gemeinde- und Vereinshauses; – ich bin gegen den Neubau eines Gemeinde- und Vereinshauses; – ich enthalte mich der Stimme zu einem solchen Vorhaben." Wie es sich für eine „verbindliche Erklärung" gehört, waren auch der Name und die Anschrift des Absenders anzugeben.

Die Erhebung personenbezogener Daten – um eine solche handelt es sich bei der Befragungsaktion – ist nach § 12 Abs. 1 LDSG nur zulässig, wenn ihre Kenntnis zur rechtmäßigen Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Diese Voraussetzung lag insoweit nicht vor, als der Name und die Anschrift erfragt wurden. Eine Befragungsaktion in anonymer Form – Rückantwort ohne Absenderangabe – hätte ausgereicht, die Einstellung der Gemeindeeinwohner zu dem Projekt zu erfragen. Da keine gesetzliche Auskunftspflicht und auch keine Antwortpflicht im Sinne einer Obliegenheit bestand, waren die Betroffenen auf die Freiwilligkeit ihrer Angaben hinzuweisen (§ 12 Abs. 2 Satz 3 LDSG). Nach § 5 Abs. 2 LDSG bedarf die Einwilligung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Wenn die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden soll, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

Nach Absatz 3 der zitierten Vorschrift hätten die Betroffenen in geeigneter Weise über die Bedeutung der Einwilligung, den Verwendungszweck der Daten und den möglichen Empfängerkreis aufgeklärt werden müssen. Ferner hätten sie im konkreten Falle darauf hingewiesen werden müssen, daß aus einer Verweigerung der Einwilligung keine Nachteile entstehen.

Der LfD beanstandete die Verstöße gegen geltendes Datenschutzrecht und informierte die Aufsichtsbehörde hierüber.

Im übrigen hielt er es für geboten, die bereits eingegangenen oder noch eingehenden Befragungsbögen sofort und ohne weitere Unterrichtung von Beigeordneten oder Ratsmitgliedern zu vernichten.

18.11 Datenerhebung zur Erstellung eines Mietspiegels

Nach § 2 Abs. 5 des Gesetzes zur Regelung der Miethöhe sollen Gemeinden, soweit hierfür ein Bedürfnis besteht und dies mit einem für sie vertretbaren Aufwand möglich ist, Mietspiegel erstellen. Sie bieten, wenn sie aufgrund verläßlicher Daten erstellt sind, Mietern und Vermietern eine objektive und neutrale Grundlage für die Vereinbarung von Mieten und tragen dazu bei, Streitfälle über eine angemessene Miethöhe zu vermeiden.

Das Gesetz enthält indessen keine Rechtsgrundlage für die Erteilung von Auskünften, so daß nach § 12 LDSG nur eine freiwillige Datenerhebung zulässig ist. Der LfD hat immer wieder Veranlassung, Städte und Gemeinden daran zu erinnern, daß hierauf in den Anschreiben an die zu befragenden Haushalte in aller Deutlichkeit hinzuweisen ist. Er besteht allerdings nicht darauf, daß eine Einwilligungserklärung in Schriftform eingeholt wird, sondern hält die in Kenntnis der Freiwilligkeit durch Teilnahme an der Befragung zum Ausdruck kommende konkludente Einwilligung vor dem Hintergrund der besonderen für den Mietspiegel geltenden gesetzlichen Regelungen für angemessen. Es ist indessen geboten, die Betroffenen entsprechend § 5 Abs. 3 LDSG über die Bedeutung der Einwilligung, den Verwendungszweck der Daten und den möglichen Empfängerkreis aufzuklären. Ferner ist ein Hinweis geboten, daß aus einer Verweigerung der Einwilligung keine Nachteile entstehen.

18.12 Outsourcing von Großrechneranwendungen

Insbesondere Anwender von Großrechenanlagen im öffentlichen Bereich bemühen sich um eine Verbesserung der Wirtschaftlichkeit durch Outsourcing von DV-Anwendungen.

Datenschutzrechtlich ist Outsourcing in aller Regel als Auftragsdatenverarbeitung zu qualifizieren.

Unabhängig davon, ob Auftragnehmer eine öffentliche oder nichtöffentliche Stelle ist, bleibt der Auftraggeber nach § 3 Abs. 3 LDSG als datenverarbeitende Stelle für die Einhaltung der Bestimmungen des LDSG und anderer Vorschriften über den Datenschutz verantwortlich (§ 4 Abs. 1 Satz 1). Während indessen von öffentlichen Stellen als Auftragnehmern die Bestimmungen des LDSG – vgl. § 4 Abs. 4 Satz 1 – unmittelbar anzuwenden sind, ist dies bei Auftragnehmern, die nichtöffentliche Stellen sind, durch Vertrag sicherzustellen. Dies gilt auch für die Unterwerfung unter die Kontrolle des LfD (§ 4 Abs. 1 Satz 3).

Schon aus den unterschiedlichen Einwirkungsmöglichkeiten auf den Auftragnehmer – einerseits direkte Anwendung des LDSG und Durchsetzung im Aufsichtsweg, andererseits vertragliche Zusicherung und Durchsetzung vertraglicher Ansprüche im gerichtlichen Verfahren – folgt, daß dessen rechtliche Stellung bei der Entscheidung über die Auftragsvergabe nicht unberücksichtigt bleiben kann. Die Rechtsstellung ist sowohl bei der Zuverlässigkeitsprüfung nach § 4 Abs. 2 wie auch bei der Beurteilung der Angemessenheit unter Berücksichtigung der Empfindlichkeit von Daten und der schutzwürdigen Interessen von Betroffenen (§ 4 Abs. 4 Satz 2) von Bedeutung.

Mit der letztgenannten Vorschrift hat der Gesetzgeber einzelne Bereiche von der Auftragsdatenverarbeitung durch private Stellen grundsätzlich ausgenommen. Hierzu gehören:

- Tätigkeiten mit weitreichenden Befugnissen (z. B. Systemverwaltung) in Bereichen, die gesetzlich einen erweiterten Schutz genießen, z. B. medizinische Daten, Sozialdaten, Steuerdaten (vgl. hierzu 14. Tb., Tz. 13.3), Daten aus dem Polizeibereich und der Nachrichtendienste.
- Tätigkeiten, die Voraussetzung oder von grundlegender Bedeutung für die Wahrnehmung staatlicher (hoheitlicher) Aufgaben sind, z. B. Betrieb oder Administration zentraler Kommunikationsnetze der Verwaltung (Globig, Kommentar zum LDSG, Erl. 8 zu § 4).

Für die Verarbeitung von Sozialdaten durch private Auftragnehmer enthält § 80 Abs. 5 SGB X die Konkretisierung, daß sie nur zulässig ist, wenn beim Auftraggeber sonst Störungen im Betriebsablauf auftreten können oder die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfaßt. Soweit die Auftragsverarbeitung von Sozialdaten in Rede steht, ist danach nur die Übertragung eines Teilbereichs der Datenverarbeitung auf einen privaten Auftragnehmer zugelassen. Der Kostengesichtspunkt kommt nicht nur im Vergleich der Auftragsdatenverarbeitung durch Private mit der Datenverarbeitung durch den Leistungsträger selbst, sondern auch im Vergleich mit der Auftragsverarbeitung durch öffentliche Stellen zum Tragen. Im übrigen kann diese Regelung auch als Auslegungshinweis für § 4 Abs. 4 LDSG herangezogen werden, m. a. W., die Sollregelung des LDSG schließt bei Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, eine Datenverarbeitung durch private Auftragnehmer aus, es sei denn, diese könnten eine Datenverarbeitung sowohl im Vergleich zur datenverarbeitenden Stelle selbst als auch zu einer öffentlichen Stelle als Auftragnehmer erheblich kostengünstiger ausführen, und es wäre nicht die gesamte Datenverarbeitung betroffen, sondern nur einzelne Phasen oder Teilmengen.

Bei der Auftragsverarbeitung von Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, kommt es vor dem Hintergrund der einschlägigen Bestimmungen des LDSG darauf an, zunächst zu beurteilen, ob die nichtöffentlichen Auftragnehmer gleichermaßen zuverlässig sind wie öffentliche Auftragnehmer und ob sie bereit sind, die vertraglichen Pflichten zur Gewährleistung des technisch-organisatorischen Datenschutzes und der Datenschutzkontrolle zu übernehmen. Nur wenn dies gewährleistet ist, können Wirtschaftlichkeitsüberlegungen und die übrigen oben dargestellten Gesichtspunkte ergänzend berücksichtigt werden.

18.13 Datenübermittlungen an die Abwasserwerke

Den LfD erreichen immer wieder Eingaben, in denen beklagt wird, daß Daten über den Wasserverbrauch für die Berechnung der Abwassergebühren genutzt und in solchen Fällen, in denen unterschiedliche gemeindliche oder außergemeindliche Einrichtungen zuständig sind, auch übermittelt werden.

Eine Nutzung der Wasserverbrauchsdaten zum Zwecke der Gebührenfestsetzung für die Abwasserbeseitigung ist nur dann zulässig, wenn die Entgeltsatzung Abwasserbeseitigung eine entsprechende Regelung enthält. Häufig ist bestimmt: „Als in die öffentliche Abwasserbeseitigungsanlage gelangt gilt die dem Grundstück aus öffentlichen oder privaten Wasserversorgungsanlagen zugeführte und durch Wasserzähler ermittelte Wassermenge." Die Zulässigkeit der Übermittlung von Angaben zum Wasserverbrauch ergibt sich aus § 3 KAG i. V. m. § 31 Abs. 1 AO. Danach dürfen Abgabenbemessungsgrundlagen an Körperschaften des öffentlichen Rechts zur Festsetzung von solchen Abgaben mitgeteilt werden, die an diese Bemessungsgrundlagen anknüpfen.

18.14 Interessenkonflikte bei behördlichen Datenschutzbeauftragten

Nach der amtlichen Begründung des LDSG – Drucksache 12/3824 S. 31 ff. – soll im Rahmen der Zuverlässigkeit des behördlichen Datenschutzbeauftragten sichergestellt werden, daß mit dieser Funktion nur solche Bedienstete betraut werden, die dadurch nicht in einen Interessenwiderstreit mit ihren regelmäßig wahrzunehmenden sonstigen Aufgaben geraten. Es muß danach grundsätzlich davon ausgegangen werden, daß existierende Interessenkonflikte Zweifel an der Zuverlässigkeit des behördlichen Datenschutzbeauftragten begründen.

Angesichts der Einschränkung des Aufgabenfeldes des behördlichen Datenschutzbeauftragten auf unterstützende und beratende Funktionen ist die Gefahr von Interessenkollisionen freilich allenfalls bei Mitarbeitern der Organisationsabteilung oder in der automatisierten Datenverarbeitung evident. Mit der Aufgabe, die öffentliche Stelle bei der Ausführung des LDSG sowie anderer Vorschriften über den Datenschutz zu unterstützen, wäre es sicherlich nur schwerlich zu vereinbaren, wenn ein Mitarbeiter in erster Linie seine eigene Tätigkeit beurteilen müßte.

Ob freilich solche Gesichtspunkte im konkreten Falle der Bestellung einer EDV-Fachkraft als behördlicher Datenschutzbeauftragter entgegenstehen, läßt sich nur in Kenntnis ihrer Stellung innerhalb der Behördenorganisation und der sonstigen dienstlichen Aufgaben beurteilen. Im Blick auf die Organisationshoheit der datenverarbeitenden Stellen ist der LfD hier sehr zurückhaltend.

19. Telekommunikation

19.1 EG-Richtlinie zum Datenschutz im ISDN

Seit 1990 ist ein Vorschlag für eine Datenschutz-Richtlinie vorhanden. Bereits im 14. Tb., Tz. 20.1.4 und 15. Tb.,Tz. 20.1. hat der LfD über den Stand der Dinge berichtet. Die für Post und Telekommunikation zuständigen Minister der Europäischen Union haben sich auf einen gemeinsamen Standpunkt geeinigt, den das Europäische Parlament bis auf wenige Änderungswünsche akzeptiert hat (Gemeinsamer Standpunkt [EG], Nr. 57/96, vom Rat festgelegt am 12. September 1996 im Hinblick auf den Erlaß der Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz [ISDN] und in digitalen Mobilfunknetzen [96/C32/06], ABl. EG Nr. C 315 vom 24. Oktober 1996, S. 30).

Mit dieser Fassung des Entwurfs wird den wesentlichen Gesichtspunkten des Datenschutzes Rechnung getragen. So ist der Anwendungsbereich dahin gehend erweitert worden, daß er nicht mehr (nur) auf digitale Telekommunikationsnetze beschränkt sein soll, sondern die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation allgemein regelt. Allerdings war die Einbeziehung unternehmensinterner Netze (Corporate Networks) im Ministerrat nicht durchsetzbar. Der Richtlinienentwurf bezieht sich unter diesem Gesichtspunkt gem. Art. 3 Abs. 1 auf die Verarbeitung personenbezogener Daten im Zusammenhang mit der Erbringung öffentlich zugänglicher Telekommunikationsdienste in öffentlichen Telekommunikationsnetzen. In diesem Zusammenhang ist jedoch auf eine Erklärung im Ratsprotokoll hinzuweisen, in der Rat und Kommission feststellen, daß die Richtlinie die nationalen Gesetzgeber in keiner Weise daran hindert, die Bestimmungen der Richtlinie auch auf nichtöffentliche Telekommunikationsnetze und nichtöffentlich zugängliche Telekommunikationsdienste anzuwenden. Nach den Regelungen im Telekommunikationsgesetz gelten die Datenschutzbestimmungen für alle Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen, sind also nicht – wie im Richtlinienentwurf – auf öffentlich zugängliche Telekommunikationsdienste beschränkt.

Weiterhin ist zu begrüßen, daß dem Grundsatz der Vertraulichkeit ein hoher Stellenwert beigemessen wird. So stellt der Richtlinienentwurf mit Artikel 5 die Vertraulichkeit der Kommunikation an den Anfang der materiell-rechtlichen Regelungen. Danach haben die Mitgliedstaaten insbesondere das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Kommunikation durch andere Personen als die Benutzer zu untersagen, wobei Abhör- und Überwachungsmaßnahmen nur gerechtfertigt sind, wenn entweder die betroffenen Benutzer eingewilligt haben oder ein Gesetz zur Durchführung derartiger Maßnahmen ermächtigt. Auch dürfen gem. Art. 6 Daten über einzelne Telekommunikationsverbindungen (soweit keine weitergehende Einwilligung vorliegt) nur zur Gebührenabrechnung verwendet werden. Daten, die nicht dafür gebraucht werden, sind nach Beendigung der Verbindung zu löschen. In diesen Bereichen werden die Forderungen bereits durch die Regelungen im Telekommunikationsgesetz und in der Telekommunikationsdienstunternehmen-Datenschutzverordnung (vgl.Tz. 19.6) erfüllt. Was die Ausgestaltung des Zweckbindungsgrundsatzes anbelangt, geht der Richtlinienentwurf über die – noch geltende – Widerspruchsregelung in § 4 Abs. 2 TDSV hinaus. Denn der Richtlinientext verbietet die elektronische Profilbildung durch zweckentfremdende Vermarktung von Abrechnungsdaten durch den Betreiber, wenn der (Neu-) Kunde nicht eingewilligt hat.

Ferner verlangt der Richtlinienentwurf beispielsweise bei der Verwendung von Telefaxgeräten für Zwecke des Direktmarketings, daß dieses nur bei vorheriger Einwilligung der Adressaten gestattet ist. Bei Telefonmarketing haben die Mitgliedstaaten Vorkehrungen zu treffen, daß Anrufe bei Teilnehmern, die keine derartigen Anrufe wünschen, unterbunden werden können.

Voraussichtlich wird die ISDN-Richtlinie noch im Jahre 1997 endgültig beschlossen.

Nach Auffassung des LfD ist von besonderer Bedeutung, daß der Europäische Rat bei den Beratungen zum Gemeinsamen Standpunkt grundsätzlich hat erkennen lassen, daß im Hinblick auf die bestehenden Datenschutzdefizite in der Europäischen Union bereichsspezifische Regelungen für erforderlich gehalten werden. In dem hier dargestellten Sektor beispielsweise ist die EG-Datenschutzrichtlinie (vgl. Tz. 3.1) vom Ansatz her überfordert, die Anwenderrechte im europäischen Telekommunikations-Binnenmarkt angemessen zu schützen.

19.2 Telekommunikationsrecht in Bewegung (Postreform III)

Die „Postreform I" aus dem Jahre 1989 führte zu der Verselbständigung der Deutschen Bundespost Postdienst, der Telekom und der Postbank. Im Bereich der Telekommunikation war damit insbesondere die Aufhebung des Endgerätemonopols verbunden.

Mit den Entschließungen vom 22. Juli 1993 und 22. Dezember 1994 hat der Rat der Europäischen Union festgelegt, daß die Telekommunikationsinfrastrukturen und der öffentliche Telefondienst zum 1. Januar 1998 liberalisiert werden sollen (Entschließung 93/C 213 des Rates vom 22. Juli 1993 zur Prüfung der Lage im Bereich der Telekommunikation und zu den not-

wendigen künftigen Entwicklungen in diesem Bereich, ABl. EG Nr. C 213, 1 vom 6. August 1993; Entschließung 94/C 379 vom 22. Dezember 1994 über die Grundsätze und den Zeitplan für die Liberalisierung der Telekommunikationsinfrastrukturen, ABl. EG Nr. C 379, 4 vom 30. Dezember 1994; vgl. auch die Entschließung 95/C 258 des Rates vom 18. September 1995 zur Entwicklung des künftigen ordnungspolitischen Rahmens für die Telekommunikation, ABl. EG Nr. C 258, 1 vom 3. Oktober 1995). In deren Folge wurde zunächst die „Postreform II" (vgl. 15. Tb., Tz. 20.2) auf den Weg gebracht. Sie schuf mit einer Änderung des Grundsgesetzes (Art. 87 f) die verfassungsrechtlichen Voraussetzungen für die Privatisierung der Postunternehmen.

Das Telekommunikationsgesetz beseitigt nunmehr im Zuge der „Postreform III" die noch bestehenden Monopole der Deutschen Telekom AG und schafft den ordnungspolitischen Rahmen für den deutschen Telekommunikationsmarkt. Das Übertragungswegemonopol der Deutschen Telekom AG hat am 1. August 1996 geendet, das Sprachtelefondienstmonopol wird zum 1. Januar 1998 gem. § 100 Abs. 1 TKG aufgehoben. Damit ist der langjährige Prozeß der allmählichen Liberalisierung der Telekommunikationsmärkte abgeschlossen.

19.3 Grundsätzliches zum Telekommunikationsgesetz

Am 1. August 1996 ist das Telekommunikationsgesetz (BGBl. I, 1120) – „Kernstück der Postreform III" – in Kraft getreten. Zu dem Gesetzentwurf hat der LfD gegenüber der Landesregierung Stellung genommen. In einer Entschließung (vgl. Anlage 3) hatten die Datenschutzbeauftragten des Bundes und der Länder im Vorfeld des Entwurfs ihre Forderungen formuliert. Das Telekommunikationsgesetz regelt unter dem Titel „Fernmeldegeheimnis, Datenschutz, Sicherung" die Grundsätze des Datenschutzes in der Telekommunikation, die vorher lediglich auf der Ebene von Rechtsverordnungen festgelegt waren.

Gemäß der Begriffsdefinition in § 3 Nr. 16 TKG handelt es sich bei der Telekommunikation um das „Aussenden, Übermitteln und Empfangen von Nachrichten jeglicher Art in Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen". Mithin geht es hier nicht um die Aufbereitung oder Verwendung von übertragenen Inhalten, sondern um den technischen Vorgang der Übertragung. Dieser Gesichtspunkt ist hinsichtlich der Unterscheidung von Telekommunikationsdiensten einerseits und Mediendiensten sowie Telediensten andererseits von wesentlicher Bedeutung, wobei von der „Einordnungslogik" her die Feststellung wichtig ist, daß sowohl Rundfunk als auch Medien- und Teledienste stets unter Nutzung von Telekommunikation erbracht werden.

Nach dem Entwurf in der Fassung vom 30. Januar 1996 sollte sich das Telekommunikationsgesetz insgesamt nur auf gewerbliche Telekommunikationsdienstleistungen beschränken. In seiner Stellungnahme zu dem Entwurf hat der LfD zu diesem Vorhaben u. a. folgendes ausgeführt: „In § 86 TKG-E ist die Ermächtigung zum Erlaß von Datenschutzverordnungen enthalten, wonach der Datenschutz lediglich für Unternehmen gilt, die Telekommunikationsdienstleistungen erbringen. Gem. § 3 TKG-E sind per Begriffsbestimmung nur gewerbliche Angebote als Telekommunikationsdienstleistungen zu verstehen. Mit dieser Formulierung wird auf eine Gewinnerzielungsabsicht des Anbieters abgestellt. Nicht erfaßt werden damit Telekommunikationsdienste für eigene Zwecke des Betreibers (z. B. Corporate Networks). Es ist indessen nicht ersichtlich, weshalb der gewerbliche Charakter des Angebots einer Telekommunikationsleistung ein unterschiedliches Datenschutzniveau rechtfertigen soll. So wären beispielsweise für den Bereich der Corporate Networks die Vorschriften über technische Schutzmaßnahmen nach § 84 TKG-E und die Datenschutzvorschriften nach § 86 TKG-E nicht anwendbar. Daher wird vorgeschlagen, in den genannten Bestimmungen auf die Erbringung geschäftsmäßiger Telekommunikationsdienste abzustellen, wie dies auch § 82 Abs. 2 Satz 1 TKG-E im Hinblick auf die Verpflichtung zur Wahrung des Fernmeldegeheimnisses festlegt. So sind mit ‚geschäftsmäßig' die auf eine gewisse Dauer angelegten Aktivitäten im Telekommunikationsbereich gemeint, ohne daß es auf eine Gewinnerzielungsabsicht ankommt." Dieser Vorschlag wurde im Gesetzgebungsverfahren aufgegriffen, so daß nunmehr (z. B.) auch Coporate Networks, die nicht in Gewinnerzielungsabsicht betrieben werden, in den Schutzbereich des Gesetzes fallen.

Die Vorschriften über die Kontrolle des Datenschutzes wurden verändert (§ 91 Abs. 4 TKG). Der BfD ist nunmehr als zentrale Stelle zuständig für die Kontrolle der Einhaltung von Datenschutzbestimmungen bei Unternehmen, die in den Geltungsbereich des Telekommunikationsgesetzes fallen. Seine Kontrolle tritt bei privaten Unternehmen, die Telekommunikationsdienste erbringen, an die Stelle der Kontrolle nach § 38 BDSG durch die Datenschutzaufsichtsbehörden der Länder. Es bedarf hier keines konkreten Anlasses für die Durchführung von Prüfungen. Werden Telekommunikationsdienstleistungen durch öffentliche Stellen der Länder angeboten, so bleiben jedoch weiterhin die Landesbeauftragten für den Datenschutz zuständig.

19.4 Das einfachgesetzliche Fernmeldegeheimnis

Das durch Art. 10 Abs. 1 GG garantierte verfasssungsrechtliche Fernmeldegeheimnis wirkt direkt weiterhin im Verhältnis Staat – Bürger. Die Wahrung des einfachgesetzlichen Fernmeldegeheimnisses ist in § 2 Abs. 2 Nr. 1 TKG ausdrücklich als Regulierungsziel in das Gesetz aufgenommen worden. Danach ist zur Wahrung des Fernmeldegeheimnisses nach dem Telekommunikationsgesetz verpflichtet, wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (§ 85 Abs. 2 Satz 1 TKG). Das Fernmeldegeheimis bietet einen umfassenden Schutz für den Inhalt der Telekommunikation und „ihre

näheren Umstände". Damit werden die Verbindungsdaten angesprochen, die Auskunft darüber geben, wer wann mit wem telefoniert oder elektronisch Daten ausgetauscht hat. Die Einhaltung des einfachgesetzlichen Fernmeldegeheimnisses ist allerdings im Straf- und Bußgeldkatalog des Telekommunikationsgesetzes (bedauerlicherweise) nicht abgesichert. Ein Verstoß gegen § 85 TKG kann aber u. U. nach § 354 StGB (Verletzung des Post- und Fernmeldegeheimnisses) zu ahnden sein.

Die Datenschutzbestimmungen und die Regelungen zum Fernmeldegeheimnis im Telekommunikationsgesetz beziehen sich gem. § 89 Abs. 1 i. V. m. § 3 Nr. 5 TKG auf Telekommunikationsdienste, die gegenüber Dritten erbracht werden. Dem Fernmeldegeheimnis unterliegen somit beispielsweise auch Telekommunikationsdienste, die als Nebenleistung erbracht werden, ohne daß – wie z. B. in Hotels und Krankenhäusern – die Gewinnerzielungsabsicht im Vordergrund steht.

Das Führen dienstlicher Anrufe aus einer (selbst betriebenen) Nebenstellenanlage fällt nicht unter den Geltungsbereich des Telekommunikationsgesetzes; denn hier handeln die Beschäftigten als Angehörige der Stellle, die die Telekommunikationsanlage betreibt und sind nicht Dritte im Sinne des Gesetzes. Allerdings sind Nebenstellenanlagen im Eigenbetrieb nach der Begründung zum Gesetzentwurf des Telekommunikationsgesetzes erfaßt, soweit sie den Beschäftigten zur privaten Nutzung zur Verfügung gestellt werden (vgl. Bundestagsdrucksache 13/3609). In dieser Situation erbringt der Betreiber der Kommunikationsanlage einen geschäftsmäßigen Telekommunikationsdienst im Sinne von § 3 Nr. 5 TKG, weil die Beschäftigten hier nicht im Auftrag und im Namen der Stelle handeln, die die Telekommunikationsanlage betreibt, sondern als Dritte, denen gegenüber die Regelungen zum Fernmeldegeheimnis wiederum gelten. Allgemein läßt sich feststellen, daß im Telekommunikationsgesetz Inhalt und Anwendungsbereich des Fernmeldegeheimnisses wesentlich präziser als bislang im Fernmeldeanlagengesetz definiert sind.

19.5 Sicherheitsanforderungen

Die Sicherheit in der Telekommunikation hat einen erhöhten Stellenwert mit wachsender Bedeutung erhalten. Dieser Entwicklung entspricht das Telekommunikationsgesetz mit seinen Regelungen zur Sicherheit in der Telekommunikation. Es soll gewährleistet bleiben, daß auch mit der Liberalisierung und Privatisierung in der Telekommunikation eine ausgewogene Standardsicherheit erhalten bleibt, die sich an den Interessenlagen der Nutzer, der Betreiber und der Hersteller orientiert.

Bestimmte spezifische Lösungen (organisatorische, sicherheitstechnische oder systembezogene Maßnahmen) sind nicht vorgegeben. Sie sollen der technischen Entwicklung und den Gestaltungsmöglichkeiten der Betreiber überlassen bleiben. Es ist Aufgabe der Betreiber einzuschätzen, wie sicherheitssensibel ihre Telekommunikationsanlagen sind, welche Bedeutung diese für die Allgemeinheit haben und welche Schutzmaßnahmen mit welchem technischen und wirtschaftlichen Aufwand getroffen werden müssen. Der Schutzbereich umfaßt das Fernmeldegeheimnis und personenbezogene Daten.

Der Gesetzgeber hat das Bundesministerium für Post und Telekommunikation mit § 87 Abs. 3 TKG ermächtigt, die Erfüllung dieser allgemeinen Sicherheitsanforderungen in einer Rechtsverordnung näher zu regeln. Es ist beabsichtigt, von dieser Ermächtigung zunächst keinen Gebrauch zu machen, solange die Betreiber die Gefährdungen sachgerecht beurteilen und entsprechende Vorsorgemaßnahmen treffen. Wer Telekommunikationsanlagen zum geschäftsmäßigen Erbringen von Telekommunikationsdiensten betreibt, hat nach § 87 Abs. 1 TKG angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten gegen unerlaubte Zugriffe und gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen können, zu treffen, wobei der Stand der technischen Entwicklung zu berücksichtigen ist. Als Maßstab ist die Bedeutung der zu schützenden Rechte anzulegen. Die sachgerechte Umsetzung von Schutzmaßnahmen ist zudem ausgehend von der Bedeutung der zu schützenden Anlagen und dem Umfang möglicher Gefährdungen zu beurteilen. Grundsätzlich sollten die Interessen sowohl der Betreiber als auch die Interessen der Nutzer angemessen und sachgerecht in Betracht gezogen werden.

Eine Gefährdung des Fernmeldegeheimnisses und personenbezogener Daten ist insbesondere im Bereich der Peripherie (z. B. im Anschlußleitungsnetz) vorhanden, weil hier überwiegend einzelne Telekommunikationsverbindungen betroffen sind. In diesem Zusammenhang ist der Schutz programmgesteuerter Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe im oberen Systembereich erforderlich, da dort am ehesten ernste Schäden – auch aufgrund illegaler Handlungen – auftreten können.

Der bislang seitens des Bundesministeriums für Post und Telekommunikation vorgelegte Katalog von Sicherheitsanforderungen enthält größtenteils objektbezogene, nicht aber system- und organisationsbezogene Komponenten (z. B. Paßwortschutz bei den eingesetzten Datenverarbeitungssystemen, Bestellung eines Sicherheitsbeauftragten) und ist daher aus der Sicht des Datenschutzes ungeeignet, um den Anforderungen des § 87 TKG zu entsprechen.

19.6 Telekommunikationsdienstunternehmen-Datenschutzverordnung

Fast zeitgleich mit dem Telekommunikationsgesetz, aber noch basierend auf § 10 Abs. 1 des Gesetzes über die Regulierung der Telekommunikation und des Postwesens (das gem. § 97 Abs. 2 TKG am 31. Dezember 1997 außer Kraft tritt) hat die Bundes-

regierung mit der Telekommunikationsdienstunternehmen-Datenschutzverordnung Einzelheiten für die Beachtung der informationellen Selbstbestimmung in der Telekommunikation bestimmt. Auch hierzu haben die Datenschutzbeauftragten des Bundes und der Länder im Vorfeld der Regelung eingehend Stellung genommen und ihre Grundpositionen in einer Entschließung formuliert (vgl. Anlage 3). In dieser Verordnung regelt der Bund, was Netzbetreiber und Anbieter von Telekommunikationsleistungen zum Schutz personenbezogener Daten der am Fernmeldeverkehr Beteiligten zu beachten haben.

19.6.1 Verbindungsdaten

Die Verbindungsdaten gehören zu den datenschutzrechtlich sensibelsten Daten. Sie werden bei der Inanspruchnahme von Telekommunikationsdienstleistungen erhoben, verarbeitet und genutzt. Zum einen sind sie erforderlich für das technische Bereitstellen der Verbindung, werden aber auch nach deren Ende gem. § 5 Abs. 2 TDSV für die Entgeltberechnung und andere von der Verordnung erlaubte Zwecke genutzt, wie beispielweise für das Identifizieren von Anschlüssen bei bedrohenden oder belästigenden Anrufen. Verbindungsdaten stellen, da sie Aussagen über den stattgefundenen Fernmeldeverkehr erlauben, nach den Darlegungen im „Fangschaltungsbeschluß" des Bundesverfassungsgerichts vom 25. März 1992 (BVerfGE 85, 386) zugleich Eingriffe in das Fernmeldegeheimnis dar. In § 6 TDSV sind die Rechtsgrundlagen für das Erheben und Verarbeiten von Bestands- und Verbindungsdaten zum Ermitteln und Nachweisen des Entgelts für die in Anspruch genommen Telekommunikationsdienstleistungen enthalten. Grundsätzlich ist das Telekommunikationsunternehmen nur berechtigt, die Zielnummer nach dem Ende der Verbindung um die letzten 3 Ziffern gekürzt zu speichern. Der Kunde kann allerdings verlangen, daß die Verbindungsdaten vollständig gespeichert oder spätestens mit Versendung der Rechnung vollständig gelöscht werden, wobei der Diensteanbieter von der Pflicht zur Vorlage der Verbindungsdaten zu Beweiszwecken befreit wird, wenn diese auf Wunsch des Kunden gem. § 6 Abs. 4 TDSV gelöscht wurden.

19.6.2 Einzelverbindungsnachweis

Die Voraussetzungen für den Einzelverbindungsnachweis sind in § 6 Abs. 7 TDSV geregelt. Der anrufende Kunde hat die Möglichkeit, sich Einzelverbindungsnachweise mit vollständigen Zielnummern erstellen zu lassen, ohne daß der angerufene Teilnehmer der Aufnahme seiner Zielnummer in den Einzelverbindungsnachweis widersprechen kann. Das von den Datenschutzbeauftragten des Bundes und der Länder empfohlene „Holländische Modell" wurde nicht übernommen. Bei diesem in den Niederlanden praktizierten Verfahren können die Anschlußinhaber selbst entscheiden, wie ihre Rufnummern im Einzelverbindungsnachweis dargestellt werden.

Eine Sonderregelung für anonyme Kommunikation als Voraussetzung für die Arbeit sozialer und kirchlicher Telefonberatung findet sich in § 6 Abs. 8 TDSV. Die Nichterkennbarkeit derartiger Verbindungen zu Beratungsstellen auf dem Einzelverbindungsnachweis setzt allerdings voraus, daß sie einen begründeten Antrag gestellt haben, wonach ihre Tätigkeit in sozialen oder kirchlichen Bereichen überwiegend telefonisch wahrgenommen wird und ihre Mitarbeiter besonderen Verschwiegenheitspflichten unterliegen.

19.6.3 Fangschaltung

Die Fangschaltung gehört zu den sensibelsten Formen der Verbindungsdatenverarbeitung. Sie wird dementsprechend häufig problematisiert und soll auch hier etwas ausführlicher dargestellt werden.

Mit den detaillierten Verfahrensvorkehrungen in § 8 TDSV für das Mitteilen ankommender Verbindungen wurde der „Fangschaltungsbeschluß" des Bundesverfassunsgerichts umgesetzt (vgl. 14.Tb. Tz. 20.3). Die Vorschrift gibt den Telekommunikationsunternehmen die Möglichkeit, als zusätzliche Dienstleistung die sog. „Feststellung ankommender Verbindungen bei bedrohenden und belästigenden Anrufen" anzubieten. Grundsätzlich gibt es hierbei mehrere Möglichkeiten. Die erste besteht in der Schaltung einer Fangeinrichtung. Dabei wird der Anrufer beim Einsatz von analoger Vermittlungstechnik dadurch „gefangen", daß der Angerufene eine bestimmte Fangziffer von seinem Telefonanschluß aus während der gerade bestehenden Telefonverbindung wählt. Dies bewirkt, daß die Telefonverbindung auch nach der Beendigung des Anrufs so lange technisch festgehalten wird, bis der genaue Verbindungsweg und damit der Anschluß, von dem aus angerufen wurde, in der Vermittlungsstelle festgestellt wird. Eine weitere Möglichkeit bei analoger Technik besteht in der Anschaltung einer sog. Zählvergleichseinrichtung (ZVE). Vorausssetzung hierfür ist jedoch ein konkreter Verdacht des Kunden im Hinblick auf den Telefonanschluß, von dem aus die unerwünschten Anrufe erfolgen. Die an den vom Kunden benannten Anschluß angeschaltete ZVE registriert dann sämtliche Wählvorgänge mit Zielrufnummern, die von diesem Anschluß ausgehen, und zwar unabhängig davon, ob eine Telefonverbindung zustande kommt oder nicht.

Im Bereich der Digitaltechik werden schon systemtechnisch alle Verbindungen oder Verbindungsversuche des Kunden erfaßt. Sie können somit bei vorliegenden Voraussetzungen für einen Auftrag zur Feststellung ankommender Verbindungen gespeichert und nach der Zielrufnummer der Belästigten ausgewertet werden. Der belästigten oder bedrohten Person kann dann nach Eingrenzung der Zeit, in denen der Anruf erfolgte, der in Frage kommende Anschluß (Rufnummer, Name und Anschrift)

bekanntgegeben werden. Ob tatsächlich eine Bedrohung oder vorsätzliche Belästigung vorliegt, kann von dem Telekommunikationsunternehmen natürlich nicht beurteilt werden, da bei der Feststellung ankommender Verbindungen keinerlei Nachrichteninhalte aufgezeichnet werden dürfen.

Allerdings ist der Kunde des Anschlusses, von dem die als bedrohend oder belästigend bezeichneten Anrufe ausgegangen sind, zu unterrichten, daß über die diese Anrufe betreffenden Verbindungen Auskunft erteilt wurde. Davon kann nur abgesehen werden, wenn die antragstellende Person darlegt, daß ihr aus dieser Mitteilung wesentliche Nachteile entstehen können und diese Nachteile bei Abwägung mit den schutzwürdigen Interessen der Anruferin oder des Anrufers als wesentlich schwerwiegender erscheinen.

Anders als noch in der alten Fassung der TDSV – der Kunde mußte hier eine Bedrohung oder Belästigung gegenüber dem Telekommunikationsunternehmen glaubhaft machen – reicht es für die Einrichtung einer Fangschaltung nunmehr aus, wenn der Kunde in einem zu dokumentierenden Verfahren schlüssig vorträgt, daß bei seinem Anschluß bedrohende oder belästigende Anrufe ankommen (vgl. dazu auch Tz. 7.1.4.4).

20. Medien

20.1 Datenschutz in der multimedialen Gesellschaft

20.1.1 Begriff und Anwendungsfelder

Der rasante Fortschritt im Bereich der Informations- und Kommunikationstechniken – wofür als Synonym derzeit der Begriff „Multimedia" steht – kann unser Leben in vielen Bereichen verändern.

Die herkömmliche Unterscheidung von Individual- und Massenkommunikation ist bei den Informations- und Kommunikationstechnologien mit der wachsenden Zahl der Anwendungen fließenden Übergängen gewichen.

Eine Definition, was Multimedia eigentlich ist, gibt es noch nicht. Das Wort wird vielfach als Oberbegriff für eine Vielzahl neuer Produkte und Dienstleistungen verwendet. Wenn man sich fragt, worin nun die besonderen Risiken des vorausgesagten Multimedia-Zeitalters liegen, ist es Grundvoraussetzung, zunächst einmal eine Vorstellung zu gewinnen, welche „multimedialen" Dienste künftig angeboten werden.

Digitales Fernsehen, elektronische Post (E-Mail) und Videokonferenzen sind in aller Munde. Hinzu kommen eine ganze Menge sog. „Teledienste"; z. B.

- Telebanking, Homebanking (elektronische Erledigung von Bankgeschäften),
- Telemedizin (Gesundheitsinformation und Gesundheitsberatung, Diagnosedaten, Krankenakten),
- Telelearning (Abruf von Lernprogrammen für Ausbildung und Weiterbildung),
- Consulting-Dienste (Kundenberatung, Kundendienst, Fernwartung usw.),
- Elektronische Bestell-, Buchungs- und Maklerdienste (Bestellung von Theaterkarten, Reisebuchungen, Wohnungsvermittlung usw.),
- Homeshopping (interaktive Bestell- und Buchungsdienste),
- Telearbeit (außerbetriebliche Arbeitsstätten, virtuelle Firmen).

Die Verlagerung von Verkehrsvolumen auf die „abgasfreie Datenautobahn" besitzt also ein enormes Potential: Telearbeit statt Berufsverkehr, Videokonferenzen statt Geschäftsreisen, Teleshopping statt Parkplatzsuche, elektronische Ferndiagnose statt Arztbesuch, Video-on-demand statt Kinobesuch, Telebanking statt der Fahrt zur Bank.

Wenn sensibelste private, medizinische oder betriebliche Daten übertragen werden, ist die Sicherung des Rechts auf informationelle Selbstbestimmung im Datenverkehr von zentraler Bedeutung.

Die Bestimmungen zum Datenschutz sollten auch durch grenzüberschreitenden Datenverkehr nicht umgangen werden können. In internationalen multimedialen Netzen wie dem Internet (vgl. Tz. 20.2) fehlen allerdings verantwortliche Betreiber.

20.1.2 Datenverschlüsselung – ein „heißes Eisen"

Die Frage nach der Zulässigkeit von Kryptographie – also der Verschlüsselung von Daten – ist ein rechtspolitisch höchst brisantes Thema. Dabei geht es im Kern um die Frage, ob zwei Menschen frei entscheiden können, wie sie miteinander kommunizieren. Menschen sprechen miteinander, indem sie Zeichen austauschen. Wenn zwei Menschen ihre Kommunikation ver-

schlüsseln, wählen sie ein für andere unbekanntes Zeichen-Zuordnungssystem. Dazu ist grundsätzlich kein besonderes Werkzeug notwendig. Es genügt beispielsweise, eine unbekannte Sprache zu sprechen. Die Verschlüsselung erfüllt zwei Aufgaben: Erstens stellt sie Vertraulichkeit sicher, indem außer den gewünschten Kommunikationspartnern keine andere Person an der Kommunikation teilhaben kann. Zweitens garantiert sie Authentizität: Weil nur die beiden Kommunikationspartner die gegenseitigen Botschaften entschlüsseln können, weiß jeder, daß die Botschaft auch wirklich vom anderen kommt. Die moderne Technik ermöglicht Verschlüsselungen, die nicht mehr einfach „geknackt" werden können. Die Restriktion der Verschlüsselung bedeutet, daß der Staat seine Bürger zwingt, ausschließlich in einem ihm bekannten Zeichensystem zu kommunizieren, so daß der Inhalt ihrer Kommunikation verständlich wird. Das heißt, daß Bürger untereinander nur auf für Dritte potentiell verständliche Weise kommunizieren dürfen. Die Auffassungen in diesem Bereich stehen sich dergestalt gegenüber, daß auf der einen Seite die Verfechter einer frei zugänglichen Kryptographie darin die Möglichkeit erblicken, dem Bürger ein gewisses Maß an Privatheit zu garantieren, während auf der anderen Seite die Befürworter einer Regulierung berechtigte Informationsbedürfnisse des Staates gefährdet sehen, wenn eine staatlich kontrollierte Entschlüsselungsmöglichkeit nicht vorhanden ist.

Hier ist über die aktuelle rechtspolitische Diskussion hinaus eine umfassende grundrechtliche Thematisierung notwendig, die u. a. der Frage nachgehen sollte, wie die informationelle Selbstbestimmung in ihrer Ausprägung als Recht auf kommunikative Selbstbestimmung auch in der multimedialen Welt gewährleistet werden kann.

20.2 Datenschutz im Internet

Das Internet ist das größte Computernetzwerk der Welt. Es wird auch als das „Netz der Netze" bezeichnet und hat sich zum Rückgrat der globalen Informationsgesellschaft entwickelt, allerdings ohne organisierte Verantwortlichkeit und ohne Kontrolle. Das weltweite Internet kennt keine Länder- und Staatsgrenzen, seine Nutzung führt in verschiedenen Staaten zu Datenverarbeitungsvorgängen. In mehr als 140 Staaten bestehen Zugänge, über fünf Millionen Rechner sind angeschlossen, die von mehr als 50 Millionen Menschen genutzt werden.

Bei der Diskussion über die gesellschaftlichen Risiken des Internet wird bisher viel über die Verbreitung von Kinderpornographie sowie über rechtsradikale Inhalte geredet. Weniger Aufmerksamkeit finden dagegen die Gefahren, die das Internet für den Schutz des Persönlichkeitsrechts, nämlich für den Datenschutz, darstellen. Die Datenreisenden hinterlassen mit jedem Tastendruck im Netz vielfältige Spuren, aus denen sensitive Datensammlungen werden: So z. B. – unabhängig vom eigentlichen Inhalt – Bestandsdaten bei den Internetanbietern, Verbindungsdaten in allen beteiligten Knotenrechnern, Entgeltdaten bei den Zugangs- und Inhaltsanbietern. Bestandsdaten sind diejenigen Daten, die dauerhaft gespeichert und bereitgehalten werden, um den Betrieb des Netzes oder die Bereitstellung eines Dienstes zu ermöglichen. Hierzu zählen die Namen und Anschriften der Benutzer sowie deren Adressen für die elektronische Post; je nach Art des Dienstes aber beispielsweise auch die Konto-Nummer des Nutzers von Telebanking. Verbindungsdaten geben Auskunft über die näheren Umstände der Kommunikation. Hierzu gehören Angaben über Kommunikationspartner, z. B. Internet-Adressen des Absenders und Empfängers von elektronischer Post sowie Zeitpunkt und Dauer einer Verbindung. Entgeltdaten sind diejenigen personenbezogenen Angaben, die für Abrechnungszwecke verarbeitet werden. Sie werden aus Verbindungsdaten abgeleitet. Üblicherweise entstehen Entgeltdaten bei den Zugangsanbietern. Anhand der Bestands- und Verbindungsdaten ist leicht nachvollziehbar, wer wann mit wem kommuniziert hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Die über das Internet übertragenen Nachrichten können unberechtigt verändert, gefälscht, verzögert, wiedereingespielt oder unterdrückt werden. Die Gefährdung der Integrität betrifft sowohl den Nachrichteninhalt als auch die Verbindungsdaten. Verschlüsselung kann zwar die unberechtigte Kenntnisnahme von Inhaltsdaten verhindern, grundsätzlich nicht jedoch das Ausspionieren der Verbindungsdaten. „Firewall"-Systeme sollen den mißbräuchlichen Zugriff verhindern. Unter einer Firewall (Brandschutzmauer) wird eine Schwelle zwischen zwei Netzen verstanden, die überwunden werden muß, um Systeme im jeweils anderen Netz zu erreichen. Die Hauptaufgabe einer Firewall besteht darin zu erreichen, daß jeweils nur zugelassene netzübergreifende Aktivitäten möglich sind und daß Mißbrauchsversuche frühzeitig erkannt werden. Die Firewall ist die definierte und kontrollierte Schnittstelle zwischen dem zu schützenden und dem nichtvertrauenswürdigen Netz.

Die im Internet genutzten Dienste können Teledienste wie „electronic banking" sein, sie können Mediendienste wie elektronisches Publizieren sein, sie können Rundfunk wie Internet-Fernsehen sein, sie können Telekommunikation wie elektronische Post sein. Der rechtliche Umgang mit dem Internet unterliegt damit den für diese Dienste geltenden Gesetzen. Die Telekommunikation dem Telekommunikationsgesetz, die Teledienste dem Teledienstegesetz und dem Teledienstedatenschutzgesetz, die Mediendienste dem Mediendienstestaatsvertrag, der Rundfunk dem Rundfunkstaatsvertrag. Nationales Datenschutzrecht ist im internationalen Raum jedoch nur eingeschränkt anwendbar. Ein drängendes Thema der globalen Internetbeziehungen sind daher internationale Rechtsregeln. Der begrenzte räumliche Bereich der nationalen Datenschutzgesetze gestaltet sich angesichts der globalen Struktur des Internet schwierig. Einen ersten Ansatz bietet u. U. Art. 4 der EG-Datenschutzrichtlinie, wonach für die Datenverarbeitung jeweils das nationale Recht des Landes anzuwenden ist, in dem der für die Datenverarbeitung Verantwortliche eine Niederlassung betreibt. Für den Transport gilt jeweils das Recht derjenigen Staaten, in denen die Betreiber der Fernmeldeanlagen ihren Sitz haben. Aber auch europäische Regelungen bleiben wirkungslos, da sie umgangen werden können. Mithin ist in diesem Bereich eine internationale Zusammenarbeit erstrebenswert.

20.3 Die Regelungen des Informations- und Kommunikationsdienste-Gesetzes

Der Bundesrat hat am 4. Juli 1997 dem Informations- und Kommunikationsdienste-Gesetz, besser bekannt unter der Bezeichnung „Multimedia-Gesetz", in der Fassung des Beschlusses des Deutschen Bundestages vom 13. Juni 1997 zugestimmt. Es wurde eine begleitende Entschließung gefaßt, wonach das Gesetz einer ständigen Überprüfung unterzogen werden soll. Ferner ist vorgesehen, in zwei Jahren einen Erfahrungsbericht vorzulegen. Das Gesetzeswerk ist, wie geplant, zusammen mit dem Mediendienstestaatsvertrag (vgl. Tz. 20.4) am 1. August 1997 in Kraft getreten. Es ist in den wesentlichen datenschutzrechtlichen Aussagen mit den Datenschutzbeauftragten des Bundes und der Länder abgestimmt.

Ausgangspunkt für die datenschutzrechtlichen Regelungen ist das verfassungsrechtlich verbürgte Recht auf informationelle Selbstbestimmung. Das traditionelle Datenschutzkonzept wird ergänzt, soweit die Risiken der neuen Dienste dies erforderlich machen.

Die bestehenden Datenschutzkonzepte orientieren sich größtenteils am Muster der zentralen Datenverarbeitung, also an dem, was man in den 70er Jahren vorgefunden hat. In dieser „behüteten" Datenschutzwelt gibt es die Datei, die personenbezogene Daten enthält und von einer verantwortlichen datenverarbeitenden Stelle in einer Datenverarbeitungsanlage verarbeitet oder zu einer solchen übermittelt wird.

In der multimedialen Welt läßt sich dieser Ansatz nicht mehr halten. Denn dort werden personenbezogene Daten von einem Medium in ein anderes überführt und inhaltlich beliebig kombiniert, verändert oder erzeugt, die Daten nicht nur in einer Datenverarbeitungsanlage, sondern im Netz von vielen Beteiligten, aber oftmals ohne einen hierfür verantwortlichen Betreiber und ohne durchgreifende zentrale Kontrollmöglichkeiten verarbeitet.

In den entsprechenden Vorschriften des Informations- und Kommunikationsdienste-Gesetzes sowie des Mediendienstestaatsvertrags wird nun das traditionelle Datenschutzkonzept durch neue Strukturvorgaben ergänzt.

Mit dem Informations- und Kommunikationsdienste-Gesetz wurden neben einer Reihe von Änderungen bereits bestehender Gesetze (Anpassung des Straf- und Ordnungswidrigkeitenrechts, Jugendschutzrechts, Verbraucherschutzrechts und Urheberrechts) drei Gesetze neu geschaffen: Das Teledienstegesetz bezweckt die Schaffung einheitlicher wirtschaftlicher Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste. Das Teledienstedatenschutzgesetz hat die Datenschutzvorschriften für den Betrieb eines Teledienstes zum Inhalt. Das Signaturgesetz enthält Vorgaben für die Rahmenbedingungen der digitalen Signatur.

20.3.1 Teledienstegesetz

Bei dem Gesetz über die Nutzung von Telediensten handelt es sich um Regelungen zur Zugangsfreiheit der Informations- und Kommunikationsdienste und zur Verantwortlichkeit von Diensteanbietern (Provider) bei Telediensten. Diese Dienste werden durch das Merkmal der individuellen Nutzung definiert (§ 2 TDG). Darunter fallen z. B. Dienste wie elektronische Post, aber auch Nutzungsbereiche wie Telebanking, Telearbeit, Telemedizin und Fernlernen. Die zivilrechtliche und strafrechtliche Haftung der Provider ist nach § 5 TDG lediglich dann gegeben, wenn sie von den rechtswidrigen fremden Inhalten, die sie zur Nutzung bereithalten, Kenntnis haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern. Kenntnis im Sinne des Gesetzes ist nur positives Wissen. Daraus folgt beispielsweise, daß die reine Vermittlung des Zugangs zu fremden Inhalten keine haftungsrechtlichen Folgen hat.

20.3.2 Teledienstedatenschutzgesetz

Im Hinblick auf die besondere Bedeutung des Datenschutzes hat sich die Bundesregierung entschlossen, die diesbezüglichen Vorschriften aus dem ursprünglichen Entwurf des Teledienstegesetzes in ein besonderes Gesetz über den Datenschutz bei Telediensten auszulagern. Nach der Bestimmung des Anwendungsbereichs (§§ 1 und 2 TDDSG) werden in den §§ 3 und 4 TDDSG die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten formuliert. Verglichen mit dem Bundesdatenschutzgesetz, das bislang einschlägig war, gehen die Regelungen erfreulich weit. Hier finden sich nach Einschätzung des LfD richtungsweisende Ansätze, die für die weitere Datenschutzgesetzgebung Bedeutung erlangen werden. Aus diesem Grunde sind nachfolgend die beiden letztgenannten Vorschriften im Wortlaut wiedergegeben:

„§ 3 TDDSG – Grundsätze für die Verarbeitung personenbezogener Daten –

(1) Personenbezogene Daten dürfen vom Diensteanbieter zur Durchführung von Telediensten nur erhoben, verarbeitet und genutzt werden, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.

(2) Der Diensteanbieter darf für die Durchführung von Telediensten erhobenen Daten für andere Zwecke nur verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.

(3) Der Diensteanbieter darf die Erbringung von Telediensten nicht von einer Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig machen, wenn dem Nutzer ein anderer Zugang zu diesen Telediensten nicht oder in nicht zumutbarer Weise möglich ist.

(4) Die Gestaltung und Auswahl technischer Einrichtungen für Teledienste hat sich an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen.

(5) Der Nutzer ist vor der Erhebung über Art, Umfang, Ort und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten. Bei automatisierten Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten, ist der Nutzer vor Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muß für den Nutzer jederzeit abrufbar sein. Der Nutzer kann auf die Unterrichtung verzichten. Die Unterrichtung und der Verzicht sind zu protokollieren. Der Verzicht gilt nicht als Einwilligung im Sinne der Absätze 1 und 2.

(6) Der Nutzer ist vor Erklärung seiner Einwilligung auf sein Recht auf jederzeitigen Widerruf mit Wirkung für die Zukunft hinzuweisen. Absatz 5 Satz 3 gilt entsprechend.

(7) Die Einwilligung kann auch elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, daß
1. sie nur durch eine eindeutige und bewußte Handlung des Nutzers erfolgen kann,
2. sie nicht unerkennbar verändert werden kann,
3. ihr Urheber erkannt werden kann,
4. die Einwilligung protokolliert wird und
5. der Inhalt der Einwilligung jederzeit vom Nutzer abgerufen werden kann.

§ 4 TDDSG – Datenschutzrechtliche Pflichten des Diensteanbieters –

(1) Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

(2) Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, daß
1. der Nutzer seine Verbindung mit dem Diensteanbieter jederzeit abbrechen kann,
2. die anfallenden personenbezogenen Daten über den Ablauf des Abrufs oder Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht werden, soweit nicht eine längere Speicherung für Abrechnungszwecke erforderlich ist,
3. der Nutzer Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,
4. die personenbezogenen Daten über die Inanspruchnahme verschiedener Teledienste durch einen Nutzer getrennt verarbeitet werden; eine Zusammenführung dieser Daten ist unzulässig, soweit dies nicht für Abrechnungszwecke erforderlich ist.

(3) Die Weitervermittlung zu einem anderen Diensteanbieter ist dem Nutzer anzuzeigen.

(4) Nutzungsprofile sind nur bei Verwendung von Pseudonymen zulässig. Unter einem Pseudonym erfaßte Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden."

Damit ist erstmals der Grundsatz der Datenvermeidung und der Datensparsamkeit gesetzlich festgeschrieben.

Die §§ 5 und 6 enthalten die bereichsspezifischen Voraussetzungen für die Verarbeitung von Bestands- und Abrechnungsdaten. Eine zweckentfremdende Nutzung dieser Daten (etwa für Werbung oder Marktforschung) ist an die ausdrückliche Einwilligung der nutzenden Person gebunden. In § 7 wurde ein umfassendes Auskunftsrecht des Nutzers verankert. Erweiterte Kontrollmöglichkeiten der Aufsichtsbehörden – nämlich die anlaßfreie Kontrolle – bietet § 8 TDDSG.

Mit der Entstehungsgeschichte des Teledienstedatenschutzgesetzes ist ein weiterer Erfolg des Datenschutzes verbunden. Im Entwurf der Bundesregierung vom 20. Dezember 1996 sollten die Anbieter von Telediensten dazu verpflichtet werden, insbesondere der Polizei und den Nachrichtendiensten Auskunft über die Bestandsdaten der Kunden hinsichtlich der Begründung und inhaltlichen Ausgestaltung der Vertragsverhältnisse zu erteilen. Zu diesen Bestandsdaten gehören neben Namen und Anschriften auch Angaben über die Art der Nutzung der Dienstleistung, z. B. die Kontonummer und ein etwaiger Verfügungsrahmen beim Telebanking. Der LfD hatte daraufhin im Januar 1997 die Landesregierung gebeten, sich im Bundesrat für eine Streichung dieser Auskunftspflichten einzusetzen. In seinem Schreiben warb er für die Erwägung folgender Gesichtspunkte: „Soweit die Strafverfolgungsbehörden Kenntnis über Bestandsdaten haben müssen, um Straftaten aufzuklären, die mittels Telediensten begangen wurden, ist zu berücksichtigen, daß die Befugnisse aus der Strafprozeßordnung, z. B. die Beschlagnahmevorschriften einschließlich der Pflicht der Diensteanbieter zur Zeugenaussage, auch ohne die geplante Sonderregelung in § 5 Abs. 3 TDDSG-E vorhanden sind und ausreichen. Was die geltende Rechtslage in Rheinland-Pfalz anbelangt, so finden sich

angemessene Vorschriften in § 25 a Abs. 1 POG, der die allgemeinen polizeilichen Befugnisse bei der Informationserhebung und Informationsverarbeitung regelt." Dieses Thema war auch Gegenstand einer Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom April 1997 (vgl. Anlage 13). Ihre beharrliche Ablehnung im Hinblick auf die geplante Verpflichtung von Teledienstanbietern, Kundendaten an Sicherheitsbehörden zu übermitteln, hat Wirkung gezeigt: Die Bestimmung des § 5 Abs. 3 TDDSG-E ist vom Deutschen Bundestag ersatzlos gestrichen worden.

20.3.3 Signaturgesetz

Das Signaturgesetz enthält grundsätzliche organisatorische Anforderungen für die Unverfälschtheit elektronischer Dokumente im Rechtsverkehr. Vorgesehen ist eine privatwirtschaftlich organisierte Infrastruktur für die Zuordnung von Schlüsseln zu natürlichen Personen. Es wird damit möglich, rechtsgeschäftlich relevante Erklärungen (z. B. im Internet) abzugeben. Das Gesetz sieht die Einrichtung von Zertifizierungsstellen vor, die Signaturschlüsselzertifikate an Interessierte ausgeben. Das Signaturgesetz ermöglicht auch pseudonymes Handeln in elektronischen Netzen. Die Ausstellung eines Signaturschlüsselzertifikats auf ein Pseudonym ist in § 7 SigG geregelt. Allerdings muß dieser Umstand für die Kommunikationspartner erkennbar sein, so daß sie entscheiden können, ob unter diesen Bedingungen (ein Teilnehmer tritt nicht unter seinem richtigen Namen auf) die Kommunikation fortgeführt oder abgebrochen werden soll.

Ganz bewußt enthält das Signaturgesetz zur politisch umstrittenen Frage eines Verschlüsselungsverbotes keine Regelung. Die Begründung des Entwurfs stellt dazu fest: „Ob unabhängig davon unter besonderen Aspekten spezielle ‚Kryptoregelungen' erforderlich sind, ist nicht Gegenstand des Gesetzentwurfes. Die Funktionen Signatur und Verschlüsselung sind technisch wie rechtlich völlig eigenständig zu betrachten" (vgl. Bundesratsdrucksache 966/96, S. 30).

Aus der Sicht des Datenschutzes sind digitale Signaturverfahren zu begrüßen, denn sie tragen zur Wahrung der Datensicherheit bei.

20.4 Der Staatsvertrag über Mediendienste

Bereits 1983 haben die Bundesländer im Bildschirmtext-Staatsvertrag Regelungen zu Informationsdiensten auf Abruf getroffen. Die grundlegenden technischen und strukturellen Veränderungen der letzten Jahre führten zu einem dringenden Anpassungsbedarf. So wurde durch die Entwicklung der neuen Online-Dienste dem Bildschirmtext-Staatsvertrag, der auf einer strikten Trennung zwischen der Betreiberebene und den Inhaltsanbietern beruhte, das Fundament entzogen. Zwischen Bund und Ländern haben intensive Gespräche mit dem Ziel stattgefunden, zu möglichst einheitlichen Regelungen auf Bundes- und Landesebene für alle neuen Multimedia-Dienste zu gelangen. Was den jeweiligen Geltungsbereich anbelangt, wurde vereinbart, daß die bundes- und landesrechtlichen Regelungen dergestalt voneinander abgegrenzt werden, daß der Bund Regelungen für Angebote im Bereich der Individualkommunikation (Teledienste) trifft, während die Länder das Angebot und die Nutzung von an die Allgemeinheit gerichteten Informations- und Kommunikationsdiensten (Mediendiensten) regeln.

Die datenschutzrechtlichen Bestimmungen sind weitgehend wortgleich mit denen des Teledienstedatenschutzgesetzes. Unterschiede ergeben sich für Anbieter von journalistisch-redaktionell gestalteten Angeboten, in denen vollständig oder teilweise Inhalte periodischer Druckerzeugnisse in Text oder Bild wiedergegeben oder in periodischer Folge Texte verarbeitet werden. Sie müssen zusätzlich einen Verantwortlichen mit Angabe des Namens und der Anschrift benennen. Ferner wird eine Sorgfaltspflicht für derartige journalistische Angebote aufgestellt. Eine Sonderregelung ist ebenfalls die Aufnahme von Gegendarstellungen.

Die Datenschutzkontrolle der Mediendienste wurde der nach Landesrecht zuständigen Aufsichtsbehörde zugeordnet.

20.5 Das Landesgesetz zum Mediendienste-Staatsvertrag

Das Landesgesetz enthält die nach Art. 101 Satz 2 der Verfassung für Rheinland-Pfalz erforderliche Zustimmung des Landtags zu dem Mediendienste-Staatsvertrag. Außerdem werden die Aufsichtsbehörden bestimmt.

Der Gesetzentwurf wies in § 2 Abs. 1 Satz 3 dem LfD die Überwachung der Datenschutzbestimmungen für den öffentlichen Bereich zu. Diese Regelung stand nur insofern in Einklang mit § 2 Abs. 5 des Landesgesetzes zu dem Staatsvertrag über den Rundfunk im vereinten Deutschland, als der LfD die Einhaltung der Datenschutzvorschriften des Bildschirmtext-Staatsvertrages zu beobachten hatte. In § 2 Abs. 2 des Entwurfs eines Landesgesetzes zum Mediendienste-Staatsvertrag war indessen festgelegt, daß diejenige Behörde, die nach den Bestimmungen des Absatzes 1 für die Überwachung zuständig ist, auch die Zuständigkeit für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 20 des Mediendienste-Staatsvertrages erhält. Die Umsetzung dieser Regelung hätte bedeutet, daß der LfD mit exekutiven Befugnissen ausgestattet werden müßte, die dem in Rheinland-Pfalz bewährten Beauftragtenmodell völlig fremd sind. In seinem 15. Tb., Tz. 3.1.2.7 hat der LfD in der Diskussion zur Struktur der Kontrollstelle im Hinblick auf die Umsetzung der EG-Datenschutzrichtlinie darauf aufmerksam gemacht, daß die „Stellung der Landesbeauftragten für den Datenschutz (. . .) 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."

Der LfD hat darum gebeten, bei den parlamentarischen Beratungen des Gesetzentwurfs diesen Erwägungen Rechnung zu tragen und die vorgesehenen Exekutivbefugnisse des LfD dem Ministerium des Innern und für Sport zuzuweisen. Daraufhin hat der Medienpolitische Ausschuß beschlossen, dem Landtag die Annahme des Gesetzentwurfs zu empfehlen mit der Maßgabe, daß bezüglich Zuwiderhandlungen gegen datenschutzrechtliche Bestimmungen des Mediendienste-Staatsvertrages das Innenministerium die zuständige Behörde für die Verfolgung und Ahndung von Ordnungswidrigkeiten ist.

20.6 Digitales Fernsehen

Im Berichtszeitraum hat die Markteinführung des digitalen Fernsehens begonnen. Neben der Vervielfachung von Übertragungskapazitäten werden neue Sende- und Abrechnungsformen ermöglicht. Ein Beispiel dafür ist „pay-per-view", also die Einzelabrechnung der jeweils gesehenen Sendungen.

Zu diesem Thema hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ebenfalls eine Entschließung verabschiedet (vgl. Anlage 9). Die zentrale datenschutzrechtliche Forderung lautet: Auch beim digitalen Fernsehen muß (optional) eine unbeobachtete Mediennutzung möglich bleiben. So sind die technischen Voraussetzungen für datenschutzfreundliche Zugriffs- und Abrechnungsverfahren vorhanden, beispielsweise in Form von vorausbezahlten Chipkarten. Es besteht nämlich die Gefahr, daß Mediennutzungsprofile – bezogen auf den einzelnen Konsumenten – erstellt werden. Auskünfte über persönliche Vorlieben, Interessen und Sehgewohnheiten wären dann auf Knopfdruck möglich.

Diese Gesichtspunkte sollten anläßlich der Vorarbeiten zum Vierten Rundfunkänderungsstaatsvertrag, der insbesondere Regelungen zum digitalen Fernsehen enthalten wird, berücksichtigt werden.

20.7 Anwendung des neuen Rechts

Die Grenzen zwischen Datenverarbeitung, Telekommunikation und Rundfunk sind fließend. Es ist zu begrüßen, daß nunmehr in Deutschland begonnen wurde, einen Ordnungsrahmen für das Telekommunikations- und Medienrecht zu schaffen. In der Begründung zum Informations- und Kommunikationsdienstegesetz ist die Abgrenzung zwischen Telediensten und Rundfunk folgendermaßen dargestellt: „Zielrichtung der Informations- und Kommunikationsdienste ist nicht die auf öffentliche Meinungsbildung angelegte massenmediale Versorgung (. . .), sondern die durch den Nutzer bestimmbare Kommunikation." Zur Abgrenzung zwischen Telediensten und dem Telekommunikationsgesetz wird ausgeführt: „Die Informations- und Kommunikationsdienste setzen die Übermittlung von Inhalten mittels Telekommunikation im Sinne des § 3 Nr. 16 TKG voraus. Das Informations- und Kommunikationsdienstegesetz regelt die Nutzung der mittels Telekommunikation übermittelten Inhalte, nicht die Telekommunikation selbst."

Es wird noch einige Zeit dauern, bis die Datenschutzbeauftragten des Bundes und der Länder, die Aufsichtsbehörden sowie die Rundfunk-Datenschutzbeauftragten hinsichtlich der Anwendbarkeit und Einordnung des neuen Rechts Einigkeit erzielen werden. Auch die Frage nach der Datenschutz-Kontrollzuständigkeit spielt eine wichtige Rolle.

Die Landschaft der neuen Dienste ist sehr vielgestaltig. Auf Netzebene gilt es beispielsweise Corporate Networks, private Funkanlagen, Kabelanlagenbetreiber, Mobilfunkbetreiber, das Deutsche Forschungsnetz, allgemeine Behördennetze, Nebenstellenanlagen in Firmen und in der öffentlichen Verwaltung sowie länderübergreifende Polizeinetze rechtlich einzuordnen. Bei den Diensteanbietern treten öffentlich-rechtliche Anbieter (z. B. Internet-Zugang für öffentliche Stellen im Hinblick auf Mitarbeiter und Studenten) neben kommerziellen Anbietern mit und ohne eigene Netze auf; ausländische Anbieter werden den Netz-Zugang zum Sprachtelefondienst innerhalb und außerhalb der Europäischen Union nebst Internet-Telefonie anbieten. Um Inhalte geht es beim öffentlich-rechtlichen und privaten Rundfunk sowie bei Tele- und Mediendiensten. Hier sind z. B. angesiedelt telefonische Zusatzdienste wie die Telefonauskunft (durch Netzbetreiber und sonstige Anbieter) sowie die „voicemailbox" (angeboten von Netzbetreibern und sonstigen Anbietern), Fernwirkdienste im Angebot durch öffentliche Stellen (z. B. Eigenbetriebe) und private Einrichtungen (z. B. Wachdienste), Telearbeit (abgewickelt von öffentlichen und privaten Arbeitgebern), Telemedizin (angeboten von öffentlichen Stellen und niedergelassenen Ärzten), Teleunterricht (z. B. durchgeführt von Fernuniversitäten), auch Fernsehtext (mit journalistischer Aufbereitung durch den Anbieter und ohne journalistische Aufbereitung bei Direktübernahme von Dritten) gehört dazu.

In diesem Zusammenhang muß der Gefahr begegnet werden, daß der Bereich immer kleiner wird, in dem sich der Bürger unbeobachtet verhalten und bewegen kann. Den „gläsernen Bürger" darf es in unserem Rechtsstaat nicht geben. Ob interaktives Fernsehen, Multimedia oder Datenautobahn – auf leisen Sohlen schleichen sich neue Techniken in unseren Alltag ein. Auch die öffentliche Verwaltung treibt die Vernetzung beständig voran. In der multimedialen Zukunft wird es darauf ankommen, daß ein solch kostbares Gut wie das informationelle Selbstbestimmungsrecht auf der Datenautobahn nicht unter die Räder gerät.

21. Technischer und organisatorischer Datenschutz

21.1 Kontroll- und Beratungstätigkeit

Im Berichtszeitraum wurden unter technisch-organisatorischen Gesichtspunkten in 40 Fällen örtliche Feststellungen nach § 24 Abs. 1 LDSG in unterschiedlichen Bereichen der staatlichen und kommunalen Verwaltung getroffen. Ergänzt wurden diese durch 25 Beratungen vor Ort nach § 24 Abs. 4 LDSG. Die Anzahl der Kontrollen liegt unter der des vorhergehenden Berichtszeitraumes, da der zuständige Mitarbeiter dem LfD für einen längeren Zeitraum nur mit einem Teil seiner Arbeitszeit zur Verfügung stand.

Feststellungen wurden u. a. getroffen bei:

- einer Bezirksregierung
- dem Daten- und Informationszentrum Rheinland-Pfalz
- einem Katasteramt
- mehreren Krankenkassen
- einzelnen Kreisverwaltungen
- dem Landesamt für Soziales, Jugend und Versorgung
- dem Landeskriminalamt
- dem Landesmedienzentrum Koblenz
- der Landesversicherungsanstalt Speyer
- einem Ministerium
- der Oberfinanzdirektion Koblenz
- einer Sparkasse
- einem Sozialamt
- dem Sparkassen- und Giroverband
- mehreren Staatsanwaltschaften
- einer Universität
- und dem Verfassungsschutz.

Die Kontrollen erfolgten sowohl anlaßbezogen, z. B. aufgrund von Eingaben oder Anmeldungen, als auch als allgemeine Prüfungen der getroffenen technisch-organisatorischen Maßnahmen beim Einsatz der Informationstechnik.

Im Vordergund der Prüfungen standen dabei regelmäßig die Zugriffskontrolle, die Nachvollziehbarkeit der automatisierten Verarbeitung und die Löschung nicht mehr erforderlicher personenbezogener Daten. Die genannten Bereiche haben sich als neuralgische Punkte insbesondere dort erwiesen, wo Verfahren von den öffentlichen Stellen selbst entwickelt wurden. In dem Bemühen um eine mit wenig Aufwand zu realisierende, praxisgerechte Lösung treten datenschutzrechtliche Gesichtspunkte häufig in den Hintergrund. In Fällen, in welchen das Sicherheitsniveau aus Datenschutzsicht unzureichend war, hat der LfD Anpassungen empfohlen.

Zunehmend wurde der LfD im Vorfeld geplanter Umstrukturierungen des IT-Einsatzes oder im Zusammenhang mit der Erstellung von Sicherheitskonzepten um Beratung in sicherheitstechnischen Fragen gebeten. Häufig war dies auf eine Anregung des behördlichen Datenschutzbeauftragten oder der Personalvertretung der jeweiligen öffentlichen Stelle zurückzuführen. Daneben hat der LfD in Einzelfragen zu technisch-organisatorischen Punkten Unterstützung geleistet.

Die Schulungsaktivitäten wurden im bisherigen Umfang beibehalten.

21.2 Technisch-organisatorische Datenschutzfragen in ausgewählten Bereichen

21.2.1 DNS-Spurendokumentation beim Landeskriminalamt

Im Rahmen kriminaltechnischer Untersuchungen betreibt das Landeskriminalamt Rheinland-Pfalz auf einem Arbeitsplatzrechner ein Verfahren zur Dokumentation von DNS-Analysen. Bei den Analysedaten handelt es sich um sogenannte „Marker", d. h. typische DNS-Sequenzen. Nach dem gegenwärtigen Kenntnisstand sind diese Marker nicht kodierend, d. h. sie erlauben keinen Rückschluß auf Erbanlagen oder genetische Dispositionen (zu rechtlichen Fragen in diesem Zusammenhang s. Tz. 7.1.2 und Anlage 13).

Bei der DNS-Spurendokumentation werden einerseits Datensätze mit Analysedaten bekannter Spurenträger (Vergleichsmaterial) und andererseits Analyseergebnisse, für die eine personenmäßige Zuordnung nicht vorliegt (Spurenmaterial), verarbeitet.

Im Rahmen einer Kontrolle des Verfahrens durch den LfD wurde festgestellt, daß die Art der verarbeiteten Daten nicht über die in der Errichtungsanordnung genannten Angaben hinausgeht. Insbesondere war nicht erkennbar, daß neben den für die Identifizierung erforderlichen „Markern" weitere DNS-Angaben gespeichert werden.

Die DNS-Datei wurde seinerzeit kurzfristig, vor dem Hintergrund drastisch angestiegener Serienstraftaten bestimmter Tätergruppen, eingerichtet. Das derzeitige Verfahren kann daher aus Sicht des LfD nicht als endgültige Lösung angesehen werden. Die Realisierung auf der Grundlage eines Tabellenkalkulationsprogramms wurde dabei als problematisch erachtet. Aufgrund der umständlichen und damit fehleranfälligen Handhabung, insbesondere bei gewachsenem Datenbestand, der unzureichenden Möglichkeiten der Eingabekontrolle sowie der fehlenden automatisierten Überwachung von Wiedervorlage- und Löschfristen sollte diese Form der Realisierung überdacht werden.

Das Landeskriminalamt hat sich dem grundsätzlich angeschlossen. Der Anregung des LfD, eine Lösung auf der Basis eines Datenbankverwaltungsprogramms in Betracht zu ziehen und dabei die genannten Gesichtspunkte zu berücksichtigen, soll gefolgt werden. Weiterhin wurden Empfehlungen zu Verbesserungen im Bereich der Zugriffs-, Speicher- und Eingabekontrolle umgesetzt, u. a. werden die Daten künftig in verschlüsselter Form gespeichert.

Für die ebenfalls problematisierte Frage der Löschung der Datensätze des Vergleichsmaterials wurde eine vorläufige Regelung gefunden. Danach erfolgt künftig anhand eines Wiedervorlagedatums alle zwölf Monate ab der Erfassung bei allen personenbezogenen Datensätzen eine Relevanzüberprüfung. Die für Polizeidienststellen anderer Bundesländer oder des Bundes im Rahmen der Amtshilfe gespeicherten Daten werden nach zwölf Monaten ebenfalls auf Relevanz überprüft und spätestens nach zwei Jahren gelöscht.

Gegenwärtig ist vorgesehen, im Zusammenhang mit dem Aufbau ähnlicher Verfahren in anderen Bundesländern die rheinland-pfälzische Lösung zu überarbeiten und anzupassen. Gegen eine abgestimmte Struktur von DNS-Dateien bestehen aus Sicht des LfD keine Bedenken, soweit die Empfehlungen der 53. Konferenz der Datenschutzbeauftragten zu DNS-Analysedateien berücksichtigt werden (vgl. Anlage 13). Dies gilt insbesondere im Hinblick auf eine regelmäßige automationsunterstützte Relevanzprüfung bzw. Löschung der gespeicherten Daten.

21.2.2 Überwachung des Fernmeldeverkehrs

21.2.2.1 Überwachung von ISDN- und Mobilfunktelefonaten durch das Landeskriminalamt

Vor dem Hintergrund der Digitalisierung des Telefonnetzes der Deutschen Telekom AG und der Einführung von Mobilfunknetzen wurden die für die Telefonüberwachung vorhandenen Einrichtungen der Polizei der technischen Entwicklung angepaßt. Im Hinblick auf die eingesetzte Technik hat der LfD beim Landeskriminalamt örtliche Feststellungen getroffen.

Danach verfügt das LKA seit einiger Zeit über die technischen Möglichkeiten zur Überwachung von ISDN- und Mobilfunktelefonaten. Die Telefonüberwachung setzt auf den von den Netzbetreibern nach § 8 FÜV zur Verfügung gestellten Schnittstellen auf. Damit besteht grundsätzlich die Möglichkeit, Überwachungen funkzellen- und vermittlungsübergreifend im gesamten Bereich der Bundesrepublik durchzuführen.

Nach Vorliegen eines TÜ-Beschlusses beim Netzbetreiber richtet das Network Service Center (NSC) die Überwachungsmaßnahme ein und schafft die Voraussetzungen, um bei einer Kommunikation bzw. Aktivität des zu überwachenden Anschlusses die Sprachdaten zum Bedarfsträger zu übermitteln.

Die entsprechenden Anschlüsse des LKA sind ausschließlich für die Übertragung überwachter Telefonate vorgesehen. Zwischen dem NSC und dem LKA-Anschluß erfolgt eine gegenseitige Authentifizierung gem. § 12 Abs. 3 FÜV. Andere Telefonate, die z. B. irrtümlich einen solchen Anschluß angewählt haben, werden abgewiesen.

Bei der Überwachung von Festanschlüssen werden die Verbindungsdaten in Form von verbindungsbegleitenden Informationen am gleichen Anschluß zur Verfügung gestellt. Bei der Überwachung von Mobiltelefonen werden die Verbindungsdaten als sog. S-Records zu einem Datex-P-Anschluß übermittelt. Die S-Records enthalten die Angaben Datum/Uhrzeit, Dauer der Verbindung, Anschluß- bzw. Zielrufnummer und Funkzellenkennung.

Die TÜ-Daten werden von einem angeschlossenen Rechner entgegengenommen, dabei wird gleichzeitig ein Ausdruck der Verbindungsdaten für die TÜ-Akte erstellt. Eine Speicherung der Verbindungsdaten der Gespräche erfolgt bislang nicht. Abhängig von der Art des Telefonats werden die Gesprächsdaten entweder in analoge Signale umgewandelt und im herkömmlichen Ver-

fahren auf Magnetbandkassetten aufgezeichnet oder ohne Umwandlung in digitaler Form auf einem System mit magneto-optischem Datenträger (MOD) unter einer laufenden, nicht änderbaren Nummer gespeichert. Das eingesetzte System verfügt lediglich über ein MOD-Laufwerk, womit die bisherige Erstellung eines Beweis- und eines Arbeitsbandes entfällt. Alle Daten werden ausschließlich auf dem Originaldatenträger gespeichert.

Neben dem Gesprächsinhalt werden Datum und Uhrzeit des Gesprächs sowie die Nummer des überwachten Anschlusses aufgezeichnet. Die genannten Angaben können über eine vorhandene Suchfunktion für das gezielte Abspielen bestimmter Gespräche genutzt werden. Die Möglichkeit der automatisierten Auswertung der Gesprächsinhalte, etwa anhand bestimmter Suchbegriffe, besteht nicht. Die Speicherkapazität der MOD von 1,2 Gigabyte erlaubt die Aufzeichnung von Telefonaten mit einer Gesamtdauer von ca. 30 Stunden. Ein Überspielen der Gesprächsdaten von MOD auf Kassette ist möglich.

Die Überwachungseinrichtung ist in besonders gesicherten Räumen installiert, der Zugriff auf die gespeicherten Daten erfordert eine Benutzeranmeldung und die Eingabe eines Paßwortes. Anmeldungen sowie teilweise die Art der Nutzung (z. B. Löschung) werden protokolliert.

Die im Rahmen der Überwachung digitaler Mobilfunknetze eingeführte Verfahrensweise ist ein erster Schritt zur Ablösung der bisherigen Technik für die Telefonüberwachung in Rheinland-Pfalz. Das Verfahren eignet sich allgemein für die Überwachung und digitale Speicherung von Gesprächen, d. h. sowohl für Mobilfunktelefonate als auch für Gespräche im Festnetz.

Der LfD hat das Verfahren in technischer Hinsicht unter folgenden Gesichtspunkten problematisiert:

– Die vom Netzbetreiber zur Verfügung gestellten Daten umfassen neben den eigentlichen Gesprächsdaten auch Verbindungsdaten, bei eingehenden Anrufen u. a. die Nummer des Anschlusses sowie Angaben über die Funkzelle, von welcher aus das Gespräch geführt wurde. Je nach Größe der Funkzelle kann damit der Standort eines Gesprächsteilnehmers bis auf mehrere hundert Meter genau bestimmt werden. Dies wurde in der Vergangenheit bereits bei der Aufklärung von Straftaten genutzt.

Nach Auskunft des LKA wird die Standortbestimmung z. Z. nur in Einzelfällen und nach ausdrücklicher Aufforderung der Staatsanwaltschaft vorgenommen. In Ermangelung der Kenntnis der Funkzellensystematik muß hierfür gegenwärtig der Netzbetreiber angesprochen werden. Die beschriebene Möglichkeit könnte an Bedeutung gewinnen, falls regelmäßig alle Verbindungsdaten automatisiert auswertbar gespeichert werden und mit überschaubarem Aufwand die Bildung von Bewegungsprofilen der Teilnehmer aller erfaßten Mobiltelefonate möglich ist. Zur rechtlichen Problematik dieser Nutzung s. Anlage 17, Nr. 8.

– Die digitale Speicherung der Gesprächs- und (teilweise) der Verbindungsdaten auf MOD erlaubt die gezielte Suche und Löschung einzelner Gespräche sowie u. U. die Veränderung von Daten. Da gegenüber früher kein separates „Beweisband" mehr existiert, stellt sich die Frage nach der Authentizität und Integrität der gespeicherten Daten bzw. der Beweiseignung des neuen Speichermediums. Datenänderungen sind gegenwärtig im nachhinein nicht erkennbar, Abhilfe könnte jedoch durch technische Maßnahmen (z. B. „Versiegelung" der Daten mit einer Prüfsumme) bzw. eine Protokollierung der Zugriffe auf die Daten überwachter Gespräche erfolgen.

Das Ministerium des Innern und für Sport hat die Empfehlungen des LfD aufgegriffen. Das Ergebnis der Prüfung, ob der Einsatz von Prüfsummen von den Herstellern der Überwachungstechnik zu realisieren ist, steht noch aus. Unabhängig davon teilt das Ministerium die Auffassung, daß die Authentizität der gespeicherten Daten und ein absoluter Schutz gegen Änderungen sichergestellt werden muß. Weiterhin ist beabsichtigt, bei digitalen Aufzeichnungsanlagen künftig eine umfassende Protokollierung vornehmen zu lassen.

– Die Daten aus der Überwachungsmaßnahme werden an eigens hierfür reservierten ISDN-Anschlüssen zur Verfügung gestellt. Auf der Verbindungsleitung zwischen dem Network Service Center des Betreibers und der Überwachungsstelle werden somit ausschließlich Gespräche aus Telefonüberwachungen übertragen. Die Tatsache, daß und in welchem Umfang für bestimmte Anschlüsse TÜ-Maßnahmen durchgeführt werden, ist auch gegenüber dem Personal des Netzbetreibers (z. B. in Vermittlungsstellen oder bei Wartungsarbeiten) geheimhaltungsbedürftig. Die Möglichkeit einer Verschlüsselung bei der Übermittlung der Daten überwachter Telefonate vom NSC an die Bedarfsträger sollte daher aus Sicht des LfD geprüft werden.

Das Ministerium hat die Empfehlungen des LfD zum Anlaß genommen, die Frage der Verschlüsselung in den entsprechenden Bundesgremien zu thematisieren. Gleiches gilt für die – aus Sicht des Datenschutzes – empfehlenswerte Verschlüsselung der gespeicherten Daten auch auf dem Datenträger als Schutz vor unbefugter Nutzung.

– Die optischen Datenträger besitzen eine erhebliche Speicherkapazität (ca. 30 bis 40 Stunden Gesprächsaufzeichnung pro Platte). Aus datenschutzrechtlicher Sicht wäre in diesem Zusammenhang verbindlich anzuordnen, daß analog zur bisherigen Regelung für jede TÜ-Maßnahme ein besonderer Datenträger zu verwenden ist. Weiterhin sollte festgelegt werden, daß die Datenträger Bestandteil der TÜ-Akte werden und ein Überspielen der Gesprächsdaten – z. B. auf Kassetten – nur zu Arbeitszwecken erfolgen darf. Die beweissichernde Grundlage müßte jedoch das originale Speichermedium bleiben.

Nach Mitteilung des Ministeriums soll für jede TÜ-Maßname ein gesonderter Datenträger eingesetzt werden, der nach Abschluß der Maßnahme zu den Akten zu nehmen ist.

Der LfD wird die Umsetzung seiner Empfehlungen im Zusammenhang mit der vorgesehenen Modernisierung der im Bereich der polizeilichen Telekommunikationsüberwachung eingesetzten Technik weiter verfolgen.

21.2.2.2 Neukonzeption der Überwachung des Fernmeldeverkehrs

Die Entwicklung der Telekommunikation, sowohl bei der Technik als auch in bezug auf die Zahl der Betreiber, ist für die Überwachung des Fernmeldeverkehrs durch die Strafverfolgungsbehörden in Rheinland-Pfalz in mehrfacher Hinsicht bedeutsam. So wurde seitens der Polizei darauf hingewiesen, daß aufgrund der Digitalisierung des Netzes der Deutschen Telekom die vorhandene Technik für die Überwachung analoger Gespräche und Telefaxe nur noch für einen begrenzten Zeitraum genutzt werden kann und für die Überwachung neu hinzukommender Kommunikationsdienste ungeeignet ist. Bestehende Nachfolgelösungen haben lediglich Pilotcharakter.

Das Ministerium des Innern und für Sport beabsichtigt, die für die Telekommunikationsüberwachung eingesetzte Technik zu modernisieren. Der LfD hat zum Entwicklungskonzept Stellung genommen und die Konkretisierung bestimmter Anforderungen in den Ausschreibungsunterlagen angeregt.

Im zwischenzeitlich erstellten Anforderungskatalog für die Ausschreibung des Systems wurden die Empfehlungen des LfD zur Datenträgerverwaltung, Protokollierung, Zugriffskontrolle und der Löschung von Verteidigertelefonaten aufgegriffen und im Grundsatz berücksichtigt. Positiv hervorzuheben ist, daß insbesondere eine umfassende Protokollierung und damit Nachvollziehbarkeit der Nutzung des Systems erfolgen soll.

Der LfD hat weiterhin die aus seiner Sicht bestehende Notwendigkeit betont, die einer Fernmeldeüberwachung entstammenden Daten zur Sicherung der Vertraulichkeit bei der Übertragung auf öffentlichen Kommunikationswegen zu verschlüsseln. Angesichts der Sensibilität der einem Eingriff in das Fernmeldegeheimnis entstammenden Daten und im Blick auf die mögliche Nutzung anderer Übertragungswege als das Festnetz der Telekom sowie die steigende Zahl privater Telekommunikationsanbieter gewinnt dieser Gesichtspunkt an Bedeutung. Außer für die eigentlichen Gesprächsinhalte gilt dies insbesondere für die im Rahmen des Zugriffs auf das System übertragenen Paßworte. Für die anstehende Ausschreibung wurde daher empfohlen, die Forderung nach Unterstützung etwaiger Verschlüsselungslösungen, z. B. durch eine Schnittstelle für den Einsatz entsprechender Programme, aufzunehmen.

Der Einsatz von Verschlüsselungs- und Signaturverfahren zur Sicherung polizeisensitiver Daten wird nach Auskunft des Ministeriums gegenwärtig in polizeilichen Arbeitsgruppen auf Bundesebene erörtert. Der LfD hat darum gebeten, dabei die genannten Aspekte zu berücksichtigen und ihn über die weitere Entwicklung zu unterrichten.

21.2.3 Elektronische Zeiterfassung bei den obersten Landesbehörden

Für den Bereich der Landesregierung, mit Ausnahme des Ministeriums der Justiz sowie des Landtags, wurde ein einheitliches Verfahren zur elektronischen Erfassung und Abrechnung der Arbeitszeit eingeführt. Die einzelnen Ressorts betreiben dabei die jeweiligen Anwendungen in eigener Verantwortung.

Der LfD wurde frühzeitig an den Planungen beteiligt. Die aus seiner Sicht erforderlichen Maßnahmen für eine datenschutzgerechte Ausgestaltung des Verfahrens wurden dabei weitgehend in den Entwurf einer Musterdienstvereinbarung und in die im Rahmen der Beteiligung der Personalvertretungen abgeschlossenen Dienstvereinbarungen übernommen. Es handelte sich dabei im wesentlichen um Empfehlungen zur Begrenzung der Zugriffs- und Auswertungsmöglichkeiten, die Löschung der Zeiterfassungsdaten sowie die Absicherung der eingesetzten Arbeitsplatzrechner.

Bei einer Kontrolle des Verfahrens wurde festgestellt, daß die Art des Einsatzes nicht den Angaben aus der Anmeldung zum Datenschutzregister und den datenschutzrechtlichen Vorgaben der zugrundeliegenden Dienstvereinbarung entsprach. Neben der technischen Umsetzung im betroffenen Ministerium beruhte dies vor allem auf dem Fehlen entsprechender Funktionen des eingesetzten Zeiterfassungsprogramms. Entgegen der Zusicherung des Herstellers gewährleistete dieses keine ausreichende Nachvollziehbarkeit personenbezogener Auswertungen, insbesondere in bezug auf Zeitpunkt, Umfang und Anlaß. Eine Nachbesserung war lediglich teilweise erfolgt. Darüber hinaus waren entgegen den Regelungen der Dienstvereinbarung die über den vereinbarten Umfang hinausgehenden Auswertungsmöglichkeiten nicht programmtechnisch unterbunden. Aufgrund unzureichender Löschfunktionen wurden weiterhin die Daten abgeschlossener Zeiträume nicht gelöscht.

Der LfD hat bemängelt, daß das Verfahren nicht im Einklang mit den getroffenen Vereinbarungen betrieben wird und auf die Notwendigkeit hingewiesen, das Zeiterfassungsprogramm den Vorgaben der Dienstvereinbarung anzupassen. Dabei sollte das

Programm auch dahin gehend ergänzt werden, daß die Daten abgeschlossener Abrechnungszeiträume mit geringem Aufwand gelöscht werden können. Die angesprochenen Defizite bestehen grundsätzlich bei allen obersten Landesbehörden, die das gleiche Verfahren einsetzen. Der LfD hat daher empfohlen, die erforderlichen Anpassungen in Abstimmung mit den übrigen betroffenen Ressorts vorzunehmen.

Zwischenzeitlich wurde ein Konzept vorgelegt, welches die Empfehlungen des LfD berücksichtigt. Unter anderem soll künftig eine zusätzliche Protokollierungskomponente zum Einsatz kommen und sichergestellt werden, daß die Daten abgelaufener Abrechnungszeiträume nach sechs Monaten gelöscht werden.

21.2.4 Computerunterstützte Betriebsprüfung (CuB) bei der Landesversicherungsanstalt Rheinland-Pfalz

Die Träger der Rentenversicherung prüfen nach § 28 p SGB IV die ordnungsgemäße Entrichtung der Sozialversicherungsbeiträge durch den Arbeitgeber. Die LVA Rheinland-Pfalz betreibt hierzu das Verfahren „Computerunterstützte Betriebsprüfung". Die Prüfungszuständigkeit der LVA erstreckt sich dabei insgesamt auf ca. 50 000 Arbeitgeber; pro Jahr werden etwa 16 000 Arbeitgeber geprüft.

Im Rahmen der Prüfungen greifen die Außendienstmitarbeiter der LVA von ihren Privaträumen aus per Notebookrechner und ISDN-Verbindung auf Daten der Bundesversicherungsanstalt, des Verbandes der Rentenversicherungsträger sowie der LVA zu. Die Prüfberichte werden ebenfalls in elektronischer Form zur Verfügung gestellt. Das Verfahren befindet sich noch im Aufbau, zum Prüfungszeitpunkt waren von 81 vorgesehenen Außenprüfern ca. 30 im Einsatz.

Hinsichtlich der technisch-organisatorischen Absicherung der Notebooks und des Zugriffs der Außendienstprüfer auf das System der LVA hat der LfD örtliche Feststellungen bei der Anstalt getroffen. Gründe für eine Beanstandung haben sich dabei nicht ergeben. Die entsprechend dem Verfahrenskonzept vorgesehenen Maßnahmen sind geeignet, eine ausreichende Datensicherheit zu gewährleisten.

So ist insbesondere durch die Konfiguration der Anschlüsse sichergestellt, daß nur mit dem Notebook des jeweiligen Prüfers ein Zugriff auf die Daten der LVA erfolgen kann. Die Notebooksysteme sind mit einer Sicherheitsoberfläche ausgestattet, die geeignet ist, einen Zugriff Unbefugter wirksam zu verhindern; die auf der Festplatte befindlichen Daten werden verschlüsselt. Insgesamt entsprach die Absicherung der Geräte den Empfehlungen des LfD zu Sicherheitsmaßnahmen beim Einsatz tragbarer Systeme (vgl. 14. Tb., Tz. 21.6).

Eine Leitungsverschlüsselung bei der Kommunikation zwischen Prüfer und Landesversicherungsanstalt war zum Prüfungszeitpunkt noch nicht umgesetzt, diese ist im Verfahrenskonzept für die computerunterstützte Betriebsprüfung jedoch vorgesehen.

21.2.5 Verarbeitung medizinischer Daten bei einer Beratungsstelle

Im Rahmen der Tätigkeit einer Beratungseinrichtung werden freiwillig erhobene Anamnese- und Befunddaten u. a. auf einem Arbeitsplatzrechner gespeichert. Neben üblichen Stammdaten wie Name, Anschrift usw. handelt es sich dabei um Ergebnisse aus ärztlichen und labormäßigen Untersuchungen sowie sonstige Angaben zum Gesundheitszustand und der Krankheitsgeschichte der Ratsuchenden.

Im Hinblick auf die erforderlichen Datenschutzmaßnahmen ist die Einrichtung an den LfD mit der Bitte um Beratung herangetreten. Daraufhin wurden örtliche Feststellungen getroffen und geeignete Maßnahmen empfohlen.

Der eingesetzte Arbeitsplatzrechner war nur unzureichend gegen unbefugte Zugriffe gesichert. Der Rechner war weiterhin so plaziert, daß die Daten eines aufgerufenen Falles am Bildschirm für Besucher einsehbar waren. So war im Anmeldungsbereich die Tatsache des Schwangerschaftsabbruchs einer bestimmten Ratsuchenden für die Mitarbeiter des LfD erkennbar. Durch eine geeignete Aufstellung des Bildschirms sowie der Aufteilung der Bildschirmmaske in einen standardmäßig angezeigten Stammdatenteil (Name, Adresse u. ä.) und einen gesonderten Untersuchungs- und Diagnoseteil wären derartige Probleme vermeidbar.

Die genannten Mängel wurden zwischenzeitlich abgestellt. Gleiches gilt für die Aufbewahrung von Akten und Datenträgern, für die geeignete Aufbewahrungsmöglichkeiten geschaffen wurden.

Der Datenbestand der Patientendatei umfaßte alle bisherigen Beratungsfälle (ca. 15 500) aus den vergangenen 18 Jahren. Die über verschiedene Selektionskriterien (u. a. Namen, Adresse) recherchierbaren Daten wurden überwiegend für die Klärung zurückliegender Beratungen sowie bei Nachfragen der Betroffenen genutzt. Gleiches gilt für die parallel geführten Beratungsakten. Löschungen oder Aussonderungen waren in der Vergangenheit nicht erfolgt, entsprechende Zeitpunkte waren nicht festgelegt. Die Notwendigkeit einer längerfristigen Speicherung aufgrund der möglichen Bedeutung der Untersuchungsergebnisse auch in späteren Jahren wurde begründet dargelegt. Dies rechtfertigt es aus Sicht des Datenschutzes jedoch nicht, alle

Diagnose- und Untersuchungsdaten der zurückliegenden Fälle jederzeit für eine automatisierte Abfrage vorzuhalten. Telefonische Auskünfte hierzu werden nicht erteilt und Fragen zu länger zurückliegenden Fällen grundsätzlich nur auf der Grundlage der jeweiligen Beratungsakte beantwortet. Die Zahl der Nachfragen reduziert sich zudem mit dem zeitlichen Abstand zum Beratungstermin.

Der LfD hat daher empfohlen, einen Zeitpunkt festzulegen, zu dem eine Reduzierung des Datenbestandes in der Weise erfolgt, daß für zurückliegende Fälle lediglich diejenigen Angaben automatisiert vorgehalten werden, die ein direktes Auffinden der Beratungsakte sicherstellen (z. B. Name, Aktenzeichen, Datum der Beratung). Im übrigen sollten die Anamnese- und Befunddaten gelöscht werden. Ein Zeitraum von fünf Jahren erscheint insoweit angemessen. Dies entspricht der bisherigen Praxis, die Angaben überwiegend zur Klärung der Frage nach zurückliegenden Beratungen heranzuziehen und nicht als Befunddatenbank zu nutzen.

Die entsprechende Anpassung des eingesetzten Programms ist zwischenzeitlich erfolgt; die automatisiert gespeicherten, sensiblen Daten der Ratsuchenden werden künftig nach fünf Jahren gelöscht.

Die Fragebögen der Beratungsstelle enthielten bislang keine Hinweise auf die Freiwilligkeit der Datenerhebung, die automatisierte Verarbeitung und die Dauer der Speicherung. Künftig ist eine separate Erklärung nach § 5 LDSG vorgesehen, in der die Betroffenen auf die Art der Verarbeitung, die Speicherungsdauer sowie die bestehende Widerrufsmöglichkeit hingewiesen werden sollen.

21.2.6 Zugriffskontrolle bei der Verarbeitung von Krankenversicherungsdaten

Vor dem Hintergrund der Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum eingeschränkten Zugriff auf Versichertendaten bei landesweiten oder überregionalen gesetzlichen Krankenkassen (vgl. Tb. 15, Anlage 17) wurden vom LfD im Bereich der allgemeinen Ortskrankenkassen, der Innungskrankenkassen sowie der Betriebskrankenkassen örtliche Feststellungen getroffen. Schwerpunkte waren dabei insbesondere die Ausgestaltung der Speicher- und Zugriffskontrolle nach § 78 a SGB X.

Dabei hat sich ergeben, daß überwiegend eine an Funktionsbereichen orientierte Steuerung der Zugriffe erfolgt. Diese zielt vorrangig auf die Unterscheidung schreibender bzw. ändernder Zugriffe. Programmfunktionen, die lesend auf die Versichertendaten zugreifen, werden weitgehend einheitlich allen Benutzern zur Verfügung gestellt. Angesichts des in der Vergangenheit erfolgten Zusammenschlusses ehemals selbständiger Kassen zu landesweiten Organisationen und der damit einhergehenden Zusammenführung der einzelnen Datenbestände, kann damit im Ergebnis häufig eine Vielzahl der Bediensteten einer Krankenversicherung auf die Angaben der Versicherten, darunter Diagnose- und Leistungsdaten, zugreifen. Angesichts der regional beschränkten Zuständigkeit von Geschäftsstellen wird der bestehende Umfang des Datenzugriffs vom LfD als problematisch angesehen.

Erforderlich ist aus seiner Sicht eine Zugriffssteuerung, die es im Grundsatz erlaubt, entsprechend der regionalen Zuständigkeit einer Geschäftsstelle die jeweiligen Zugriffsrechte zu differenzieren. Die hierzu notwendige Anpassung der eingesetzten EDV-Verfahren liegt in der Regel im Verantwortlichkeitsbereich der jeweiligen Landes- bzw. Bundesverbände. Die betroffenen Kassen wurden daher gebeten, nachdrücklich dafür einzutreten, daß die erforderlichen Funktionen baldmöglichst zur Verfügung gestellt werden. In einzelnen Kassenbereichen sind hier bereits entsprechende Programmergänzungen absehbar. Der LfD wird die weitere Entwicklung in diesem Bereich mit der gebotenen Aufmerksamkeit verfolgen.

21.2.7 Bibliothekssystem einer Universität

21.2.7.1 Erfolgreicher „Hack" bei den Benutzerdaten

Von einem Studierenden wurde der LfD darauf hingewiesen, daß es im Bibliothekssystem einer Universität des Landes möglich sei, unbefugt auf die Daten der Bibliotheksbenutzer zuzugreifen. Gegenüber der regionalen Presse sowie der Universitätszeitung wurde der Vorfall ebenfalls dargestellt.

Nach den Feststellungen des LfD führte eine Schwachstelle beim Zugang zu den Servern der Universitätsbibliothek dazu, daß auf die Daten des Bibliothekssystems zugegriffen werden konnte: auf einem Server der Universität wurden allgemein zugängliche Anwendungen, darunter auch die Möglichkeit der Recherche im Bibliothekskatalog, zur Verfügung gestellt. Beim Aufruf der Katalogrecherche wurde automatisch zum Bibliotheksserver verzweigt. Die für den automatisierten Zugang erforderlichen Angaben (Verbindungskommando, Benutzerkennung und Paßwort) waren im Klartext in allgemein zugänglichen Dateien auf dem Gästeserver hinterlegt und konnten ausgelesen werden. Dies wurde genutzt, um mit den genannten Angaben die Anmeldung am Bibliotheksrechner manuell vorzunehmen und damit die für den automatisierten Zugang vorgesehene Zugriffssteuerung zu umgehen. Aufgrund der vorhandenen IT-Struktur und der Konfiguration der eingesetzten Rechner war dies grund-

sätzlich von allen ca. 1 200 Arbeitsstationen des Campus-Netzes aus möglich. Neben Grundkenntnissen der eingesetzten Programme erforderte der erfolgreiche Versuch lediglich eine gewisse Neugier und Findigkeit. Angeregt wurde er offenbar durch eine nicht unterdrückte Bildschirmmeldung bei der automatischen Anmeldung auf dem Bibliotheksserver.

An personenbezogenen Daten waren vor allem Angaben über Name, Anschrift, Immatrikulationsnummer, Säumnisgebühren, Paßworte und entliehene, vorgemerkte oder bestellte Bücher der ca. 16 000 eingetragenen Bibliotheksnutzer (Studenten, Lehrpersonal, Beschäftigte, sonstige Nutzer) betroffen. Nach den Erkenntnissen des LfD wurden offenbar auch Benutzerdaten auf Datenträger kopiert. Besonders ins Gewicht fällt der Zugriff auf die auch hier im Klartext gespeicherten Paßworte der Benutzer für die Anmeldung am Bibliothekssystem. Mit deren Kenntnis ist es, solange diese nicht geändert werden, möglich, sich gezielt unter einem bestimmten Benutzernamen anzumelden und in die genannten Daten Einblick zu nehmen oder diese zu verändern. Die Bibliotheksnutzer wurden daher auf die Notwendigkeit hingewiesen, ihre Paßworte zu ändern.

Innerhalb des Bibliothekssystems wurde der unbefugte Zugriff durch die bestehenden, weitgehenden Zugriffsrechte erleichtert. Diese sind zum Teil durch die Programmstruktur des Bibliothekssystems BABSY bedingt. Aufgrund der sich daraus ergebenden Risiken empfiehlt der Hersteller, das Programm in einer geschlossenen Umgebung, d.h. nicht innerhalb eines allgemein zugänglichen Netzes, einzusetzen.

Eine campusweite Bereitstellung des Programms, wie sie an der betroffenen Universität erfolgt ist, erfordert – den erhöhten Risiken im Netzwerkbetrieb entsprechende – Sicherungsmaßnahmen. Dies wurde bei der Einrichtung des Verfahrens nicht ausreichend berücksichtigt. Zur Verfügung stehende Möglichkeiten wurden nicht genutzt. Wie von der Universitätsbibliothek dargelegt, wurden aus Zeitgründen und wegen der begrenzten Betreuungskapazität die Einstellungen des Herstellers bei der Installation übernommen. Bei der Einrichtung des netzwerkweiten Zugriffs ist eine Überprüfung dieser Einstellungen unter Sicherheitsgesichtspunkten nicht erfolgt.

Die vorhandene Schwachstelle beim Zugang zum Bibliotheksserver wurde zwischenzeitlich beseitigt. Defizite bestehen jedoch weiterhin u. a. bei der Nachvollziehbarkeit der Systemnutzung. So ist es mangels einer entsprechenden Protokollierung nicht möglich nachzvollziehen, ob, wann und wie viele unbefugte Zugriffe stattgefunden haben, auf welche Dateien konkret zugegriffen wurde und ob unbefugte Veränderungen der gespeicherten Daten oder Manipulationen am System („Hintertüren") vorgenommen wurden.

Die Ausgestaltung des Bibliothekssystems entsprach aus Sicht des LfD nicht den Anforderungen des § 9 LDSG an die datenschutzgerechte Verarbeitung personenbezogener Daten. Dies wurde als Verstoß gegen datenschutzrechtliche Bestimmungen gemäß § 25 Abs. 1 LDSG beanstandet. Zur Beseitigung der festgestellten Mängel hält der LfD insbesondere folgende Maßnahmen für geeignet:

- Es darf keine Speicherung der für den Zugang zu den Bibliotheksservern erforderlichen Paßworte im Klartext erfolgen. Die relevanten Angaben sollten in chiffrierter Form gespeichert und erst beim Aufruf des Verbindungsbefehls programmgesteuert entschlüsselt werden. Um der Aufdeckung bei einer denkbaren Analyse des Programmcodes mit gängigen Hilfsprogrammen entgegenzuwirken, sollten diesbezügliche Programmkonstanten ebenfalls nicht im Klartext erscheinen.

- Die Zugriffsrechte auf den Bibliotheksservern sind zu überprüfen und einzuschränken. Dabei sollte geprüft werden, inwieweit die Möglichkeit besteht, kritische Funktionen wie den Zugang zum Ausleihserver und allgemein verfügbaren BABSY-Funktionen (z. B. Katalogrecherche) auf verschiedene Benutzerkennungen mit unterschiedlichen Zugriffsrechten aufzuteilen.

Die Feststellungen haben ergeben, daß auf dem Ausleihserver Benutzerkennungen eingerichtet waren, die nicht oder nur vorübergehend benötigt wurden (NOBODY, LESESAAL). Zugangsberechtigungen sollten nur im erforderlichen Umfang bestehen und im übrigen gelöscht oder gesperrt werden.

- Die Zugriffsrechte innerhalb der Bibliotheksanwendung BABSY bedürfen einer Überprüfung und erforderlichenfalls der Einschränkung. Die angetroffene Konfiguration sah keine Differenzierung der Rechte der unterschiedlichen Benutzerkreise vor.

- Um die Kenntnisnahme personenbezogener Daten beim unbefugten Zugriff auf den Ausleihserver zu verhindern, sollten diese in verschlüsselter Form gespeichert werden. Entsprechende kryptografische Lösungen stehen gerade im Hochschulbereich zur Verfügung. Darüber hinaus kommt die Nachrüstung des Ausleihservers mit am Markt verfügbaren Sicherheitslösungen in Betracht.

- Ungewöhnliche Benutzeraktivitäten sind zu protokollieren und regelmäßig zu überprüfen. Der automatisierte Zugang zum Bibliothekssystem aus dem Campus-Netz heraus erfolgt regelmäßig über festgelegte Kommandofolgen, abweichende Formen des Zugangs stellen Ausnahmen dar. Diese sollten daher mit den systemseitig bereits vorhandenen Protokollfunktionen aufgezeichnet und ausgewertet werden.

Gleiches gilt für Anmeldungen außerhalb der Arbeitszeiten der Bibliothek, wiederholt erfolglose Anmeldeversuche, Verstöße gegen Zugriffsbeschränkungen und unübliche „Attach-" und „Login"-Vorgänge. Über die geschilderte Protokollierung läßt sich eine Verbesserung der derzeitigen Situation erreichen, in der ungewöhnliche Benutzeraktivitäten weitgehend unerkannt bleiben.

Die Empfehlungen des LfD wurden zum Teil bereits aufgegriffen, eine endgültige Stellungnahme über die künftige Gestaltung des Verfahrens steht noch aus.

21.2.7.2 Was Paßwörter über ihre Benutzer erzählen

Im Zusammenhang mit dem Eindringen in das Bibliothekssystem wurden vom Bibliotheksserver personenbezogene Daten, darunter die Zugangspaßworte der Benutzer, auf eine Diskette kopiert.

In der Campus-Zeitung der Universität wurde kurz darauf eine Darstellung der am häufigsten verwendeten Paßwörter veröffentlicht. Daraus ist erkennbar, daß trotz zunehmender Diskussion von Sicherheitsfragen beim Einsatz der Informationstechnik unbefugte Zugriffe nach wie vor vor allem durch die Sorglosigkeit der Anwender bei der Gestaltung und Verwendung ihrer Paßwörter begünstigt werden.

So benutzte nach der Darstellung der Universitätszeitung die überwiegende Zahl der Benutzer ihr Geburtsdatum, den eigenen Vornamen oder solche aus dem Bekanntenkreis als Paßwort. Zu beliebten Paßwörten bei den Studierenden zählten auch Begriffe wie „SONNE" oder „HALLO". Hinsichtlich ihrer Tauglichkeit als effektive Schutzmaßnahme sind diese ähnlich zu beurteilen wie die ebenfalls verwendeten Angaben „ICHBINS" oder „ICHBINDA".

Begriffe wie „MAGISTERARBEIT", „RELIGIONSBUCH", „BEVÖLKERUNGSDRUCK" oder „SOZIALVERSICHERUNG" sind zwar weniger offenkundig, entsprechen aber, nicht den Empfehlungen an die Gestaltung und Verwendung von Paßwörtern, wie sie der LfD in Anlage 11 zu seinem 14. Tb. veröffentlicht hat.

Der Einsatz von Paßwörtern ist nach wie vor die häufigste Form der Absicherung des Rechnerzugangs und gleichzeitig diejenige, auf die der Benutzer den größten Einfluß hat. Auch wenn sich zusätzliche Gefährdungen für die Datensicherheit aus technischen Entwicklungen und der Komplexität von IT-Lösungen ergeben, sollte die Bedeutung eines sorgfältigen Umgangs mit Paßwörtern nicht aus dem Blickfeld geraten.

21.2.8 ISDN-Telekommunikationsanlage der Landesregierung

Im Hinblick auf die datenschutzrechtlichen Aspekte beim Betrieb von Nebenstellenanlagen wurde der LfD im Vorfeld der Einführung der ISDN-Telekommunikationsanlage der Landesregierung beteiligt. Die Empfehlungen zum datenschutzgerechten Betrieb des Verfahrens sind in die Dienstvereinbarungen über den Betrieb und die Nutzung der ISDN-Telekommunikationsanlage eingeflossen.

Von Bedeutung waren dabei insbesondere die Konfiguration und Dokumentation der aus Sicht des Datenschutzes sensiblen Leistungsmerkmale, der Umfang und die Speicherungsdauer der für die Abrechnung von Telefonaten erforderlichen Daten, die Modalitäten der Auswertung von Gesprächs- und Protokolldaten sowie die Maßnahmen der Zugangs- und Zugriffskontrolle beim Betrieb und der Betreuung des Systems.

Angesichts der vorgesehenen Nutzung der ISDN-Infrastruktur außer für die Telefonie auch für die Datenkommunikation innerhalb der Landesregierung sind ausreichende Sicherheitsmaßnahmen von grundsätzlicher Bedeutung. Der LfD wird daher die Umsetzung seiner Empfehlungen sowie die getroffenen Sicherheitsmaßnahmen im Rahmen örtlicher Feststellungen überprüfen.

21.2.9 Verarbeitung von Krankenversicherungsdaten bei der Arbeitsgemeinschaft AOK Rechenzentrum Mitte

Für den gemeinsamen Betrieb eines Rechenzentrums wurde von den Allgemeinen Ortskrankenkassen in Hessen, Rheinland-Pfalz und im Saarland eine Arbeitsgemeinschaft nach § 219 SGB V in der Form einer Gesellschaft bürgerlichen Rechts gegründet. Rechenzentrum der Arbeitsgemeinschaft ist das bisherige Rechenzentrum der AOK Hessen. Trotz der vorgenommenen Konzentration der DV-Dienstleistungen werden die Datenbestände der jeweiligen Landes-AOK weiterhin separat, d. h. getrennt voneinander, verarbeitet. Eine bestandsübergreifende Datenverarbeitung erfolgt nicht, die bisherigen Datenbestände werden in ihrer ursprünglichen Form weitergeführt und bleiben physisch und logisch getrennt. Für jede Landes-AOK wird zu diesem Zweck eine eigene Betriebssystemumgebung eingerichtet. Die gegenseitige Absicherung erfolgt über die Vereinbarung entsprechender Namenskonventionen und den Einsatz eines geeigneten Sicherungssystems.

Angesichts des besonderen Charakters der Arbeitsgemeinschaft wurden in Abstimmung mit den Datenschutzbeauftragten der betroffenen Länder gemeinsame örtliche Feststellungen getroffen und Empfehlungen im Hinblick auf eine datenschutzgerechte Ausgestaltung des Verfahrens ausgesprochen. Diese betrafen im wesentlichen

- die Gestaltung des Vertrags über die Datenverarbeitung im Auftrag i. S. v. § 80 SGB X,
- die Bestellung eines Datenschutzbeauftragten,
- das Verfahren und die Zuständigkeiten bei der Datenverarbeitung durch die Arbeitsgemeinschaft,
- den Abschluß einer Datenschutzvereinbarung,
- die Festlegung von Grundsätzen für das Test- und Freigabeverfahren,
- die Tätigkeit der Arbeitsgemeinschaft als Datenannahmestelle sowie die Zugriffskontrolle im Bereich des Rechenzentrums der Arbeitsgemeinschaft.

Aus der Sicht des Datenschutzes ist die gegenwärtige Organisation der Datenverarbeitung an die erweiterte Aufgabenstellung des Rechenzentrums anzupassen; insbesondere sollte, gestützt auf eine Risikoanalyse, ein Sicherheitskonzept erarbeitet werden.

Die Arbeitsgemeinschaft sowie die AOK Rheinland-Pfalz haben diese Empfehlungen aufgegriffen und in Teilen bereits umgesetzt. Der LfD wird die weitere Umsetzung, insbesondere auch des Archivierungs- und Löschkonzepts, weiter verfolgen.

21.2.10 Einsatz von Chipkarten im Sozialamt einer Stadtverwaltung

Aufgrund von Presse- und Rundfunkberichten war dem LfD der Einsatz von Chipkarten für die Barauszahlung von Sozialhilfeleistungen zur Kenntnis gelangt. Zur Klärung der Ausgestaltung des Verfahrens wurden beim Sozialamt der betroffenen Stadtverwaltung örtliche Feststellungen getroffen. Danach erhalten die Empfänger von Barleistungen statt des bisherigen „gelben Verwaltungsschecks" eine entsprechend codierte Chipkarte, mit der an geeigneten Auszahlungsautomaten im Publikumsbereich des Sozialamtes der jeweilige Geldbetrag ausgezahlt wird. Die Kartendaten werden für Abrechnungszwecke (Tagesabschluß, Monatsabschluß) elektronisch gespeichert, in das Haushaltskassen- und Rechnungswesen der Stadtverwaltung übernommen und die Chipkarte danach automatisch einbehalten und gelöscht. Das Verfahren wird in Zusammenarbeit mit der Stadtsparkasse betrieben, die auch die Auszahlungsautomaten mit den erforderlichen Barmitteln bestückt. Die Abrechnung der Stadtverwaltung mit der Sparkasse erfolgt anhand von Tagesabschlüssen in Listenform und dem Aktenzeichen als Zuordnungsmerkmal. Name und Anschrift des Sozialhilfeempfängers werden nicht auf der Karte gespeichert.

Das Verfahren ist aus datenschutzrechtlicher Sicht nicht zu beanstanden. Im Vergleich zum bisherigen Verfahren mit der Einlösung von Verwaltungsschecks sind in dieser Hinsicht sogar gewisse Vorteile erkennbar.

Nach den Erkenntnissen des LfD ist der Einsatz entsprechender Lösungen auch von anderen Kommunen in Rheinland-Pfalz vorgesehen.

21.3 Behinderung der Kontrolltätigkeit des LfD

Bei der Kontrolle einer Betriebskrankenkasse wurde dem LfD die nach § 28 Abs. 1 LDSG zu gewährende Unterstützung – konkret die Einsichtnahme in gespeicherte Daten – durch den Vorstand der Betriebskrankenkasse ausdrücklich verweigert. Bereits im Vorfeld der Kontrolle wurden erbetene Unterlagen ohne Rückäußerung nicht zur Verfügung gestellt.

Wiederholte Hinweise der Mitarbeiter des LfD auf die bestehende Unterstützungspflicht wurden ignoriert. Form und Ton der Äußerungen entsprachen dabei weitgehend nicht dem Gebot der Sachlichkeit im Umgang mit Behördenvertretern. Die Einlassungen offenbarten im übrigen einen Mangel der Kenntnis elementarer Grundlagen des Sozialdatenschutzes. Die Kontrolle wurde daraufhin abgebrochen.

Die entgegen den gesetzlichen Bestimmungen verweigerte Unterstützung hat der LfD als Verstoß gegen datenschutzrechtliche Vorschriften nach § 25 Abs. 1 Nr. 4 LDSG beanstandet und die Aufsichtsbehörden gebeten sicherzustellen, daß er die ihm gesetzlich zugewiesenen Aufgaben wahrnehmen kann. Erst nach wiederholten Interventionen der Aufsichtsbehörden konnte die Kontrolle fortgesetzt werden.

In einem weiteren Fall forderte der LfD anläßlich der Bearbeitung einer Eingabe ein Gesundheitsamt auf, zum Sachverhaltsvortrag des Petenten Stellung zu nehmen. Das Gesundheitsamt bestritt die Kontrollkompetenz des LfD und vertrat die Auffassung, daß es zur Auskunftserteilung über medizinische Sachverhalte nur aufgrund einer schriftlichen Schweigepflichtentbindungserklärung des Petenten befugt sei.

Wegen der Bedeutung des Vorgangs unterrichtete der LfD das Ministerium des Innern und für Sport und bat, aufsichtlich tätig zu werden. Das Ministerium bestätigte, daß dem LfD nach § 28 LDSG eine umfassende Kontrollbefugnis zusteht, die allenfalls

dann eingeschränkt wäre, wenn der Betroffene nach § 24 Abs. 2 Nr. 2 b i. V. m. Abs. 6 BDSG einer Kontrolle im Einzelfall widersprochen hätte. Dies war aber nicht der Fall. Der Betroffene hatte – im Gegenteil – eine Kontrolle durch den LfD ausdrücklich gewünscht.

Das Gesundheitsamt folgte schließlich dieser Rechtsauffassung. Unerfreulich war nicht nur die Hartnäckigkeit, mit der es die im Gesetz klar und deutlich geregelte Prüfungskompetenz des LfD bestritt, sondern auch, daß die Eingabe erst nach mehr als fünf Monaten abschießend bearbeitet werden konnte.

21.4 Landesdaten- und Kommunikationsnetz Rheinland-Pfalz

21.4.1 Abkehr vom reinen Verwaltungsnetz

Das Landesdaten- und Kommunikationsnetz Rheinland-Pfalz ist gegenwärtig einem Wandel unterworfen, der für die Sicherheit und den Datenschutz im Netz von zentraler Bedeutung ist. Mit dem Anschluß von Teilbereichen des LDKN an öffentliche Kommunikationsnetze wie das Internet und der vorgesehenen Öffnung für Hochschulen, Wirtschaft und private Stellen ändert sich der bisherige Charakter des LDKN als ein lediglich verwaltungsintern genutztes Netz. Nutzungsmöglichkeiten von Stellen außerhalb der Verwaltung und Übergänge zu öffentlichen Kommunikationsnetzen dürfen aus Sicht des LfD nur eröffnet werden, wenn eine wirksame Abschottung der verschiedenen Bereiche sichergestellt ist und Vorkehrungen gegen unbefugte Datenzugriffe getroffen sind.

Die Bildung virtueller Netzwerke ist dazu grundsätzlich geeignet, bedarf jedoch der Ergänzung durch weitere technische Maßnahmen. Die Verschlüsselung auf dem Übertragungsweg oder Authentisierungsverfahren für die beteiligten Netzkomponenten sind Punkte, die dabei einer näheren Prüfung unterzogen werden sollten. Bei der beabsichtigten Einrichtung virtueller privater Netze (VPN) muß aus Sicht des LfD gewährleistet sein, daß insbesondere Übergriffe in das Netz der Polizei und das allgemeine Verwaltungsnetz verhindert bzw. entsprechende Versuche erkannt werden.

Im Zusammenhang mit der Einbindung der Hochschulen ist die Einführung zusätzlicher Übertragungsprotokolle vorgesehen. Nach Auskunft des DIZ wird dabei der Datenverkehr zwischen den Backbone-Knoten des LDKN künftig über entsprechende ATM-Vermittlungsrechner der Telekom geführt. Dies stellt eine Änderung der bisherigen Situation dar, bei der die Knotenrechner des LDKN ausschließlich bei Stellen der Landesverwaltung untergebracht waren, und damit der Zugang zu den Vermittlungsrechnern kontrolliert werden konnte. Mit der Verlagerung des Datenverkehrs zwischen den zentralen Knoten des Netzes auf Rechner im Bereich eines privaten Dienstleisters stehen die Übertragungswege nur noch eingeschränkt unter der Kontrolle der LDKN-Verwaltung.

Aus der Sicht des Datenschutzes sind daher Maßnahmen erforderlich, die der geänderten Situation Rechnung tragen. So könnte beispielsweise eine Leitungsverschlüsselung zwischen den Backbone-Knoten des LDKN vorgenommen werden, mit der die Vertraulichkeit der Kommunikation unabhängig vom gewählten Übertragungsweg sichergestellt werden kann. Erweiterungen des Nutzungsspektrums des LDKN sollten aus datenschutzrechtlicher Sicht nur erfolgen, wenn gleichzeitig die vorhandenen Sicherungsmaßnahmen gestiegenen Risiken angepaßt werden. Datenschutz- und Sicherheitsaspekte müssen, gerade bei den Bemühungen um die Bereitstellung einer leistungsfähigen Kommunikationsinfrastruktur, angemessen Berücksichtigung finden. In diesem Zusammenhang hat der LfD wiederholt auf die Notwendigkeit eines auf einer Risikoanalyse aufbauenden, in sich geschlossenen Sicherheitskonzepts für das LDKN hingewiesen (vgl. u. a. 15. Tb., Tz. 21.3). Dieses steht weiterhin aus, die vorhandenen Ansätze beschränken sich auf Teilbereiche. Angesichts der Veränderungen, denen das LDKN unterworfen ist, hält der LfD ein derartiges Sicherheitskonzept für dringend erforderlich. In diesem Zusammenhang bedürfen auch die auf das ehemalige Landesdatennetz ausgerichteten Benutzungsbedingungen (MinBl. 1994, 131) einer Überarbeitung.

Die Organisation, Infrastruktur und Administration des LDKN, die Sicherung der Übertragungswege, die Abschottung von Teilnetzen, die Übergänge in andere Kommunikationsnetze, Anschlußvoraussetzungen, Zugangskontrolle sowie Art und Umfang nutzbarer Netzdienste sind Punkte, die einer einheitlichen Sicherheitsbetrachtung bedürfen. Ohne dokumentierte und für die Nutzer verbindliche Sicherheitsrichtlinien besteht die Gefahr, daß aus der zunehmenden Komplexität des LDKN Nachteile für den Datenschutz erwachsen.

21.4.2 Die „Brandmauer" – das Firewall-Konzept des LDKN

Für die Anbindung des LDKN an öffentliche Kommunikationsnetze, hier vor allem der zentrale Übergang zum Internet, ist die Einrichtung einer Firewall vorgesehen. Das DIZ folgt damit den Empfehlungen der Orientierungshilfe der Datenschutzbeauftragten zum Anschluß von Netzen der öffentlichen Verwaltung an das Internet.

Kern des Firewall-Konzepts für das LDKN ist die Gliederung in abgeschottete Bereiche mit unterschiedlichen Sicherheitsanforderungen. So werden die für die Bereitstellung im Internet vorgesehenen Informationen auf entsprechenden Servern

außerhalb des durch eine Firewall geschützten Bereichs in der sog. „red zone" bereitgestellt. Die für eine begrenzte Öffentlichkeit im Intranet des Landes verfügbaren Daten befinden sich hinter der Firewall („yellow zone"), die Bereiche der einzelnen virtuellen privaten Netze des LDKN sind durch eine weitere Firewall hiervon getrennt („green zone") . An den Übergängen erfolgt über definierte Regeln eine Prüfung und Filterung anhand von IP-Adressen, Internetdiensten und ggf. weiteren Kriterien.

Gegen das vorgestellte Konzept bestehen, insbesondere weil der zentrale Großrechner weiterhin über das Internet-Protokoll nicht direkt erreichbar sein wird, keine grundsätzlichen Bedenken. Eine endgültige Bewertung kann jedoch erst im Zusammenhang mit der praktischen Umsetzung erfolgen. Hier sind aus Sicht des LfD insbesondere folgende Punkte zu berücksichtigen:

- Filterregeln sind so zu formulieren, daß alle Verbindungen, die nicht ausdrücklich zugelassen sind, unterbunden werden. Eine umgekehrte Vorgehensweise, nur gezielt bestimmte Verbindungen zu untersagen, trägt den im Internet bestehenden Risiken nur unzureichend Rechnung.

- Aufbau und Struktur des internen Netzes dürfen für externe Teilnehmer nicht erkennbar sein. Dies gilt auch, soweit – was dem Grunde nach nicht ausgeschlossen werden kann – aus dem im Konzept als „yellow zone" bezeichneten Netz ungesicherte Übergänge zu weiteren Netzen bestehen.

- Die Nutzung zugelassener Dienste sowie sicherheitsrelevante Ereignisse sind angemessen zu protokollieren. Dabei müssen insbesondere zurückgewiesene Datenpakete, erfolglose Verbindungswünsche und Verstöße gegen die Sicherheitsfestlegungen erkannt werden können.

- Für die Firewall-Rechner muß eine anderweitige Nutzung ausgeschlossen werden; insbesondere dürfen sie nicht als Web-, Mail-, FTP- oder Datenbankserver betrieben werden. Telnet-Verbindungen sind auf das unverzichtbare Maß zu beschränken. Benutzeranmeldungen dürfen nur nach erfolgreicher Identifizierung und Authentifizierung möglich sein.

- Von Fernzugriffen auf die Firewall-Rechner ist grundsätzlich abzusehen. Wo dies in Einzelfällen unverzichtbar ist, dürfen derartige Zugriffe nur unter eng begrenzten Voraussetzungen möglich sein (vgl. 15. Tb., Tz. 21.6).

21.5 Fernwartung

Im Hinblick auf die datenschutzgerechte Durchführung von Fernwartungs- und Fernbetreuungsverfahren hatte der LfD im 15. Tb., Tz. 21.6.2 entsprechende Empfehlungen ausgesprochen. Im Zusammenhang mit den Änderungen im Bereich der Kommunikationstechnik ist feststellbar, daß Fernwartungs- und Fernbetreuungslösungen an Bedeutung gewonnen haben.

Zur Klärung der Frage, inwieweit die Empfehlungen des LfD in der Praxis Berücksichtigung gefunden haben, wurde mit einer entsprechenden Querschnittsprüfung begonnen. Die bislang vorliegenden Erkenntnisse sind im wesentlichen zufriedenstellend. Bei allen kontrollierten Verfahren war der Zugriff der fernwartenden Stelle auf das jeweilige IT-System an eine entsprechende Identifikationsprüfung gebunden. Von Ausnahmen abgesehen, konnten Fernwartungszugriffe nur unter Mitwirkung der jeweils betroffenen öffentlichen Stelle erfolgen. Angesichts der Bedeutung von Fernzugriffen auf Behördenrechner sind jedoch zum Teil Verbesserungen bei der Steuerung und insbesondere der Nachvollziehbarkeit von Fernwartungszugriffen zu empfehlen.

Der LfD wird die Querschnittsprüfung im folgenden Berichtszeitraum fortführen.

21.6 Anbindung öffentlicher Stellen an das Internet

Im Zusammenhang mit dem vollzogenen Wandel des Internet vom ehemaligen Hochschul- und Forschungsnetz zu einem zentralen Informations- und Kommunikationsmedium ist auch in Rheinland-Pfalz die vermehrte Anbindung öffentlicher Stellen an das Internet zu verzeichnen.

Die Struktur des Internet, die Art der eingesetzten Kommunikationsprotokolle, die Sicherheitslücken vieler Programme sowie die offene Zahl und Art der Teilnehmer bergen Sicherheitsrisiken, denen durch geeignete Maßnahmen begegnet werden muß. Der Arbeitskreis „Technik" der Datenschutzbeauftragten hat daher eine Orientierungshilfe für den Anschluß öffentlicher Stellen an das Internet erstellt, in der die wesentlichen für eine sichere Anbindung erforderlichen Maßnahmen dargestellt werden.

Danach empfiehlt es sich, einen Anschluß an das Internet über einen zentralen, kontrollierten und abgesicherten Zugang zu realisieren (Firewall). Dieser sollte es ermöglichen, ein- und ausgehende Verbindungen anhand von Internetadressen, Internetdiensten (WWW/http, E-Mail/smtp, Filetransfer/ftp, Telnet, Usenet/nntp, Domain Name Service/DNS usw.) sowie von Quell-und Zielports zu filtern. Entsprechende Funktionen werden über spezifische Hard- oder Softwarelösungen angeboten. Zugänge, die nicht über den Firewall-Rechner erfolgen, sind zu untersagen und, soweit möglich, technisch zu unterbinden.

Grundsätzlich ist darauf zu achten, daß lediglich diejenigen Dienste bereitgestellt werden, die für die Aufgabenerledigung erforderlich sind. Dadurch läßt sich das Risiko, daß Schwachstellen in vorhandenen Programmen ausgenutzt werden, begrenzen.

Bestimmte Internet-Dienste (z. B. ftp, smtp) bergen das Risiko, daß die aus dem Internet übernommenen Dateien Computer- oder Makroviren enthalten. Den hiervon ausgehenden Gefährdungen kann durch eine Virenprüfung begegnet werden, wie sie auch für die Behandlung eingehender Datenträger empfohlen wird. Ähnliches gilt für die Ausführung von ActiveX oder Java-Applikationen, über welche auf dem Client-Rechner Anwendungen ausgeführt werden können. Aufgrund der in diesem Zusammenhang bekanntgewordenen Sicherheitsprobleme sollte diese Möglichkeit in den eingesetzten Internet-Browsern deaktiviert werden.

Weiterhin sollten anhand einer aussagefähigen Protokollierung Zugriffe in und aus dem Internet nachvollzogen werden können und in als sicherheitsrelevant erachteten Fällen eine Alarmierung der Systembetreuung über Bildschirmmeldungen oder den Versand elektronischer Nachrichten erfolgen.

Solange ein abgesicherter Zugang zum Internet nicht zur Verfügung steht, lassen sich die Risiken dadurch begrenzen, daß davon abgesehen wird, eine Internet-Anbindung auf Arbeitsplatzrechnern bereitzustellen, die an das lokale IT-System der öffentlichen Stellen angeschlossen sind. Entsprechende Zugangsmöglichkeiten sind lediglich auf solchen Rechnern vorzusehen, die vom lokalen Netzwerk physikalisch getrennt sind und auf denen keine datenschutzrelevanten Daten verarbeitet werden.

Angesichts der für die wirksame Absicherung erforderlichen Kombination technischer und organisatorischer Maßnahmen sind die Regelungen für die Einrichtung und Nutzung einer Internet-Anbindung in einer Dienstanweisung nach § 9 Abs. 2 LDSG darzustellen.

Die Risiken der einzelnen Internet-Dienste sowie Empfehlungen zur Anordnung und Gestaltung von Firewall-Lösungen sind in der o. g. Orientierungshilfe dargestellt. Diese kann über den LfD bezogen werden. Zur Frage, ob und in welchem Umfang Personaldaten im Internet bereitgestellt werden dürfen, s. o. Tz. 17.3.

21.7 Telearbeit und Datenschutz

Gesichtspunkte des technisch-organisatorischen Datenschutzes bei der Telearbeit im Verwaltungsbereich
(veröffentlicht in DuD, Nr. 11/97)

Telearbeit wird zunehmend als eine Arbeitsform angesehen, die geeignet ist, den veränderten Lebens- und Arbeitsbedingungen in besonderer Weise Rechnung zu tragen. Dabei spielen sowohl individuelle Gesichtspunkte wie der Wunsch nach einem wohnortnahen Arbeitsplatz, einer flexiblen Arbeitszeitgestaltung oder der besseren Vereinbarkeit von Familie und Beruf als auch allgemeine Überlegungen wie Kostenreduzierungen, geringere Verkehrs- und Umweltbelastungen und Ziele der regionalen Arbeitsmarktförderung eine Rolle. Insgesamt hat dies zu einer deutlichen Belebung der Diskussion um die Möglichkeiten der Telearbeit geführt.

Durch die Entwicklung der Informations- und Kommunikationstechnik und den Ausbau der Kommunikationsinfrastruktur stehen auch die technischen Lösungen zur Verfügung, die mit überschaubarem Aufwand die Einrichtung von Telearbeitsplätzen, gerade auch in einem Flächenland wie Rheinland-Pfalz, erlauben.

Üblicherweise werden folgende Telearbeitsformen unterschieden (vgl. Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie: Leitfaden zur Telearbeit):

- Teleheimarbeit, bei der die Beschäftigten ausschließlich zu Hause arbeiten.
- Alternierende Telearbeit, bei welcher neben dem Heimarbeitsplatz weiterhin der betriebliche Arbeitsplatz besteht. Die jeweiligen Arbeitsinhalte bestimmen, wo wann gearbeitet wird.
- Telearbeitszentren, in denen mehrere Telearbeitsplätze in lokalen Büros zusammengefaßt werden. Träger der Telearbeitszentren können dabei auch mehrere Unternehmen oder Verwaltungen sein.
- Mobile Telearbeit für Außendienstmitarbeiter, Berater und sonstige Personen, die über eine entsprechende Telekommunikationsausrüstung verfügen, ohne an eine bestimmte Büroumgebung gebunden zu sein.
- Virtuelle Unternehmen als Zusammenschluß von rechtlich unabhängigen und räumlich getrennten Selbständigen, die auf Dauer oder bei der Abwicklung eines Projektes zusammenarbeiten.

Eine Bestandsaufnahme in Rheinland-Pfalz zeigt, daß gegenwärtig im Rahmen verschiedener Projekte die Möglichkeiten der Telearbeit im Verwaltungsbereich untersucht werden. Das Einsatzspektrum umfaßt dabei u. a. Weiterbildungsmaßnahmen, die

Überwachung und Steuerung von Datenverarbeitungsanlagen, extern ausgeübte Prüftätigkeiten sowie Tätigkeiten im Rahmen von Planfeststellungsverfahren und bei der Wirtschaftsförderung. Teleheimarbeit und alternierende Telearbeit stehen dabei eindeutig im Vordergrund.

Angesichts der bisherigen Entwicklung ist nach Auffassung des LfD davon auszugehen, daß auch im öffentlichen Bereich die Zahl der Telearbeitsplätze künftig steigen wird. Wie bei anderen Formen der automatisierten Verarbeitung personenbezogener Daten sind auch bei der Einrichtung von Telearbeitsplätzen datenschutzrechtliche Anforderungen zu berücksichtigen. Wenn wirksame Sicherungsmaßnahmen ergriffen werden und keine kontrollfreien Räume entstehen, stehen datenschutzrechtliche Gesichtspunkte der Telearbeit grundsätzlich nicht entgegen.

Soweit Telearbeit im Rahmen eines Arbeits- oder Dienstverhältnisses stattfindet, handelt es sich um Datenverarbeitung des jeweiligen Arbeitgebers. Damit hat die öffentliche Stelle die nach den datenschutzrechtlichen Vorschriften erforderlichen Maßnahmen zur Sicherstellung eines ausreichenden Datenschutzes zu treffen. Im Vordergrund stehen dabei die Absicherung der Telearbeitsplätze im jeweiligen Umfeld sowie deren Anbindung an die IT-Systeme des Arbeitgebers. Die Einrichtung von Telearbeitsplätzen unterliegt nach rheinland-pfälzischem Personalvertretungsrecht weiterhin der auch in datenschutzrechtlicher Hinsicht bedeutsamen Mitbestimmung des Personalrats.

In der meist privaten Umgebung von Telearbeitsplätzen entfällt die beaufsichtigende Wirkung des üblichen Büroumfeldes. Dies kann unter Umständen Auswirkungen auf die Umsetzung organisatorischer Vorgaben der Dienststelle haben. Die Gewährleistung eines ausreichenden technisch-organisatorischen Datenschutzes muß daher Voraussetzung sein, wenn im Rahmen der Telearbeit personenbezogene Daten verarbeitet werden sollen. Telearbeit darf nicht dazu führen, daß das für die jeweilige Verwaltung festgelegte Sicherheitsniveau unterschritten wird.

Dies setzt in der Regel voraus, daß die für die Telearbeit erforderliche IT-Ausstattung vom Arbeitgeber zur Verfügung gestellt wird und Änderungen oder Ergänzungen nur mit dessen Zustimmung erfolgen dürfen. Entsprechend der Verfahrensweise in anderen Verwaltungsbereichen ist der Einsatz privater Geräte auf Ausnahmefälle zu beschränken.

Der Anschluß von Telearbeitsplätzen erfolgt häufig über öffentliche Kommunikationsverbindungen wie das ISDN-Netz der Deutschen Telekom oder das Internet, deren Nutzung nicht auf einen festgelegten Teilnehmerkreis beschränkt ist, sondern einer Vielzahl von Teilnehmern prinzipiell offensteht. Neben einer ausreichenden Zugriffskontrolle an den beteiligten IT-Systemen ist besonderes Augenmerk auf die Sicherung der Integrität und Vertraulichkeit der übertragenen Daten zu richten.

Im Rahmen eines Datenschutzkonzepts für Telearbeitsplätze sollten daher vorhandene Risiken analysiert und Vorkehrungen gegen eine unbefugte Kenntnisnahme und Nutzung der gespeicherten Daten getroffen werden. Der LfD hat die für die Einrichtung von Telearbeitsplätzen empfohlenen Maßnahmen in einer Orientierungshilfe zusammengefaßt. Die Anforderungen gleichen dabei weitgehend denen, wie sie vom LfD für die Einrichtung und den Betrieb von Fernwartungszugängen formuliert wurden (vgl. 15. Tb., Tz. 21.6.2). Danach sollten in den jeweiligen Bereichen folgende Punkte berücksichtigt werden:

Telearbeitsplatz

- Regelung über den Umfang der zulässigen Nutzung des Telarbeitsplatzes und der eingesetzten Technik.
- Absicherung des Telearbeitsplatzes gegen die unbefugte Nutzung durch Dritte, (z. B. Familienangehörige). Neben der Kontrolle des Zugriffs auf die üblicherweise eingesetzten Arbeitsplatzrechner durch Authentifizierungsverfahren (PIN-Code, Chipkarte o. ä.) kommt hierbei insbesondere die Verschlüsselung der auf dem Telearbeitsplatz gespeicherten personenbezogen Daten in Betracht.
- Protokollierung der Nutzung des Telearbeitsplatzes. Dabei ist zu berücksichtigen, daß diese Daten, soweit sie personenbezogen sind, nach § 13 Abs. 5 bzw. § 31 Abs. 5 LDSG einer engen Zweckbindung unterliegen. Insbesondere die Nutzung zu Zwecken der Verhaltens- oder Leistungskontrolle ist danach unzulässig. Im Rahmen einer Protokollierung ist aus Sicht des Datenschutzes im wesentlichen die Art der Nutzung von Interesse. Die Erfassung leistungsbezogener Angaben ist in der Regel nicht erforderlich.
- Bereitstellung sicherer Aufbewahrungsmöglichkeiten für Unterlagen und Datenträger.
- Vereinbarung über den Zutritt und die Ausübung von Kontrollrechten durch den Arbeitgeber.
- Anbindung des Arbeitsplatzes an die jeweilige Verwaltung.
- Einrichtung geschlossener Benutzergruppen bzw. virtueller privater Netze bei den genutzten Kommunikationsdiensten. Darüber hinaus empfiehlt es sich, ggf. weitere, von den Kommunikationsdiensten angebotene Sicherheitsfunktionen zu nutzen.

- Konfiguration der Anschlußkomponenten auf fest vorgegebene Hardware-Adressen (z. B. Serien-Nr. der ISDN-Karte, Adresse des Netzadapters).
- Einrichtung eines automatischen Rückrufs beim Verbindungsaufbau (Call-back) unter Verwendung fest vorgegebener Rückrufnummern.
- Aktivierung der Anschlußkomponenten nur für die Nutzungszeit, insbesondere bei nur gelegentlich genutzten Kommunikationsverbindungen.
- Verschlüsselung der Kommunikation zwischen Telearbeitsplatz und dem Rechner des Arbeitgebers bei der Übertragung auf öffentlichen Kommunikationswegen.

IT-System des Arbeitgebers

- Einsatz filternder Komponenten zur Rückweisung unberechtigter Anschlußnummern, Adressen und Diensteanforderungen.
- Protokollierung ankommender/abgehender Verbindungen.
- Um eine Revision zu ermöglichen, sind die Zugriffe der Telearbeitsplätze (Zeitpunkt, Dauer, Art des Zugriffs) in entsprechenden Protokolldateien festzuhalten und diese zu Kontrollzwecken für einen ausreichend langen Zeitraum (sechs bis zwölf Monate) aufzubewahren. Die o. g. Ausführungen zur Zweckbindung der Protokolldaten gelten entsprechend.
- Identitäts- und Authentizitätsprüfung externer Anmeldungen (Paßwortverfahren, Challenge-response-Mechanismen).
- Restriktive Ausgestaltung der Zugriffsrechte externer Anmeldungen.
- Ausführung von Telearbeiten und Datenübertragungen unter separaten, über Identifikations- und Authentisierungsmechanismen geschützte Benutzerkenmungen. Dabei ist sicherzustellen, daß über einen bestimmten Zeitraum hinweg nicht genutzte Kennungen automatisch deaktiviert werden.

Fazit:

Datenschutzrechtliche Gesichtspunkte stehen der Telearbeit im Verwaltungsbereich grundsätzlich nicht entgegen. Die notwendigen Maßnahmen des technisch-organisatorischen Datenschutzes konzentrieren sich auf den Telearbeitsplatz und dessen Anbindung an das IT-System des Arbeitgebers.

Die speichernde Stelle muß sicherstellen, daß die Einrichtung und Nutzung von Telearbeitsplätzen nur mit ihrem Einverständnis und entsprechend ihrer Vorgaben erfolgen kann. Kontrollrechte des Arbeitgebers und anderer Stellen müssen wirksam ausgeübt werden können. Die erforderlichen Regelungen sind in einer Dienstanweisung festzulegen. Für die Einrichtung von Telearbeitsplätzen sollte ein Verfahren vorgesehen werden, das neben arbeitsrechtlichen, organisatorischen und technischen Aspekten auch die datenschutzrechtlich relevanten Punkte berücksichtigt.

21.8 Datenschutzregister

21.8.1 Entwicklung und gegenwärtiger Stand

Der LfD ist gem. § 27 Abs. 3 LDSG verpflichtet, ein Register der Verfahren, in denen personenbezogene Daten automatisiert verarbeitet werden, zu führen. Das Datenschutzregister ist für die Arbeit des LfD von nicht zu unterschätzender Bedeutung. Häufig werden datenschutzrechtliche Defizite, wie z. B. Löschungsfristen oder Speicherungen nicht erforderlicher personenbezogener Merkmale in automatisierten Verfahren nur aufgrund von Anmeldungen zum Datenschutzregister bekannt. Die Bedeutung des Datenschutzregisters ist auch aus der zahlenmäßigen Entwicklung der Anmeldungen zu ersehen. Im Jahre 1993 waren ca. 4 000 Verfahren im Datenschutzregister gespeichert (vgl. 14. Tb., Tz. 22.4). In der Zwischenzeit ist die Zahl der gespeicherten Verfahren auf ca. 7 000 angestiegen.

21.8.2 Zentral entwickelte Verfahren

Der LfD verkennt nicht den Verwaltungsaufwand, der für die Anmeldung zum Datenschutzregister gem. § 27 LDSG erforderlich ist. Er ist jedoch stets bemüht, diesen so gering wie möglich zu halten. Hierzu zählt auch, daß den Behörden neben zahlreichen Informationen zum Datenschutz auch das Anmeldeformular auf Diskette zur Verfügung gestellt werden kann. Fernerhin wurde im zurückliegenden Berichtszeitraum eine Vielzahl von Verfahren in die Liste der zentral entwickelten Verfahren gem. § 27 Abs. 2 LDSG eingetragen; inzwischen sind 131 Verfahren in dieser Liste enthalten. Diese Eintragung hat zur Folge, daß öffentliche Stellen, die ein in dieser Liste enthaltenes Verfahren einsetzen, nur noch eine verkürzte Anmeldung vornehmen

müssen. Eine Übersendung der vollständigen Verfahrensbeschreibung ist in diesen Fällen entbehrlich. Der LfD ist stets bestrebt, die Liste der zentral entwickelten Verfahren weiter auszubauen, um dadurch den Verwaltungsaufwand im Zusammenhang mit dem Anmeldeverfahren zu reduzieren.

21.8.3 Anmeldepflicht nach § 27 LDSG

21.8.3.1 Textverarbeitung

Textverarbeitung erfolgt heute regelmäßig auf multifunktional verwendbaren Geräten, die zwar eine spezialisierte Softwarekomponente „Textverarbeitung" besitzen, die jedoch grundsätzlich den Einsatz des gesamten Instrumentariums der automatisierten Datenverarbeitung (insbesondere der Datenbankerstellung und -nutzung, aber auch der Indexierung von Texten und/oder der umfassenden textübergreifenden Recherchen) zulassen.

§ 27 LDSG verpflichtet zur Anmeldung von Verfahren, in denen von öffentlichen Stellen personenbezogene Daten automatisiert verarbeitet werden. Ein automatisiertes Verfahren liegt vor, wenn wesentliche Verfahrensschritte, insbesondere das Lesen und Vergleichen von Daten, in programmgesteuerten Einrichtungen ablaufen. Dabei genügt es, daß die gespeicherten personenbezogenen Daten automatisiert ausgewertet werden können. Da dies bei den heutigen Textverarbeitungsprogrammen regelmäßig der Fall ist, sind diese damit auch gem. § 27 LDSG zur Eintragung in das Datenschutzregister anzumelden.

Sofern in Ausnahmefällen Textverarbeitungssysteme eingesetzt werden, bei denen die erstellten Texte, die personenbezogene Daten enthalten, nur kurzfristig gespeichert werden, unterliegen diese Verfahren nicht der Anmeldepflicht gem. § 27 Abs. 1 LDSG (vgl. 13. Tb., Tz. 20.7.)

Ist der Einsatz eines solchen Textverarbeitungsverfahrens einmal gem. § 27 Abs. 1 Satz 1 LDSG ordnungsgemäß angemeldet, umfaßt diese Anmeldung entsprechend dem Umfang der Angaben in der Verfahrensbeschreibung die Erstellung und Speicherung der dienstlich anfallenden Korrespondenz und vergleichbarer Texte (z. B. Schriftstücke, Vermerke, Adreßlisten für die Korrespondenz). In diesem Fall genügt in der Anmeldung die Angabe des Zwecks der Datenverarbeitung.

Werden darüber hinaus in den so beschriebenen Textverarbeitungssystemen gleichartige personenbezogene Informationen für dateiartige Nutzung auswertbar gespeichert, so löst dies eine gesonderte Anmeldepflicht aus, insbesondere dann, wenn der Zweck sowie der Eingriff für die Betroffenen der Nutzung eines gesonderten Verfahrens vergleichbar ist (z. B. Listen von Sozialhilfeempfängern, Jubilaren, Ehrengästen, Personallisten).

Wird im Zusammenhang mit der Textverarbeitung ein Datenbankverwaltungssystem oder eine Tabellenkalkulationssoftware eingesetzt, z. B. für die Verwaltung von Adressen, sind grundsätzlich die o. g. Kriterien erfüllt. Für jedes Verfahren (nicht zwingend für jede Datei) ist daher eine gesonderte Anmeldung unter Beifügung des Ausdrucks der Datenbankbeschreibung bzw. der Tabellenstruktur vorzunehmen.

21.8.3.2 Internet-Anschluß

In letzter Zeit wächst bei den öffentlichen Stellen der Wunsch nach einem Zugang zum Internet. Während in der Vergangenheit das Internet hauptsächlich von wissenschaftlichen Einrichtungen genutzt wurde, ist inzwischen eine immer stärker ausgeprägte Nutzung für kommerzielle Zwecke zu beobachten. Neben der Informationsgewinnung soll die Neztanbindung auch zur Bereitstellung von eigenen Informationen für andere dienen. Beide Nutzungsarten sind bei der Beurteilung der Anmeldepflicht gemäß § 27 LDSG zu unterscheiden.

Internet zur Informationsgewinnung

Die eingesetzten Programme zur Internet-Nutzung (Browser) bieten u. a. die Möglichkeit, Daten aus dem Internet auf den lokalen PC zu übernehmen. Bei den übernommenen Daten kann es sich auch um personenbezogene Daten handeln. Soweit es sich hierbei um Daten handelt, die im Sinne des § 2 Abs. 5 LDSG zur Veröffentlichung bestimmt sind (z. B. Autorenangaben, Literaturverzeichnisse), sind diese Daten im Internet nicht besonders geschützt. Dies hat zur Folge, daß das LDSG in diesem Falle nicht anwendbar ist; eine Anmeldepflicht des Internet-Zugangs als eigenes Verfahren nach § 27 Abs. 1 Satz 1 LDSG entfällt.

Aus einer Internet-Anbindung ergeben sich unter Sicherheitsaspekten zusätzliche Risiken für das IT-System, über welches der Zugriff erfolgt, und damit für die dort betriebenen Verfahren.

Soweit daher eine Internet-Verbindung auf Systemen eingerichtet wird, auf welchen nach § 27 LDSG meldepflichtige Verfahren betrieben werden, stellt dies eine wesentliche Änderung der technischen Rahmenbedingungen dar, die dem LfD mitzuteilen ist.

Internet zur Bereitstellung von Informationen

Immer häufiger stellen öffentliche Stellen Informationen zum Abruf im Internet bereit. Werden diese Informationen auf einem von der öffentlichen Stelle betriebenen Web-Server angeboten, stellt sich die Frage der Anmeldepflicht nach § 27 LDSG.

In aller Regel werden die Zugriffe von Internet-Benutzern durch den Server-Betreiber (öffentliche Stelle) mit Internet-Adresse, Zeitpunkt, Häufigkeit, Art und Inhalt der Zugriffe auf Web-Seiten sowie gegebenenfalls weitere Angaben protokolliert. Damit kann grundsätzlich das Kommunikations- und Nutzerverhalten nachvollzogen werden. Eine derartige Protokollierung – soweit sie personenbezogen oder personenbeziehbar ist – bewirkt, daß der Betrieb des Interet-Servers durch die öffentliche Stelle als eigenständiges Verfahren gemäß § 27 Abs. 1 LDSG zur Eintragung in das Datenschutzregister anzumelden ist. Auch eine zeitnahe Löschung der einzelnen Protokolldaten führt nicht zu einem Wegfall der Anmeldepflicht, da die Protokolldatei als solche für einen unbestimmten Zeitraum geführt wird.
Entsprechendes gilt auch, wenn die Web-Seiten im Auftrag durch einen Provider im Internet bereitgestellt werden.

Sofern der Web-Server ausnahmsweise auf einem IT-System eingerichtet wird, auf dem bereits meldepflichtige Verfahren gem. § 27 LDSG betrieben werden, stellt dies ebenfalls eine wesentliche Änderung der technischen Rahmenbedingungen im Sinne des § 27 Abs. 1 Satz 3 LDSG dar, die dem LfD mitzuteilen ist.

22. Öffentlich-rechtliche Wettbewerbsunternehmen, Sparkassen

22.1 Nutzung von Daten einer Direktmarketingfirma zu Werbezwecken

Ein rheinland-pfälzisches Wettbewerbsunternehmen, das auch Versicherungen vermittelt, fragte an, ob es sich Adressendaten bei einer Direktmarketingfirma beschaffen dürfe, um Kunden zu werben. So würden Direktmarketingfirmen Listen mit Daten von Doppelverdienern ohne Kinder anbieten. Es gebe u. a. auch Listen von Personen mit „höchster Kaufkraft" sowie Faxbesitzern.

Voraussetzung der zulässigen Speicherung und Nutzung von Daten durch sog. „öffentlich-rechtliche Wettbewerbsunternehmen" ist, daß die Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden (§ 28 Abs. 1 Satz 2 BDSG). Wenn die Daten erkennbar unzulässig durch einen Dritten gespeichert und übermittelt worden sind, ist die Erhebung dieser Daten nicht zulässig. Vor diesem Hintergrund war also zunächst zu klären, ob der Anbieter der Anschriften, eine Direktmarketingfirma, die angebotenen Daten zulässigerweise gespeichert hat. Zu diesem Zweck hat der LfD die für den Anbieter zuständige Datenschutzaufsichtsbehörde um Prüfung gebeten. Es ergab sich folgendes:

Die Adressenanbieter speichern zunächst keine konkreten Namen und Anschriften, um die Kaufkraft von Einzelpersonen bewerten zu können. Sie erfassen vielmehr bestimmte Wohngebiete, die dann bewertet werden. Für die Bewertung maßgeblich sind allgemein zugängliche statistische Daten sowie Erkenntnisse, die durch eine sog. Wohnstrukturanalyse gewonnen wurden. Dabei wurden flächendeckend Ortsbegehungen in den alten Bundesländern durchgeführt und die vorhandenen Gebäude nach Alter, Größe, Charakteristik, Gestaltung, Zustand und Lage bewertet. Die kleinste erfaßte Einheit umfaßt fünf Haushalte (entweder fünf Einfamilienhäuser oder ein Haus mit mindestens fünf Haushalten). Eine namentliche Erhebung der Hausbewohner hat nicht stattgefunden. Aufgrund der bei der Wohnstrukturanalyse gewonnenen Daten werden allgemeine Rückschlüsse auf die Vermögensverhältnisse und die Lebens- und Konsumgewohnheiten der Bewohner gezogen, da man aufgrund der Erkenntnisse der Markt- und Meinungsforschung davon ausgeht, daß sich der Lebensstil und das Kaufverhalten von Personen durch ihre Wohnverhältnisse nach dem Prinzip „gleich und gleich gesellt sich gern" erklären läßt. Die durch die Wohnstrukturanalyse erhobenen Daten dienen auch dazu, unterschiedliche Bedarfssituationen für bestimmte Konsumartikel festzulegen.

Diese Daten der Wohnstrukturanalyse werden dann mit sonstigen allgemein zugänglichen Quellendaten (aus Telefonbüchern, Adreßbüchern etc.) abgeglichen. Das Ergebnis wird an werbewillige Unternehmen verkauft.

Auch die Selektion von Altersgruppen basiert nicht auf konkretem Wissen, sondern auf mathematisch-statistischen Analyseverfahren. Das Alter einer Person wird über die Vornamensanalyse eingeschätzt und einer von insgesamt vier Altersklassen zugeordnet. Ein Fritz ist statistisch gesehen älter als ein Richard, ein Richard statistisch älter als ein Markus.

Die Zuordnung von Personen zu Zielgruppen beruht damit nicht auf konkreten Informationen, sondern ergibt sich aus einer Kombination von Wahrscheinlichkeiten. Je nach den Kriterien, die der Adreßanbieter aus dem vorhandenen Angebot auswählt, wird dieser Personenkreis bei jedem Auftrag neu zusammengestellt. Die Informationen aus der Wohnstrukturanalyse und andere statistische Erkenntnisse sind orts- bzw. straßenabschnittsbezogen gespeichert. Die Kunden der Direktmarketingfirma können diese Informationen mit ihrem eigenen Adreßbestand oder dem angemieteten Adreßbestand abgleichen lassen mit der Folge, daß alle in dem jeweiligen Straßenabschnitt wohnenden Personen automatisch der definierten Zielgruppe zugewiesen werden.

Die rechtliche Beurteilung, ob ein solches Verfahren zulässig ist, wird derzeit durch die Datenschutzaufsichtsbehörde für den privaten Bereich vorgenommen. Der hierzu laufende Abstimmungsprozeß ist nach den dem LfD vorliegenden Informationen noch nicht abgeschlossen.

Bezüglich der Liste der Doppelverdiener ohne Kinder (sog. „Dinks") konnte festgestellt werden, daß der Lieferant dieser Daten eine in Campione ansässige Firma ist. Campione ist eine italienische Exklave in der Schweiz.

Welchen Quellen diese Daten ursprünglich entnommen worden sind, konnte nicht geklärt werden.

Die Liste der Akademiker könnte nach Auffassung der Datenschutzaufsichtsbehörde aus öffentlich zugänglichen Quellen (Telefon- und Adreßbücher) entnommen worden sein.

Im Ergebnis hat der LfD festgestellt, daß wegen der ungeklärten Herkunft und der inhaltlichen Sensitivität die Listen der „Dinks" durch öffentliche Stellen des Landes Rheinland-Pfalz nicht verwendet werden dürfen. Die Erhebung dieser Daten würde nach seiner Auffassung einen Verstoß gegen § 28 Abs. 1 Satz 2 BDSG begründen. Bezüglich der anderen Listen bestehen vergleichbare Bedenken nicht.

22.2 Beschränkung der filialübergreifenden Zugriffsmöglichkeiten auf Bankkonten

Bereits im 15. Tb. (Tz. 22.1) hat der LfD über das Problem berichtet, daß Sparkassenkunden nicht die Freiheit der Wahl haben, entscheiden zu können, welche Filiale auf ihre Kontendaten zugreifen kann. Es ist vielmehr so, daß technisch jede Filiale einer großen Sparkassenorganisation auf Daten jedes Kunden Zugriffsmöglichkeiten besitzt. Allerdings werden alle Zugriffe protokolliert, so daß die Einhaltung der hier bestehenden Verbote grundsätzlich überprüft werden kann.

Auf die Eingabe eines Sparkassenkunden hin hat der LfD örtliche Feststellungen bei einer Sparkasse getroffen und die aufgezeichneten Zugriffsprotokolle daraufhin überprüft, ob unzulässige Lesezugriffe auf die Konteninformationen des fraglichen Kunden erfolgt sind.

Bei der konkreten Stichprobenprüfung hat sich kein Anhaltspunkt für unzulässige Zugriffe auf die entsprechenden Kontendaten (Girokonto und Sparkonto) ergeben.

Eine umfassende Prüfung, von welchen Terminals jeweils auf die Kontenbestandsdaten lesend zugegriffen wurde, konnte aus technischen Gründen allerdings nicht erfolgen. Die Sparkasse war an ein Verfahren angeschlossen, in dem zwar sämtliche Abfragen von allen vorhandenen Terminals auf die Kontendaten protokolliert wurden. Diese Protokolldaten, die zum Zweck der Innenrevision und der Datenschutzkontrolle erstellt wurden, waren jedoch nur auf Mikrofiches verfügbar. Nach der zeitnah erfolgenden Übertragung auf diese Datenträger wurden die zugrundeliegenden Speichermedien der EDV erneut eingesetzt und überschrieben. Eine automatisierte Auswertung dieser Protokolldaten war deshalb nicht möglich. Dementsprechend konnte sich die örtliche Prüfung nur darauf beschränken, stichprobenweise durch Auswertung der Mikrofiches die Protokollierung bezüglich einiger Abfrageterminals, die unter prüfungstechnischen Gesichtspunkten ausgewählt worden waren, daraufhin zu überprüfen, ob die Kontonummern des Beschwerdeführers betroffen waren.

Allerdings ist nunmehr flächendeckend in Rheinland-Pfalz bei allen Sparkassen ein System der automatisierten Datenverarbeitung eingesetzt, das auch die automatisierte Auswertung der Protokolldaten erlaubt. Nunmehr kann also auch flächendeckend und zeitlich umfassend festgestellt werden, von welchem Abfrageterminal aus auf bestimmte Kontonummern zugegriffen wurde. Die jetzt mögliche automationsunterstützte Kontrolle bietet aus Sicht des LfD einen weitgehenden und akzeptablen Schutz vor mißbräuchlichen Abfragen.

Das grundsätzliche datenschutzrechtliche Anliegen bleibt dennoch bestehen, auch technische Zugriffsschranken gegen unberechtigte Abrufe einzurichten.

Diesbezüglich sind allerdings derzeit keine Fortschritte ersichtlich.

22.3 Personenverwechslung bei Kontenpfändung

Ein Bürger trug vor, daß seine EC-Karte beim Versuch, den Kontostand an einem Geldautomaten abzufragen, einbehalten worden sei. Seine Sparkasse habe ihm mitgeteilt, das Finanzamt hätte wegen rückständiger Steuerschulden eine Kontopfändung vorgenommen.

Vom Finanzamt erhielt der Bürger die Mitteilung, daß diese Pfändung gegen einen Steuerschuldner mit dem gleichen Namen, aber anderer Wohnanschrift gerichtet gewesen sei.

Es ergab sich, daß die Sparkasse den Kontoinhaber mit dem Steuerschuldner verwechselt hatte. Der entscheidende Grund für die Verwechslung war, daß die Sparkasse versäumt hatte, das vom Finanzamt angegebene Geburtsdatum mit dem Geburtsdatum des verwechselten Kontoinhabers zu vergleichen.

Aus datenschutzrechtlicher Sicht war festzustellen, daß derartige Verwechslungsfälle für den Betroffenen besonders ärgerlich und mißlich sind, weil er als Nichtbetroffener mit Vollstreckungsmaßnahmen konfrontiert wird. Außerdem gehen solche Verwechslungsfälle immer auch mit überflüssigen Informationen des fälschlich in Anspruch genommenen Bürgers über die Person und die Schulden desjenigen einher, mit dem er verwechselt wurde.

Da die Sparkasse erklärt hat, alle Maßnahmen eingeleitet zu haben, um künftig ähnliche Mißgeschicke zu vermeiden, konnte der LfD von einer förmlichen Beanstandung absehen.

22.4 Umsetzung des Geldwäschegesetzes, Personalausweiskopien durch Kreditinstitute

Immer wieder wenden sich Bürger an den LfD mit dem Vortrag, daß ihre Sparkasse bei den verschiedensten Gelegenheiten auch während eines laufenden Girokontenverhältnisses erkläre, daß der Personalausweis kopiert werden müßte. So wurde dies von einem Kunden verlangt, der seinem Sohn eine Kontovollmacht erteilen wollte, obwohl er schon seit längerem Kunde der Sparkasse gewesen war. Ein anderer Kunde wurde anläßlich einer größeren Geldüberweisung aufgefordert, den Ausweis kopieren zu lassen.

Es besteht in all diesen Fällen Einvernehmen mit dem Sparkassen- und Giroverband, daß dann, wenn die Voraussetzungen des Geldwäschegesetzes nicht vorliegen, nur eine Identifikationspflicht nach § 154 AO besteht, wonach das Kreditinstitut aber nicht verpflichtet ist, den Ausweis zu kopieren. Nach Auffassung des LfD besteht zwar ein Recht der Sparkassen, auch eine Kopie des Personalausweises zu den Akten zu nehmen, dies aber nur dann, wenn die Kunden in diesen Fällen damit einverstanden sind. Es gehört zur rechtmäßigen Datenerhebung nach Treu und Glauben, die Kunden darauf aufmerksam zu machen, daß keine Pflicht besteht, die Aufnahme einer Kopie des Personalausweises in die Unterlagen der Sparkasse zu dulden.

In der Praxis wird dies nicht immer beachtet. Der LfD hat den Sparkassen- und Giroverband erneut darauf hingewiesen.

22.5 Übermittlung der Jahresabrechnung für Strom an einen Wohnungseigentümer

Ein Wohnungseigentümer, der in einem Wohnblock mit 21 Wohneinheiten wohnte, hatte Bedenken, ob seine Hausverwaltung von zutreffenden Zahlen bei der Jahresabrechnung für den Strom-, Gas- und Wasserverbrauch ausgegangen war. Deshalb verlangte er von den Stadtwerken die Übersendung der Jahresrechnung. Die Stadtwerke verweigerten ihm dies mit der Begründung, die Gesamtjahresabrechnung unterliege dem Datenschutz.

Der LfD beurteilte diesen Vorgang wie folgt:

Rechtsgrundlage für die Übermittlung von Daten durch die Stadtwerke an einen Wohnungseigentümer ist § 28 Abs. 2 Nr. 1 a BDSG. Danach ist eine Datenübermittlung dann zulässig, wenn der Datenempfänger ein berechtigtes Interesse an den Daten geltend machen kann und wenn kein Grund zur Annahme besteht, daß der Betroffene selbst ein schutzwürdiges Interesse am Ausschluß der Übermittlung hat.

Ein berechtigtes Interesse des einzelnen Wohnungseigentümers an der Kenntnisnahme der Gesamtabrechnungsdaten für die Wohnanlage ist vorhanden. Betroffener ist die Wohnungseigentümergemeinschaft insgesamt. Schutzwürdige Interessen dieser Gemeinschaft, die eine Übermittlung der Jahresabrechnung an einen einzelnen Eigentümer hindern könnten, sind allerdings nicht ersichtlich. Auch die Stadtwerke konnten auf Nachfrage keinen Gesichtspunkt nennen, der hier hätte berücksichtigt werden müssen. Im Ergebnis teilte der LfD den Stadtwerken mit, daß sie jedenfalls aus datenschutzrechtlichen Gründen nicht gehindert waren, eine Kopie der Jahresabrechnung an den Eigentümer zu übersenden. Die Stadtwerke haben schließlich dem Wunsch des Beschwerdeführers entsprochen.

23. Sonstiges

23.1 Datenübermittlung aus Akten des Bauaufsichtsamtes

Das Bauaufsichtsamt hatte versehentlich ein Schreiben in eine falsche Akte geheftet. Der Bauherr, in dessen Akte dieses Schreiben versehentlich gelangt war, nahm in seine eigene Akte Einsicht und kopierte sie auch vollständig. Das fragliche Schreiben betraf zufällig einen Freund des einsichtnehmenden Bauherrn, der dieses Schreiben in einem Rechtsstreit gegen einen Dritten verwandte.

Der LfD ist der Auffassung, daß in diesem Zusammenhang Daten unzulässig übermittelt wurden. Diese unzulässige Datenübermittlung hat er beanstandet. Bei der Gewichtung des hier in Rede stehenden Vorganges war zu berücksichtigen, daß keine Anzeichen dafür sprachen, daß ein Bediensteter vorsätzlich zum Nachteil eines Betroffenen gehandelt hätte. Andererseits ist das

fehlerhafte Abheften von Schriftstücken ein keineswegs unbeachtlicher Verstoß gegen Sorgfaltspflichten. Als Organisationsmangel ist es darüber hinaus zu werten, daß es unterlassen wurde, die Akte vor der Einsichtsgewährung daraufhin durchzusehen, ob durch die Einsichtsgewährung Belange Dritter beeinträchtigt werden könnten. Diesbezüglich existierte auch keine allgemeine Weisung bei der Kreisverwaltung. Die Pflicht, entsprechend auf die Belange Dritter zu achten, ergibt sich nach Auffassung des LfD aus § 29 Abs. 2 i. V. m. § 30 VwVfG.

23.2 Einsichtnahme in eine Bauakte durch einen Nachbarn

Die Beschwerdeführer führten mit ihren Nachbarn einen nachbarrechtlichen Grenzstreit. Den Nachbarn wurde durch die Bauaufsichtsbehörde der Stadt Einsicht in die Bauakten gegeben. Die Bauaufsichtsbehörde erklärte auf Nachfrage durch den LfD, sie habe den Nachbarn deshalb Einblick in die Bauakte gewährt, weil diese vorgetragen hätten, daß am fraglichen Grundstück baurechtswidrige Änderungen vorgenommen worden wären. Bei der gemeinsamen Einsichtnahme des Bauaufsichtsamts und der Nachbarn sei tatsächlich festgestellt worden, daß durch die betroffenen Beschwerdeführer erhebliche Veränderungen im Geländeniveau vorgenommen worden sind, für die die baurechtliche Genehmigung nicht eingeholt worden ist.

Die gemeinsame Akteneinsichtsnahme durch das Bauaufsichtsamt und die Nachbarn stellte sich im vorliegenden Fall also als Ermittlungsmaßnahme der Bauaufsichtsbehörde dar. Die Akteneinsicht war dazu bestimmt, den Sachverhalt aufzuklären. Offensichtlich haben die Nachbarn als Zeugen über die tatsächlichen Verhältnisse vor Ort Einblick in die Bauunterlagen erhalten, um auf Abweichungen zwischen Plan und Realität hinweisen zu können.

Wenn der Verdacht besteht, daß baurechtswidrige Veränderungen vorgenommen worden sind, liegt der Verdacht einer Ordnungswidrigkeit vor. Die untere Bauaufsichtsbehörde ist gleichzeitig Ordnungswidrigkeitenbehörde, die zur Aufklärung des Sachverhalts grundsätzlich die Befugnisse besitzt, die die Staatsanwaltschaft bei der Aufklärung von Straftaten in Anspruch nehmen kann. Als Rechtsgrundlage für die hier erfolgte Ermittlungshandlung war demnach § 46 Abs. 1 und 2 OwiG i. V. m. §§ 161, 69 Abs. 1 StPO heranzuziehen.

Die Ermittlungsmaßnahme war auch verhältnismäßig. Als Ergebnis war festzustellen, daß die erfolgte Einsichtsgewährung zulässig war.

23.3 Datenerhebungen und -übermittlungen im Zusammenhang mit der Aufstellung des Bebauungsplans

Eine Verbandsgemeinde wandte sich mit folgendem Anliegen an den LfD:

Im Zusammenhang mit der Aufstellung eines Bebauungsplanes habe ein Planbetroffener angeführt, daß die Grundstücke, die in seinem Eigentum stünden, wegen Pflichten aus einem landwirtschaftlichen Förderprogramm nicht für den Bebauungsplan genutzt werden könnten. Die Verbandsgemeinde wollte nun die Aussagen des Planbetroffenen überprüfen. Deshalb bat sie die Kreisverwaltung um Auskunft, ob tatsächlich eine solche Teilnahme am landwirtschaftlichen Förderprogramm vorgelegen hätte.

Die Kreisverwaltung berief sich jedoch auf Datenschutz und erteilte die Auskunft nicht.

Der LfD beurteilte die Angelegenheit wie folgt:

Für die Aufstellung des Bebauungsplanes sind die Nutzungsverpflichtungen der Eigentümer von Grundstücken im künftigen Geltungsbereich des Bebauungsplans grundsätzlich unerheblich. Dies gilt auch dann, wenn es sich um Verpflichtungen aufgrund öffentlich-rechtlicher Verträge handelt. Der Bebauungsplan hat allein die öffentlichen Interessen der Gemeinde an der weiteren Entwicklung des Gemeindegebiets, also die Interessen der Allgemeinheit, zu berücksichtigen (§ 1 Abs. 5 BauGB).

Davon zu unterscheiden ist die Frage, wie mit den Verpflichtungen, die auf den im Bebauungsplangebiet gelegenen Grundstücken lasten bzw. die die Eigentümer in bezug auf diese Grundstücke vertraglich eingegangen sind, im Rahmen des Umlegungsverfahrens umzugehen ist. Dafür enthält § 61 BauGB die maßgebliche Regelung. Derartige Rechte können durch den Umlegungsplan aufgehoben, geändert oder neu begründet werden.

Vor diesem Hintergrund bestand aus Sicht des LfD keine Erforderlichkeit zur Erhebung der von der Gemeinde begehrten Informationen. Im Rahmen des Umlegungsverfahrens würde es dann zu den Obliegenheiten des betroffenen Eigentümers gehören, die bestehenden auf den Grundstücken ruhenden Lasten (zu denen auch eine Nutzungsverpflichtung in einem landwirtschaftlichen Förderprogramm gehören kann) darzulegen und entsprechende Nachweise vorzulegen. Bei fehlender Nachweiserbringung würden die entstehenden Nachteile dann zu Lasten des betroffenen Eigentümers gehen.

Aus dieser Sicht hat der LfD das Verhalten der Kreisverwaltung für datenschutzrechtlich geboten gehalten. Es war kein Gesichtspunkt ersichtlich, unter dem die von der Gemeindeverwaltung erbetenen Informationen für den Fortgang des Bebauungsplanverfahrens erforderlich waren.

23.4 Datenübermittlungen durch die Lastenausgleichsämter

Obwohl das Lastenausgleichsrecht eigentlich als auslaufendes Rechtsgebiet anzusehen ist, haben sich im Berichtszeitraum doch im Zusammenhang mit Lastenausgleichsverfahren relevante datenschutzrechtliche Fragen ergeben.

Zunächst war zu beurteilen, ob die bei der Bezirksregierung Düsseldorf (Abt. Wiedergutmachung) bestehende Bundeszentralkartei mit Angaben über alle Entschädigungsverfahren, die im Bundesgebiet durchgeführt worden sind, zulässigerweise Daten von den rheinland-pfälzischen Entschädigungsbehörden erhält.

Zweck der Zentralkartei bei der Bezirksregierung Düsseldorf ist es vor allem, Doppelzahlungen zu vermeiden.

Die Einrichtung zentraler Datenbestände zur Vermeidung rechtswidriger Leistungen hat den LfD in der Vergangenheit bereits in verschiedenen Zusammenhängen beschäftigt. So ist eine vergleichbare Diskussion bezüglich der Frage geführt worden, ob die Festtellungsprüfungen für die Hochschulzulassung ausländischer Studienbewerber an eine Zentralstelle gemeldet werden dürfen und aufgrund welcher Rechtsgrundlage dies erfolgen kann. Auf der Ebene des Landes ist diskutiert worden, ob sog. Krankenhauswanderer, die betrügerisch Krankenhausleistungen in Anspruch nehmen, bei einer Zentralstelle gemeldet und gespeichert werden dürften. Im Zusammenhang mit der Überwachung von Zirkusunternehmen ist erörtert worden, ob eine zentrale Erfassung dieser Unternehmen zulässig ist und auf welcher Rechtsgrundlage dies ggf. erfolgen kann.

Grundsätzlich hat der LfD in diesem Zusammenhang die Auffassung vertreten, daß das Institut der Auftragsdatenverarbeitung geeignet ist, um eine solche zentrale Datenverarbeitung datenschutzrechtlich zu begründen und zu beschränken. Da der Abgleichsvorgang innerhalb der zentralen speichernden Stellen jedoch den Charakter einer eigenständigen Nutzung besitzt, hat der LfD ergänzend bereichsspezifische gesetzliche Regelungen für vorzugswürdig gehalten. Erforderlich wären solche bereichsspezifischen Regelungen jedenfalls dann, wenn die Übermittlung der „Trefferfälle" nicht auf das jeweilige Landesdatenschutzgesetz gestützt werden könnte. Im Ergebnis hat der LfD allerdings auch unter diesen Gesichtspunkten keine Einwände gegen Datenübermittlungen an die Zentralkartei bei der Bezirksregierung Düsseldorf erhoben.

Wie wichtig Auskünfte aus dieser Zentralkartei und auch weitere Informationen über Entschädigungsverfahren sein können, hat dann die derzeit umstrittene Frage gezeigt, ob an Lebensversicherungsunternehmen Auskünfte über erteilte Entschädigungsleistungen gegeben werden dürfen.

Hintergrund dieser Frage ist, daß in den Vereinigten Staaten eine Klage anhängig ist, in der ehemals Verfolgte des Naziregimes oder ihre Erben deutsche Lebensversicherungsunternehmen deshalb in Anspruch nehmen wollen, weil Lebensversicherungsverträge mit den Verfolgten nicht erfüllt worden seien.

Im Zuge dieses Rechtsstreits haben deutsche Lebensversicherungsunternehmen bei den Entschädigungsbehörden auch des Landes Rheinland-Pfalz angefragt, ob bestimmte Kläger in diesem Verfahren Entschädigungsleistungen empfangen haben.

Die Frage, ob entsprechende Auskünfte zulässig sind, hat der LfD wie folgt beantwortet:

Als Rechtsgrundlage für eine entsprechende Datenübermittlung kommt nur § 16 Abs. 1 Nr. 3 LDSG in Betracht. Damit müßten folgende Voraussetzungen vorliegen:

Die empfangende Stelle müßte ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft machen, und es darf kein Grund zur Annahme bestehen, daß überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen.

Der LfD ist der Auffassung, daß die Lebensversicherungsgesellschaften bislang ihr rechtliches Interesse noch nicht ausreichend dargelegt haben. Sie haben zwar vorgetragen, sie benötigten die Angaben, um sich gegen eine Schadensersatzklage amerikanischer Holocaustopfer verteidigen zu können, mit der ein Anspruch in Höhe von rund 29 Milliarden DM geltend gemacht werde.

Die Behauptung allein, daß die begehrten Angaben erforderlich seien, um sich gegen eine Schadensersatzklage verteidigen zu können, reicht allerdings nicht aus, um ein rechtliches Interesse zu begründen. Es müßte vielmehr plausibel dargelegt werden, daß sich die Anfragen der Versicherungen auf konkrete Kläger in diesem Schadensersatzprozeß beziehen oder daß die Kläger im Schadensersatzprozeß Rechtsnachfolger (Erben) der von den Anfragen betroffenen Personen sind. Weiter müßte dargelegt werden, welche rechtliche Folge die Information, daß eine bestimmte Person Entschädigungsleistungen erhalten hat, für den geltend gemachten Schadensersatzanspruch hat. Derzeit ist unklar, ob und unter welchen Voraussetzungen dann der Schadensersatzanspruch der amerikanischen Kläger entfallen würde und welcher konkrete Anspruch überhaupt Klagegegenstand des fraglichen Prozesses ist. Voraussetzung einer Übermittlung wäre also, daß die anfragenden Versicherungsunternehmen die rechtliche und tatsächliche Situation darlegen, die ihr rechtliches Interesse begründen. Dann wäre zu entscheiden, welche Mittel zur Glaubhaftmachung des entsprechenden Vortrages geeignet sind. Hier käme etwa die Vorlage der US-amerikanischen Klageschrift in Kopie in Betracht.

Unsubstantiierte Behauptungen sind generell nicht dazu geeignet, das rechtliche Interesse zu begründen: Die übermittelnde Stelle muß vielmehr in die Lage versetzt werden, das rechtliche Interesse konkret nachvollziehen zu können.

Wenn dies erfolgt, stehen nach Auffassung des LfD keine schutzwürdigen Belange der Betroffenen einer entsprechenden Übermittlung entgegen. Diese Interessen müßten nämlich angesichts eines rechtlichen Interesses des Übermittlungsempfängers über das bloße allgemeine Interesse an der Wahrung der Privatheit oder den Schutz von persönlichen Daten hinausgehen. Solche das Schutzbedürfnis steigernde und ein rechtliches Interesse der Anfragenden überwiegende Umstände sind nicht ersichtlich.

Mit diesem Ergebnis hat auch das nordrhein-westfälische Ministerium des Innern entsprechende Anfragen zunächst nicht beantwortet.

Welche Auffassung das Ministerium der Finanzen hierzu vertritt, ist derzeit noch nicht bekannt.

23.5 Härtefonds des Landes zur Unterstützung von Opfern des Nationalsozialismus

Im Haushaltsplan des Landes wurden Mittel für die Unterstützung von Opfern des Nationalsozialismus bereitgestellt. Für die Verteilung dieser Mittel wurden Richtlinien erlassen (Richtlinien des Ministeriums der Finanzen für den Härtefonds des Landes Rheinland-Pfalz zur Unterstützung von Opfern des Nationalsozialismus vom 30. September 1996, Az.: 434-111.1).

In diesen Richtlinien sind die materiellen Voraussetzungen geregelt, unter denen Unterstützungsleistungen gewährt werden. Voraussetzung ist jeweils die Stellung eines Antrages beim Amt für Wiedergutmachung in Saarburg. Bei der Entscheidung sind eine Reihe unbestimmter Rechtsbegriffe auszulegen. Auch die Höhe der Unterstützung ist durch die Richtlinie nicht eindeutig vorgegeben. Das Amt für Wiedergutmachung hat das Votum eines Beirats zu berücksichtigen, in dem je ein von den Landtagsfraktionen vorgeschlagenes Mitglied sowie je ein weiteres Mitglied der Organisationen der jüdischen Gemeinden und der Sinti und Roma vertreten sind. Die Mitglieder der Beirats sind ehrenamtlich tätig. Datenschutzrechtlich war insbesondere die Beteiligung des Beirats von Bedeutung.

Der LfD hat dies wie folgt beurteilt:

Die Vergabe von öffentlichen Mitteln aus sozialen Gründen ist eine öffentliche Aufgabe, die der Staat mit seinen öffentlichen Stellen zu erfüllen hat. Private oder andere externe Stellen dürfen nur dann in die Aufgabenerfüllung einbezogen werden, wenn dies auch vor dem Hintergrund der verfassungsrechtlichen Kompetenzordnung zulässig ist.

Im vorliegenden Fall war es nach Ansicht des LfD schon zweifelhaft, ob nicht die Gewährung der Leistungen durch das Amt für Wiedergutmachung unter Beteiligung des Ministeriums der Finanzen einer gesetzlichen Grundlage bedürfte. Auch wenn man davon ausgeht, daß die Bereitstellung von Mitteln im Haushaltsplan als ausreichende gesetzliche Grundlage für die Gewährung dieser Leistungen anzusehen ist, so liegt es jedenfalls nicht im Belieben der Exekutive, an der Entscheidungsfindung Externe zu beteiligen. Es ist der Verwaltung sicher unbenommen, sich in schwierigen Fällen auch privaten Sachverstandes durch die Beiziehung von Gutachtern und Sachverständigen zu bedienen, um ihre Entscheidungen auf ein tragfähiges Fundament zu stützen. Soweit aber in diesem Zusammenhang ohne Einwilligung und Kenntnis der Betroffenen personenbezogene Daten übermittelt werden, ist dies nur auf einer gesetzlichen Grundlage zulässig.

§ 16 LDSG bietet für die hier in Rede stehende Datenübermittlung keine Grundlage. Dabei kann dahinstehen, ob der Beirat als öffentliche oder private Stelle anzusehen ist. Wenn eine Datenübermittlung an eine private Stelle zulässig wäre, dann wäre sie sicher erst recht an eine öffentliche Stelle erlaubt. § 16 Abs. 1 Nr. 3 LDSG greift allerdings nicht ein, da der Beirat kein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten hat. Ein rechtliches Interesse ist ein Interesse, das auf der Grundlage von Rechtsvorschriften mit gerichtlicher Hilfe durchgesetzt werden kann. Eine Rechtsvorschrift, die als Basis des Informationsverlangens des Beirats dienen könnte, existiert jedoch nicht. Die Richtlinien stellen eine solche Vorschrift nicht dar.

Selbst wenn man den Beirat als öffentliche Stelle im Sinne des § 14 LDSG ansehen würde, fehlt es an den dort geregelten Übermittlungsvoraussetzungen. Diese knüpfen nämlich daran an, daß die empfangende Stelle eine gesetzlich zugewiesene Zuständigkeit besitzt. Daran fehlt es aber hier.

Auch die Einwilligung hat der LfD nicht für eine angemessene Lösung gehalten: Staatliche Leistungen dürfen nicht von der Einwilligung in Rechtseingriffe abhängig gemacht werden, die unverhältnismäßig in die Rechte der Betroffenen eingreifen. Angesichts der Beteiligung Privater an dem Beirat, dessen Mitglieder kein öffentliches Ehrenamt ausüben und die dementsprechend keiner gesetzlichen Geheimhaltungspflicht unterliegen, ist dies zumindest zweifelhaft.

Das Ministerium der Finanzen hat daraufhin erklärt, an den Beirat keine personenbezogenen Daten zu übermitteln. Die Fälle, für die er ein Votum abgeben soll, sollen vielmehr anonym vorgetragen werden.

23.6 Wahlgeheimnis

Vor Wahlen erreichen den LfD regelmäßig viele Zuschriften, in denen die Besorgnis geäußert wird, das Wahlgeheimnis bei der Briefwahl sei nicht gewahrt, weil der Stimmzettel in einen unverschlossenen, d. h. nicht zugeklebten Wahlumschlag zu stecken ist. Bei der Landtagswahl im Jahre 1996 war dieses Verfahren aufgrund einer Änderung von § 55 der Landeswahlordnung erstmals anzuwenden.

Diese Änderung der Landeswahlordnung wurde erforderlich, weil bei der Landtagswahl 1996 nach dem Willen des Gesetzgebers erstmals jedes Gemeindeergebnis einschließlich dem Ergebnis der Briefwahl ermittelt und ausgewiesen werden mußte. Dies hatte zur Folge, daß in Gemeinden mit einer nur geringen Zahl von Briefwahlberechtigten, in denen zur Ermittlung des Briefwahlergebnisses wegen der Gefährdung des Wahlgeheimnisses kein besonderer Briefwahlvorstand eingesetzt werden konnte, die brieflich abgegebenen Stimmen vom allgemeinen Wahlvorstand mit den Stimmen der Urnenwähler ausgezählt werden mußten. Wären die Briefwahlumschläge in diesen Fällen zugeklebt gewesen, so hätten sie sich von den Wahlumschlägen der Urnenwähler unterschieden und möglicherweise Rückschlüsse auf die Wahlentscheidung bestimmter Briefwähler zugelassen.

Gegen eine Änderung des Verfahrens in der Weise, daß alle Wahlumschläge verschlossen werden, spricht, daß das Öffnen verschlossener Umschläge vor der Stimmenauszählung zu Verzögerungen führt und mit zusätzlicher Arbeit verbunden ist. Ferner bietet das Verschließen von Stimmzetteln Möglichkeiten einer Kennzeichnung der Stimmabgabe, und außerdem ist eine Beschädigung von Stimmzetteln beim Öffnen der Wahlumschläge nicht auszuschließen.

Die durch das Landeswahlgesetz und die Landeswahlordnung vorgeschriebene Behandlung der Wahlbriefe durch den Wahlvorstand steht einer Verletzung des Wahlgeheimnisses entgegen. Die Wahlbriefumschläge bleiben bis zum Wahltag ungeöffnet in Verwahrung der Verbandsgemeinde- und Stadtverwaltungen. Sie werden erst am Wahltag den zuständigen Wahlvorständen übergeben. Alle weiteren Phasen der Behandlung der Wahlbriefe – Öffnen, Prüfung der Wahlberechtigung anhand des Wahlscheins und Einwerfen des Wahlumschlags in die Wahlurne – werden von den Mitgliedern des Wahlvorstandes unter gegenseitiger Kontrolle gemeinsam vorgenommen. Eine Verletzung des Wahlgeheimnisses durch Herausnahme des Stimmzettels aus dem unverschlossenen Wahlumschlag vor dem Einwerfen in die Wahlurne wäre nur dann möglich, wenn die Mitglieder des Wahlvorstandes gemeinsam und einvernehmlich diese strafbare Handlung begehen würden. Es ist zu berücksichtigen, daß nach den gesetzlichen Bestimmungen während der Wahl mindestens vier und bei der Stimmenauszählung alle Mitglieder des Wahlvorstandes anwesend sind.

Das OVG Rheinland-Pfalz hat in seinem Urteil vom 16. Juni 1985, Az.: 7 A 135/84, für die Kommunalwahl bestätigt, daß bei diesem Verfahrensablauf der Briefwahl mit unverschlossenen Wahlumschlägen der Grundsatz der geheimen Wahl nicht verletzt ist.

23.7 Inhalt von Abmarkungsbenachrichtigungen

Grundstückseigentümer beklagten in einer Eingabe an den LfD, daß den von einer Abmarkung Betroffenen die Abmarkungsbenachrichtigung und als Anlagen hierzu Auszüge aus Abmarkungsniederschriften übermittelt wurden, die sowohl die Namen und Anschriften der Eigentümer wie auch deren Geburtsdatum enthielten. Das Ministerium des Innern und für Sport teilte hierzu mit, daß in Verbindung mit einer Abmarkungsbenachrichtigung nur eine sehr eingeschränkte Übermittlung personenbezogener Daten notwendig und üblich sei. In der Abmarkungsniederschrift könne dagegen auf genauere Eigentümerangaben nicht verzichtet werden. Das von den Grundstückseigentümern gerügte Verfahren sei nicht üblich; es sei jedoch auch nicht auszuschließen, daß es aus Wirtschaftlichkeitsgründen auch von anderen Vermessungsstellen angewandt werde. Der konkrete Vorgang gebe deshalb Anlaß, die Regelungen zur Abmarkungsbenachrichtigung bei der aktuellen Fortschreibung der Richtlinien für die Katastervermessung um den Hinweis zu ergänzen, daß personenbezogene Daten nur im unbedingt notwendigen Umfang in die Abmarkungsbenachrichtigung aufgenommen werden. Schon früher wies das Ministerium darauf hin, daß in der Abmarkungsniederschrift auf die Angabe der Adresse und des Geburtsdatums verzichtet werden könne.

23.8 Weitergabe von Daten aus dem Waffenregister

Eine Kreisverwaltung als Waffenerlaubnisbehörde erbat eine Stellungnahme zu der Frage, ob es zulässig ist, einem Gläubiger auf Anfrage und zum Zwecke der Beurteilung, ob verwertbares Vermögen vorhanden ist, Auskünfte darüber zu erteilen, ob für den Schuldner eine Waffenbesitzkarte geführt wird und welche Waffen eingetragen sind.

Das Waffenrecht ist Teil des Ordnungsrechts. Da das Waffengesetz keine einschlägigen Datenübermittlungsregelungen enthält, sind ergänzend die Vorschriften des POG über die Informationsverarbeitung durch die allgemeinen Ordnungsbehörden anzuwenden. Nach § 25 a Abs. 1 Nr. 3 i. V. m. § 1 Abs. 3 POG ist die Übermittlung personenbezogener Daten zum Schutz privater Rechte zulässig, wenn gerichtlicher Schutz nicht rechtzeitig zu erlangen ist und wenn ohne ordnungsbehördliche oder polizeiliche Hilfe die Verwirklichung des Rechts vereitelt oder wesentlich erschwert würde.

Diese Voraussetzung lag nicht vor. Nach dem Sachverhaltsvortrag deutete nichts darauf hin, daß gerichtlicher Schutz ohne ordnungsbehördliche Hilfe nicht rechtzeitig hätte erlangt werden können. Eine Datenübermittlung war danach nicht zulässig.

24. Schlußbemerkung

24.1 Zur Situation der Geschäftsstelle

Die räumliche und sachliche Ausstattung der Geschäftsstelle ist zufriedenstellend.

Für die derzeit erforderliche Ersetzung des DV-Systems der Geschäftsstelle (wegen Totalausfalles des ca. sieben Jahre in Betrieb befindlichen alten Systems) sind im Haushalt die erforderlichen Mittel ausgewiesen.

Aufgrund der Umwandlung der bislang nicht besetzten Abordnungsstelle des höheren Dienstes in eine Planstelle konnte nunmehr eine Besetzung dieser Stelle mit einer Mitarbeiterin des höheren Dienstes erfolgen. Durch die Reduzierung der Arbeitszeit eines Referenten auf 75 Prozent bleibt im Ergebnis allerdings nur ein Personalzuwachs von einer Dreiviertelstelle.

Der LfD ist damit nach wie vor auf eine der (im Ländervergleich) kleinsten Geschäftsstellen zur Unterstützung angewiesen. Insbesondere in bezug auf die Personalausstattung im Bereich des technischen Datenschutzes hält er eine Verstärkung des Personals mittelfristig für unabdingbar. Angesichts der derzeitigen Haushaltslage ist er sich aber der geringen Realisierungschancen dieses Anliegens bewußt.

Die Unterstützung durch den Landtag bei der Wahrnehmung der Verwaltungsaufgaben des Landesbeauftragten für den Datenschutz hat sich auch im Berichtszeitraum bewährt. Dadurch konnten die vorhandenen Personalressourcen optimal für die Erfüllung seiner sachlichen Aufgaben eingesetzt werden.

24.2 Veröffentlichungen der Dienststelle

Der LfD gibt nach wie vor seine „Schriftenreihe mit Informationen zum Datenschutz" heraus. Heft 1 mit den Vorschriften zum Datenschutz wurde im Berichtszeitraum neu aufgelegt. Durch eine formale Neugestaltung dieses Heftes (Gliederung in Teile, die jeweils gesondert erneuert werden können) wird eine kontinuierliche Aktualisierung ermöglicht.

Die bereits erschienenen Hefte dieser Schriftenreihe werden nach Arbeitslage und Bedarf überarbeitet. In überarbeiteter Form liegt nunmehr Heft 3, Datenschutz im Bereich der wissenschaftlichen Forschung, vor.

Für die Erstellung der nach § 9 Abs. 5 LDSG zu fertigenden Dienstanweisung zum technisch-organisatorischen Datenschutz hat der LfD Regelungsbeispiele veröffentlicht.

Weiterhin hat er die für den behördlichen Datenschutz wesentlichsten Informationen (Text des LDSG, des BDSG, des aktuellen Datenschutzberichts, der Anmeldungsformulare zum Datenschutzregister sowie der Regelungsbeispiele für eine Dienstanweisung zum Datenschutz) auf einer Diskette veröffentlicht, die die Übernahme dieser Texte in die EDV jeder Behörde ermöglicht.

Der LfD beabsichtigt, den Umfang dieser Informationen durch Herausgabe einer entsprechenden CD-ROM zu erweitern und damit der Praxis die Erfüllung der datenschutzrechtlichen Anforderungen weiter zu erleichtern.

24.3 Zusammenarbeit mit anderen Datenschutzinstitutionen

Im Berichtszeitraum hat ein Treffen mit den Datenschutzreferenten und -sachbearbeitern des Innenministeriums und der Bezirksregierungen stattgefunden. Dabei wurde eine Reihe von Fragen gemeinsamen Interesses angesprochen. Die Abstimmungen mit den Bezirksregierungen und der obersten Datenschutzaufsichtsbehörde für den privaten Bereich, dem Ministerium des Innern und für Sport, sind ohne Reibungen vertrauensvoll erfolgt.

Der Meinungsaustausch mit dem Datenschutzbeauftragten des ZDF fand auch im Berichtszeitraum aus Anlaß der Herausgabe des Berichts des Datenschutzbeauftragten des ZDF statt. Auch hier wurde weitgehend Übereinstimmung in der datenschutzrechtlichen Bewertung von Fragen statuiert, die von gemeinsamem Interesse sind.

Die Abstimmung mit den Datenschutzbeauftragten der anderen Länder und dem des Bundes erfolgte in Arbeitskreisen und jährlich jeweils zwei Gesamtkonferenzen. Die Ergebnisse dieser Abstimmungsarbeit kommen in den Entschließungen, die als Anlage abgedruckt sind, zum Ausdruck. Die Zusammenarbeit war nicht selten aufwendig und schwierig, sie verlief angesichts des gemeinsamen Engagements für die Sache und der grundsätzlich bei allen vorhandenen Kompromißbereitschaft jedoch in angenehmer Arbeitsatmosphäre, und sie war erfreulich erfolgreich.

Die Kommission beim Landesbeauftragten für den Datenschutz hat auch im Berichtszeitraum durch regelmäßige Sitzungen ihre gesetzliche Aufgabe, den LfD bei der Wahrnehmung seiner Aufgaben zu unterstützen und den Tätigkeitsbericht vorzuberaten, in engagierter Weise wahrgenommen. Die hierdurch mögliche Rückkopplung an die Tätigkeit des Landtags ist auf diese Weise institutionalisiert worden. Der LfD möchte diese Gelegenheit benutzen, sich bei den Mitgliedern der Kommission für ihre Arbeit nachdrücklich zu bedanken.

24.4 Resümee und Ausblick

Fast ein Vierteljahrhundert nach dem Inkrafttreten des ersten Datenschutzgesetzes in Rheinland-Pfalz ist der Datenschutz in diesem Lande akzeptiert. Vorbehalte, die dem Datenschutz und der Kontrollinstanz anfangs entgegengebracht wurden, konnten weitgehend abgebaut werden. Absichtliche Verstöße gegen datenschutzrechtliche Bestimmungen sind selten. Zu dieser Entwicklung hat die mit Augenmaß betriebene Beratungs- und Kontrolltätigkeit des Personals der Behörde des LfD wesentlich beigetragen. Hierfür gebührt den Mitarbeiterinnen und Mitarbeitern, die auch in schwierigen Situationen mit fachlicher Kompetenz und Umsicht ihre Aufgaben erfüllt haben, Dank und Anerkennung.

Als Resümee und Ausblick zugleich ist darauf hinzuweisen, daß die allgemeinen gesellschaftlichen und wirtschaftlichen Entwicklungen dieses Jahrzehnts auch den Datenschutz wesentlich beeinflussen. Ihre Ursachen beruhen zu einem erheblichen Teil auf globalen Veränderungen, ihre Auswirkungen sind oftmals schmerzhaft. Stichworte sind: Verschärfung des internationalen Wettbewerbs, Arbeitslosigkeit, steigende Sozialausgaben, rückläufige Steuereinnahmen, Zunahme der Kriminalität. Wer wollte leugnen, daß diese Entwicklungen auch für den Datenschutz Bedeutung haben. Unter diesen Bedingungen muß der Staat die informationstechnischen Voraussetzungen schaffen, die unsere Wirtschaft befähigen, im globalen Wettbewerb zu bestehen, er muß den unberechtigten Bezug von Sozialleistungen eindämmen, Steuerhinterziehungen nachgehen und Verbrechen bekämpfen und aufklären. Dies alles setzt voraus, daß in einem Maße, das im vergangenen Jahrzehnt noch unvorstellbar erschienen wäre, Daten erhoben, gespeichert und übermittelt werden. Vor diesem Hintergrund bleibt die dem Schutz des Persönlichkeitsrechts gewidmete Tätigkeit des Datenschutzbeauftragten eine wichtige Aufgabe.

Anlage 1

Entschließung der Datenschutzbeauftragten des Bundes und der Länder zum Datenschutz bei elektronischen Geldbörsen und anderen kartengestützten Zahlungssystemen vom 13. Oktober 1995 (vorab im Umlaufverfahren ergangen)

Die Datenschutzbeauftragten des Bundes und der Länder halten es für dringend erforderlich, daß bei kartengestützten Zahlungssystemen, die zunehmend in Konkurrenz zum Bargeld treten, datenschutzfreundliche Verfahren eingesetzt werden. Dabei bietet es sich an, vor allem Guthabenkarten zu verwenden. Es sollten nur solche Clearingverfahren eingesetzt werden, die weder eine individuelle Kartennummer benutzen noch einen anderen Bezug zum Karteninhaber herstellen.

Sowohl im öffentlichen Personennahverkehr als auch bei der Deutschen Bahn AG können Fahrscheine bargeldlos erworben werden. Auch Autofahrer können auf Bargeld verzichten: Beim Parken, beim Tanken, künftig auch bei der Benutzung von Autobahnen wird verstärkt auf elektronisches Bezahlen zurückgegriffen. Immer mehr Telefone und Warenautomaten werden auf bargeldlose Zahlungsverfahren umgestellt, so daß viele Artikel des täglichen Bedarfs elektronisch bezahlt werden können. Von Kreditinstituten wird die Kombination verschiedener Anwendungen auf einer Karte angestrebt, z. B. mit einer Kombination der Bezahlung für den öffentlichen Nahverkehr, Parkgebühren und Benutzungsentgelte für öffentliche Einrichtungen.

Zum elektronischen Bezahlen werden entweder Kreditkarten, Debitkarten oder Guthabenkarten eingesetzt. Bei Kredit- und Debitkarten werden sämtliche Zahlungsbeträge verbucht, dem Käufer in Rechnung gestellt, auf den Kontoauszügen ausgedruckt und für mindestens sechs Jahre gespeichert. Dagegen wird bei Guthabenkarten im voraus ein Guthaben eingezahlt und bei jeder einzelnen Zahlung das Guthaben entsprechend herabgesetzt; die Zahlungsbeträge müssen keinem Käufer zugeordnet werden.

Beim elektronischen Bezahlen entstehen sehr unterschiedliche Datenschutzrisiken. Bei Kredit- und Debitkarten besteht die Gefahr, daß die aus Abrechnungsgründen gespeicherten personenbezogenen Daten ausgewertet und zweckentfremdet genutzt werden:

Informationen über den Kauf von Fahrscheinen oder über die Nutzung von Autobahnen können zu Bewegungsprofilen verdichtet werden. Das Konsumverhalten des einzelnen wird bis ins Detail nachvollziehbar, falls auch Kleineinkäufe am Kiosk nachträglich abgerechnet werden. Durch den Datenverkauf für Werbung und Marketing können sich weitere Risiken ergeben. Demgegenüber kann bei der Verwendung von Guthabenkarten auf das Speichern personen- oder kartenbezogener Daten aus erfolgten Zahlungen verzichtet werden.

Vor allem im Kleingeldbereich ist die Nutzung von Debit- und Kreditkarten entbehrlich, da fälschungssichere Guthabenkarten auf der Basis von Chipkarten mit integriertem Verschlüsselungsbaustein zur Verfügung stehen. Falls größere Geldbeträge nachträglich per Kredit- oder Debitkarte bezahlt werden, ist darauf zu achten, daß die Abrechnung zunächst über Konten erfolgt, deren Inhaber dem Zahlungsempfänger nicht namhaft gemacht wird. Erst bei Zahlungsunregelmäßigkeiten ist es notwendig, den Bezug zum Kontoinhaber herzustellen.

Angesichts der Risken, aber auch der von Chipkarten ausgehenden Chancen fordern die Datenschutzbeauftragten die Kartenherausgeber und die Kreditwirtschaft dazu auf, kartengestützte Zahlungssysteme zu entwickeln, die möglichst ohne personenbezogene Daten auskommen, und deren Anwendung so zu gestalten, daß ein karten- und damit personenbezogenes Clearing nicht erfolgt. Der Gesetzgeber muß sicherstellen, daß auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher anonym zu bleiben.

Anlage 2

Entschließung
der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995 zur Weiterentwicklung des Datenschutzes in der Europäischen Union

Die Konferenz der Datenschutzbeauftragten der Europäischen Union hat am 8. September 1995 in Kopenhagen in einer Resolution im Hinblick auf die für 1996 geplante Regierungskonferenz dafür plädiert, anläßlich der Überarbeitung der Unions- und Gemeinschaftsverträge in einen verbindlichen Grundrechtskatalog ein einklagbares europäisches Grundrecht auf Datenschutz aufzunehmen. Die Schaffung rechtsverbindlicher Datenschutzregelungen für die Organe und Einrichtungen der Union sowie die Schaffung einer unabhängigen und effektiven Datenschutzkontrollinstanz der EU werden angemahnt. Dieser Resolution schließt sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an. Sie hält angesichts der fortschreitenden Integration und des zunehmenden Einsatzes von Informations- und Kommunikationstechnologien in der EU eine Weiterentwicklung des Datenschutzes im Rahmen der EU für geboten.

Sie fordert die zuständigen Politiker und insbesondere die Bundesregierung auf, dafür einzutreten, daß im EU-Vertragsrecht ein Grundrecht auf Datenschutz aufgenommen wird, die materiellen Datenschutzregelungen in der EU verbessert werden, das Amt eines Europäischen Datenschutzbeauftragten geschaffen wird sowie eine parlamentarische und richterliche Kontrolle der Datenverarbeitung der im EU-Vertrag vorgesehenen Instanzen sichergestellt wird.

Grundrecht auf Datenschutz

Bei einer Weiterentwicklung der Europäischen Union ist es unabdingbar, daß dem Grundrechtsschutz eine angemessene Bedeutung beigemessen wird. Dies sollte dadurch geschehen, daß die Verträge zur Europäischen Union mit einem Grundrechtskatalog ergänzt werden. Mit einer Entschließung vom 10. Februar 1994 hat das Europäische Parlament einen Entwurf zur Verfassung der Europäischen Union zur Erörterung gestellt, der u. a. folgende Aussagen enthält: „Jeder hat das Recht auf Achtung und Schutz seiner Identität. Die Achtung der Privatsphäre und des Familienlebens, des Ansehens (. . .) wird gewährleistet".

Die Konferenz der Datenschutzbeauftragten ist mit ihrer Entschließung vom 28. April 1992 dafür eingetreten, daß in das Grundgesetz nach dem Vorbild anderer europäischer Verfassungen ein Grundrecht auf Datenschutz aufgenommen wird. Sie hat hierfür einen Formulierungsvorschlag gemacht. Auf ihren Konferenzen am 16./17. Februar 1993 und 9./10. März 1994 bekräftigten die Datenschutzbeauftragten des Bundes und der Länder ihre Position. Diese Forderung wurde aber wegen des Nichterreichens der notwendigen qualifizierten Mehrheit durch den Gesetzgeber nicht umgesetzt.

In Wirtschaft, Verwaltung und Gesellschaft der Staaten der EU erhält der Dienstleistungs- und Informationssektor eine zunehmende Bedeutung. Dies hat zur Folge, daß mit hochentwickelten Informationstechnologien von privaten wie von öffentlichen Stellen verstärkt personenbezogene Daten verarbeitet und auch grenzüberschreitend ausgetauscht werden. Diese Entwicklung wird gefördert durch die Privatisierung und den rasanten Ausbau transeuropäischer elektronischer Telekommunikationsnetze. Dadurch gerät das Grundrecht auf informationelle Selbstbestimmung in besonderem Maße auf der überstaatlichen Ebene in Gefahr. Dieser Gefahr kann dadurch entgegengetreten werden, daß in einen in den überarbeiteten EU-Vertrag aufzunehmenden Grundrechtskatalog das Grundrecht auf Datenschutz und zu dessen Konkretisierung ein Recht auf unbeobachtete Telekommunikation aufgenommen werden. Dies hätte folgende positive Auswirkungen:

Anhand einer ausdrücklichen gemeinsamen Rechtsnorm kann sich eine einheitliche Rechtsprechung zum Datenschutz entwickeln, an die sowohl die EU-Organe wie auch die nationalen Stellen gebunden werden. Ein solches Grundrecht wäre die Basis für eine Vereinheitlichung des derzeit noch sehr unterschiedlichen nationalen Datenschutzrechts auf einem hohen Niveau. Den Bürgerinnen und Bürgern wird deutlich erkennbar, daß ihnen in einklagbarer Form der Datenschutz in gleicher Weise garantiert wird wie die traditionellen Grundrechte. Das grundlegende rechtsstaatliche Prinzip des Datenschutzes wird dauerhaft, auch bei Erweiterung der EU, gesichert.
Mit der rechtlichen Konkretisierung eines Rechts auf unbeobachtete Telekommunikation würde der zunehmenden Registrierung des Verhaltens der Bürgerinnen und Bürger in der multimedialen Informationsgesellschaft entgegengewirkt und der Schutz des Fernmeldegeheimnisses auch nach dem Abbau der staatlichen Monopole im Sprachtelefondienst sichergestellt.

Materielle Datenschutzregelungen

Mit der kürzlich verabschiedeten EU-Datenschutzrichtlinie wird ein großer Fortschritt für den Datenschutz auf europäischer Ebene erreicht. Dies darf aber nicht den Blick dafür verstellen, daß in einzelnen Bereichen spezifische, dringend nötige Datenschutzregelungen fehlen. Insbesondere sind folgende Bereiche regelungsbedürftig:

Es bedarf eines für die EU-Institutionen verbindlichen eigenen Datenschutzrechts. Die datenschutzrechtliche Verantwortung der Mitgliedstaaten einschließlich ihrer Datenschutzkontrolle der Übermittlung von Daten an EU-Institutionen bleibt dabei unberührt.
Die geplante ISDN-Datenschutzrichtlinie darf weder einer völlig falsch verstandenen Subsidiarität zum Opfer fallen noch in unzureichender Form verabschiedet werden.
Die im Bereich der Statistik bestehenden datenschutzrechtlichen Defizite sind abzubauen.
Es soll eine Technikfolgenabschätzung bei der Förderung und Einführung neuer Informationstechniken mit Personenbezug durch die EU obligatorisch eingeführt werden.
In den Bereichen Inneres und Justiz sind aufeinander abgestimmte verbindliche Regelungen mit hohem Datenschutzstandard, die die Datenverarbeitung in Akten und die Sicherung der Datenschutzkontrolle mit umfassen, zu schaffen.
Es bedarf der Harmonisierung des Arbeitnehmerdatenschutzes auf hohem Niveau in den Staaten der EU. Für das Personal der EU-Organe ist der Arbeitnehmerdatenschutz sicherzustellen, was z. B. bei der Durchführung von Sicherheitsüberprüfungen insbesondere unter Beteiligung von Behörden der Heimatstaaten von großer Bedeutung ist. Es ist zu prüfen, inwieweit Informationszugangsrechte in weiteren Bereichen eingeführt werden sollen.

Europäischer Datenschutzbeauftragter

Die Konferenz der EU-Datenschutzkontrollinstanzen (25./26. Mai 1994, 8. September 1995) und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (25. August 1994) haben darauf hingewiesen, daß es an einer unabhängigen und effektiven Datenschutzkontrollinstanz fehlt, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der EU in seinen Rechten verletzt zu sein. Aufgabe eines Europäischen Datenschutzbeauftragten sollte die Behandlung aller Datenschutzbelange der EU sein. Dazu gehört nicht nur die Bearbeitung von Betroffeneneingaben, sondern auch die datenschutzrechtliche Beratung der EU-Organe und -Einrichtungen sowie deren anlaßunabhängige Kontrolle, die Begleitung informationstechnischer EU-Projekte und der entsprechenden EU-Normsetzung sowie die Zusammenarbeit mit den nationalen Kontrollinstanzen. Wegen der teilweise anders gelagerten Aufgaben sollen die Funktionen des Europäischen Datenschutzbeauftragten und des Bürgerbeauftragten nach den EG-Verträgen nicht vermengt werden. Die Bundesregierung sollte im Rahmen der Vorbereitung der Regierungskonferenz 1996 darauf hinwirken, daß ein unabhängiger Europäischer Datenschutzbeauftragter in den Verträgen über die Europäische Union institutionell abgesichert wird.

Parlamentarische und richterliche Kontrolle

Bei der Zusammenarbeit der EU-Staaten in den Bereichen Justiz und Inneres muß mit Besorgnis festgestellt werden, daß eine ausreichende parlamentarische und richterliche Kontrolle im EUV derzeit nicht gewährleistet ist. Die geplante Europol-Konvention ist hierfür ein Beispiel. Mit unbestimmten Formulierungen werden einem fast völlig freischwebenden Europäischen Polizeiamt informationelle Befugnisse eingeräumt, einem Amt, das keiner parlamentarischen Verantwortlichkeit und nur einer unzureichenden (teils nur nationalen) Rechtskontrolle unterworfen wird. Zur Wahrung des Datenschutzes bei der Umsetzung gemeinsamer Maßnahmen in den Bereichen Justiz und Inneres muß daher – unbeschadet der Kontrolle durch die nationalen Datenschutzbehörden – auch eine im Rahmen ihrer jeweiligen Zuständigkeiten lückenlose Kontrolle durch die nationalen Parlamente und Gerichte sowie durch das Europäische Parlament und den Europäischen Gerichtshof sichergestellt werden.

Anlage 3

Entschließung
der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995 zum Datenschutz bei der Neuordnung der Telekommunikation (Postreform III)

Mit der Postreform III soll die Neugestaltung des Telekommunikationssektors in Deutschland nach den Vorgaben des Liberalisierungskonzepts der Europäischen Union abgeschlossen werden. Entstehen wird ein riesiger Markt mit einer Vielzahl von großen und kleinen, teilweise auch grenzüberschreitend tätigen Netzbetreibern und Diensteanbietern. Die Akteure auf diesem Telekommunikationsmarkt werden zum größeren Teil als Privatunternehmen operieren, es werden aber auch öffentliche Stellen ihre Leistungen anbieten. Der gesetzgeberische Abschluß der Liberalisierung und der Privatisierung des TK-Sektors wird die rechtliche Grundlage bilden für den endgültigen Eintritt in das Zeitalter von weltweiter Vernetzung, Multimedia und interaktiven Diensten und damit für den rapiden Anstieg des Konsums von Angeboten der Telekommunikation, des interaktiven Rundfunks und der Datenverarbeitung.

Die Konsequenzen sind absehbar: Gegenüber der heutigen Situation werden unvergleichlich mehr personenbezogene Daten durch mehr Stellen registriert und ausgewertet werden. Betroffen sind alle, die fernsehen, telefonieren, fernkopieren, Texte und Dokumente über Datenleitung schicken oder Telebanking oder Teleshopping betreiben. Die Risiken für den einzelnen durch die vermehrten Möglichkeiten der Verhaltens- und Umfeldkontrolle oder der Ausforschung persönlicher Lebensgewohnheiten und Eigenschaften vergrößern sich entsprechend.

Der vom Bundesministerium für Post und Telekommunikation vorgelegte Referentenentwurf für ein Telekommunikationsgesetz (TKG-E, Stand: 6. Oktober 1995) macht es erforderlich, erneut die Realisierung der grundlegenden Rahmenbedingungen für eine datenschutzgerechte Gestaltung der künftigen Telekommunikationslandschaft – soweit die Gesetzgebungskompetenz des Bundes betroffen ist – anzumahnen.

Ein wirksamer Datenschutz muß – wie bereits jetzt gesetzlich fixiert – auch künftig gleichberechtigtes Regulierungsziel neben z. B. der Sicherstellung der flächendeckenden Grundversorgung mit Telekommunikationsdienstleistungen bleiben.

Kundenwünsche nach variablerer und komfortablerer Nutzung der technischen Möglichkeiten werden zunehmen. Gerade deshalb müssen die Prinzipien der Datenvermeidung und der strikten Begrenzung der Datenverarbeitung auf das erforderliche Ausmaß ihren Vorrang bei der Ausgestaltung der kommunikationstechnischen Infrastruktur behalten. Netzbetreiber und Diensteanbieter sollten verpflichtet werden, überall dort, wo dies technisch möglich ist, auch anonyme Zugangs- und Nutzungsformen für ihre Leistungen bereitzustellen. Für eine sichere Datenübertragung sind ohne prohibitive Zusatzkosten wirksame Verschlüsselungsverfahren bereitzustellen.

Das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis müssen für alle Netzbetreiber und Diensteanbieter ungeachtet ihrer Rechtsform und ihrer Kundenstruktur (z. B. sog. Corporate Networks) einheitlich auf einem hohen Niveau gesichert werden. Der bisherige Schutzstandard darf keinesfalls unter den durch die Postreform II erreichten Stand gesenkt werden. Ein hohes Datenschutzniveau ist als Grundversorgung unabdingbar; seine Gewährleistung sollte deshalb Teil der Universaldienstleistung sein. Die in Grundrechte eingreifenden Regelungen sind im Telekommunikationsgesetz selbst und nicht in Verordnungen zu treffen. Die untergesetzlichen, den Datenschutz betreffenden Normen gehören in eine einzige, nicht verstreut in mehrere Verordnungen.

Entscheidend für die Wirksamkeit des Grundrechtsschutzes ist die strikte Einhaltung der Zweckbindung der Verbindungs- und Abrechnungsdaten. Das „Feststellen mißbräuchlicher Inanspruchnahme" oder die „bedarfsgerechte Gestaltung" von TK-Leistungen dürfen nicht als Anlaß für eine umfassende Auswertung dieser Angaben oder sogar der Nachrichteninhalte herangezogen werden.

Für den Kunden bzw. Teilnehmer ist es von größter Bedeutung, die Verarbeitungsvorgänge im TK-Bereich überschauen zu können. Er muß auch künftig über die Nutzungsrisiken bestimmter Kommunikationstechniken (z. B. Mobilfunk) ebenso wie über seine Widerspruchsmöglichkeiten umfassend aufgeklärt werden. Keinesfalls darf die Einwilligung des Betroffenen mißbraucht werden, um bereichsspezifische Schutznormen oder effiziente Datensicherungsvorkehrungen zu umgehen.

Um auch und gerade für das besonders schutzwürdige Fernmeldegeheimnis einen durchgängig hohen Schutzstandard zu sichern, braucht es eine unabhängige Kontrolle nach bundesweit einheitlichen Kriterien. Die Zuweisung dieser Überwachungsaufgabe an die im TKG-Entwurf vorgesehene Regulierungsbehörde ist wegen deren mangelhafter Unabhängigkeit und der von ihr wahrzunehmenden Regulierungsaufgaben, die mit Interessenkonflikten verbunden sein werden, nicht akzeptabel.

Deshalb sollte aufgrund seiner langjährigen fachlichen Erfahrung bei der Kontrolle der Telekom und seiner umfassenden Querschnittskenntnisse im TK-Bereich der Bundesbeauftragte für den Datenschutz eine zentrale Funktion für die Kontrolle im Telekommunikationsbereich erhalten. Die Aufgaben, die die Landesbeauftragten für den Datenschutz und die Aufsichtsbehörden im Rahmen ihrer Zuständigkeiten erfüllen, sind gesetzlich klar zu regeln.

Die Akzeptanz der Informationsgesellschaft der Zukunft hängt wesentlich ab von der Sicherung des Grundrechts auf unbeobachtete Kommunikation. Das Telekommunikationsgesetz wird einen entscheidenden Baustein für die rechtliche Ausgestaltung der künftigen TK-Infrastruktur bilden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher dazu auf, die von ihr vorgeschlagenen Regelungen im weiteren Gesetzgebungsverfahren zu berücksichtigen und sich für ihre Umsetzung auch auf der europäischen Ebene (z. B. in der ISDN-Richtlinie) einzusetzen.

Anlage 4

Entschließung
der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995 zu Planungen für ein Korruptionsbekämpfungsgesetz

Derzeit gibt es Vorschläge, die Bekämpfung der Korruption durch Verschärfungen des Strafrechts und des Strafprozeßrechts mit weiteren Eingriffen in das Grundrecht auf informationelle Selbstbestimmung zu organisieren. Ein Beispiel dafür ist der Beschluß des Bundesrates vom 3. November 1995 zur Einbringung eines Korruptionsbekämpfungsgesetzes.

Nach dem vom Bundesrat beschlossenen Gesetzentwurf sollen Bestechlichkeit und Bestechung in den Kreis derjenigen Tatbestände aufgenommen werden, bei deren Verdacht die Überwachung des Fernmeldeverkehrs und der Einsatz technischer Mittel ohne Wissen des Betroffenen (§§ 100 a, 100 c StPO) angeordnet werden dürfen.

Die Datenschutzbeauftragten weisen demgegenüber darauf hin, daß es vorrangig um Prävention, nicht um Repression geht. Die Datenschutzbeauftragten treten für eine entschlossene und wirksame Bekämpfung der Korruption mit rechtsstaatlichen Mitteln unter strikter Beachtung der Freiheitsrechte ein.

Sie wenden sich zugleich gegen eine Rechtspolitik, welche – noch bevor sie sich darüber im klaren ist, was die bisherigen Verschärfungen und Eingriffe an Vorteilen und an Nachteilen gebracht haben – auf weitere Verschärfungen und Eingriffe setzt.

Gerade gegenüber der Korruption gibt es Möglichkeiten, welche Effektivität versprechen und gleichwohl die Privatsphäre der unbeteiligten und unschuldigen Bürgerinnen und Bürger nicht antasten:

- Rotation derjenigen Mitarbeiterinnen und Mitarbeiter einer Behörde, deren Position und Aufgaben erfahrungsgemäß für Bestechungsversuche in Betracht kommen;
- Vier- und Sechsaugenprinzip bei bestimmten Entscheidungen;
- Trennung von Planung, Überwachung und Ausführung, von Ausschreibung und Vergabe;
- Prüfverfahren und Innenrevision;
- Codes of Conduct (formalisierte „Ethikprogramme") im Bereich der Wirtschaft;
- verbesserte Transparenz von Entscheidungsprozessen in der Verwaltung.

Die in den Gesetzentwürfen vorgesehene weitere Einschränkung von Grundrechten, die mit einer abermaligen Erweiterung der Telefonüberwachung verbunden wäre, ist nur vertretbar, wenn sie nach einer sorgfältigen Güter- und Risikoabwägung zusätzlich zu den o. g. Verfahrens- und Verhaltensmaßregeln als geeignet und unbedingt erforderlich anzusehen wäre.

Die Datenschutzbeauftragten verlangen, daß vor einer zusätzlichen Aufnahme von Straftatbeständen in den Katalog der Abhörvorschrift des § 100 a StPO diese Abwägung durchgeführt wird.

Die Datenschutzbeauftragten fordern weiterhin, daß eine Erweiterung des genannten Straftatenkataloges nur befristet vorgenommen wird, damit sich vor einer Verlängerung die Notwendigkeit stellt, auf der Grundlage einer sorgfältigen Erfolgs- und Effektivitätskontrolle erneut die Erforderlichkeit und Verhältnismäßigkeit einer solchen Erweiterung des Grundrechtseingriffs zu überprüfen.

Die Datenschutzbeauftragten verlangen, daß der Gesetzgeber vor weiteren Eingriffen in Freiheitsrechte eine sorgfältige Güter- und Risikoabwägung vornimmt und dabei insbesondere verantwortlich prüft, ob sich die innenpolitischen Ziele mit Mitteln erreichen lassen, welche die informationelle Selbstbestimmung der Bürgerinnen und Bürger schonen.

Schließlich gibt die anstehende erneute Erweiterung des Katalogs von § 100 a StPO Veranlassung, den Umfang der darin genannten Straftaten sobald wie möglich grundlegend zu überprüfen.

Anlage 5

Entschließung
der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995
Datenschutzrechtliche Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 47. Konferenz am 9./10. März 1994 kritisch zum Einsatz von Chipkarten im Gesundheitswesen Stellung genommen. In dem Beschluß wird die Nutzung von Patientenkarten von mehreren Voraussetzungen zur Sicherung des Persönlichkeitsrechts abhängig gemacht.

Seitdem werden in mehreren Ländern Modellversuche und Pilotprojekte durchgeführt. Die Bandbreite reicht von allgemeinen Patientenkarten, die an möglichst viele Patienten/Versicherte ausgegeben werden, eine Vielzahl von Krankheitsdaten enthalten und von einem unbestimmten Kreis von Personen und Institutionen des Gesundheitswesens zu vielfältigen Zwecken verwendet werden können (z. B. Vital-Card der AOK Leipzig, Persönliche Patientenkarte Neuwied, BKK-Patientenkarte Berlin) bis zu krankheitsspezifischen Karten für bestimmte Patientengruppen mit reduziertem Datensatz und einer Definition der Verwendung (z. B. Dialyse-Card, Diab-Card, Krebsnachsorgekarte, Defi-Card).

Datenschutzrechtlich stellen sich vor allem folgende Probleme:

Die massenhafte Einführung der Karten erzeugt einen sozialen Druck auf die Betroffenen, sie mitzuführen und vorzuzeigen. Diesen Erwartungen wird sich der Betroffene vielfach nur unter Befremden des Arztes oder sogar der Gefahr, daß dieser die Behandlung ablehnt, verweigern können.

Die Verwendung von allgemeinen Patientenkarten bringt die Gefahr einer pauschalen Offenbarung von medizinischen Daten mit sich.

Dem Patienten wird die Last aufgebürdet, für die Sicherheit seiner medizinischen Daten selbst zu sorgen.

Die Datenschutzbeauftragten fordern alle für Kartenprojekte im Gesundheitswesen Verantwortlichen in Politik, Industrie, Ärzteschaft, Wissenschaft und in den Krankenversicherungen auf, das Recht auf informationelle Selbstbestimmung der betroffenen Patienten bzw. Versicherten zu gewährleisten. Die 50. Konferenz hält folgende Voraussetzungen für elementar:

1. Besondere Schutzwürdigkeit medizinischer Daten

   Medizinische Daten sind besonders schutzwürdig, unabhängig davon, welche Technologien eingesetzt werden, ob die Patientendaten beim Arzt gespeichert und versandt oder über ein Netz abgerufen werden oder ob der Patient die Daten auf einer Chipkarte bei sich hat. Es handelt sich oftmals um belastende, schicksalhafte Daten. Zudem geht es nicht nur um Daten des Patienten, sondern auch um fremde Einblicke in die ärztliche Tätigkeit.

2. Wirksame Entscheidung der Betroffenen über die Verwendung einer Karte

   Die freie Entscheidung der Betroffenen (Patienten/Versicherten), eine Chipkarte zu verwenden, muß gewährleistet sein. Dies umfaßt die Entscheidung,
   - ob Daten auf einer Chipkarte gespeichert werden,
   - welche der Gesundheitsdaten auf die Karte aufgenommen werden,
   - welche Daten auf der Karte wieder gelöscht werden,
   - ob die Karte bei einem Arztbesuch bzw. einem Apothekenbesuch vorgelegt wird und
   - welche Daten im Einzelfall zugänglich gemacht werden.

   Ein Widerruf der Entscheidung muß ohne Nachteile für die Betroffenen möglich sein. Die gleiche Freiheit der Entscheidung für oder gegen die Verwendung der Chipkarte muß für Ärzte und Apotheker gewährleistet sein. Eine wirksame Entscheidung für oder gegen die Verwendung einer Chipkarte setzt eine schriftliche, objektive, vollständige und nachvollziehbare Information über Zweck, Art, Umfang und Beteiligte der Chipkarten-Kommunikation voraus. Das Gesamtkonzept des Chipkarteneinsatzes und der damit verbundenen Datenverarbeitung muß für die Betroffenen überschaubar sein.

   Auf der Karte darf nicht der Datensatz der Krankenversichertenkarte nach § 291 Abs. 2 SGB V, insbesondere nicht die Krankenversicherung und die Krankenversicherungsnummer, gespeichert werden, da andernfalls – zumal bei allgemeinen Patientenkarten mit hohem Verbreitungsgrad – die Krankenversichertenkarte verdrängt und deren Nutzungsbeschränkungen umgangen werden.

3. Freiheit der Entscheidung

Die uneingeschränkte Freiheit der Entscheidung der Betroffenen für oder gegen die Verwendung einer Chipkarte muß gewährleistet sein, denn der Einsatz von Chipkarten im Gesundheitswesen führt keineswegs zwangsläufig zu größerer Autonomie der Patienten. Neue Technologien können sich auch als Verführung erweisen, deren Preis erst langfristig erkennbar wird. Die individuelle Entscheidung des Bürgers über die Verarbeitung seiner Daten war und bleibt ein zentrales Recht gegenüber Eingriffen in seine Freiheitssphäre. Mit der Chipkarte können sich jedoch Situationen ergeben, in denen wirkliche Freiheit, tatsächliche Wahlmöglichkeit der Betroffenen nicht mehr gewährleistet sind und durch technische und organisatorische, rechtliche und soziale Rahmenbedingungen wiederhergestellt werden müssen.

Dem Staat kommt hier eine veränderte Rolle zu: Freiheitsrechte nicht einzuschränken, sondern sie zu sichern, wo Entwicklungen des Marktes und der Technologien sowie Gruppeninteressen die Entscheidungsfreiheit des Bürgers bedrohen. Die Technologie selbst kann für die Sicherung der Freiheitsrechte ein wertvolles Hilfsmittel sein. Darüber hinaus kommt der Informiertheit der Betroffenen ein zentraler Stellenwert zu. Ihre Kompetenz zur Entscheidung und zum praktischen Umgang mit der Karte muß gestärkt werden, damit sie auch langfristig die größtmöglichen Chancen haben, ihre Interessen durchzusetzen.

Mit der Ausstellung der Karte dürfen nur die Vorteile verknüpft werden, die sich unmittelbar aus den Nutzungspraktiken der Karte selbst ergeben. Die freie Entscheidung der Betroffenen, eine Karte zu nutzen oder dies abzulehnen, darf nicht durch einen Nutzungszwang oder eine Bevorzugung von Karten-Nutzern (z. B. durch Bonuspunkte) bzw. von Karten-Verweigerern eingeschränkt werden.

4. Keine Verschlechterung der Situation der Betroffenen

Durch die Einführung von Kommunikationssystemen mit Chipkarten dürfen die Betroffenen nicht schlechter gestellt werden als im konventionellen Verfahren. Die medizinische Versorgung, der Schutz der Gesundheitsdaten und die Mitentscheidungsrechte der Betroffenen müssen in Umfang und Qualität erhalten bleiben.

Das therapeutische Verhältnis Arzt/Patient darf sich durch den Einsatz von Chipkarten nicht verschlechtern. Freiheit und Vertrauen innerhalb des Arzt-Patienten-Verhältnisses sowie der Grundsatz der Abschottung der dem Arzt anvertrauten Informationen und der ärztlichen Erkenntnisse nach außen, gegen die Kenntnisnahme durch Dritte, müssen erhalten bleiben. Insbesondere muß der Gesetzgeber sicherstellen, daß die auf der beim Patienten befindlichen Chipkarte gespeicherten medizinischen Daten ebenso gegen Beschlagnahme und unbefugte Kenntnisnahme geschützt sind wie die beim Arzt gespeicherten Daten. Eine Kommunikation unter Vorlage der Karte mit Personen oder Stellen außerhalb des Arzt-Patienten-Verhältnisses, z. B. Arbeitgebern oder Versicherungen, muß vom Gesetzgeber untersagt werden.

Das sich im Gespräch entwickelnde Vertrauensverhältnis zwischen Arzt und Patient darf nicht durch eine chipkartenermittelte Kommunikation verdrängt werden. Verkürzte Darstellungen medizinischer Sachverhalte auf der Chipkarte – z. B. mit Hilfe von Schlüsselbegriffen – dürfen nicht zu einer Minderung der Qualität des therapeutischen Verhältnisses führen; das liegt auch im Interesse des Arztes. Der Patient muß auch weiterhin die Möglichkeit des individuellen Dialogs wählen können. Dies schließt insbesondere die Freiheit des Betroffenen ein, eine Chipkarte im Einzelfall nicht vorzulegen, auf der Chipkarte nur einen begrenzten Datensatz speichern zu lassen oder zu entscheiden, welchem Arzt welche Informationen oder Informationsbereiche offenbart werden. Der Patient darf durch die Ausgestaltung und den Verwendungszusammenhang der Chipkarte nicht zur pauschalen Offenbarung seiner Daten gezwungen sein. So sind Daten auf der Chipkarte so zu ordnen, daß z. B. beim Zahnarzt die gynäkologische Behandlung geheim bleiben kann.

Es darf keine „Einwilligung" in Chipkarten und Chipkartensysteme mit verminderter Datensicherheit geben. Der Gesetzgeber muß die Patienten vor „billigen Gesundheitskarten" ohne ausreichende Sicherung vor einer Nutzung durch Dritte schützen.

5. Sicherstellung der Integrität und Authentizität der Daten

Zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der Daten auf Chipkarten im Gesundheitswesen und zur Differenzierung der Zugriffsmöglichkeiten nach dem Grundsatz der Erforderlichkeit in unterschiedlichen Situationen sind kryptographische Verfahren sowie geeignete Betriebssysteme zur Abschottung unterschiedlicher Anwendungsbereiche nach dem Stand der Technik in Chipkarten und Schreib-/Lese-Terminals zu implementieren. Eine Protokollierung der Lösch- und Schreibvorgänge auf der Karte ist unverzichtbar.

Darüber hinaus ist für das infrastrukturelle Kartenumfeld (Herstellung, Verteilung, Personalisierung, Rücknahme) sicherzustellen, daß ausreichende technische und organisatorische Maßnahmen Berücksichtigung finden. Für die zur Erstellung und Personalisierung von Gesundheits-Chipkarten dienenden Systeme sowie die informationstechnischen Systeme und Verfahren, mit denen Daten auf der Chipkarte gelesen, eingetragen, verändert, gelöscht oder verarbeitet werden, muß der gleiche hohe Sicherheitsstandard erreicht werden.

6. Keine neuen zentralen medizinischen Datensammlungen

   Der Einsatz von Chipkarten im Gesundheitswesen darf nicht zur Entstehung neuer zentraler Dateien von Patientendaten bei Kassenärztlicher Vereinigung, Krankenkassen, Kartenherstellern oder sonstigen Stellen führen. Dies gilt auch für das Hinterlegen von Sicherungskopien der auf der Karte gespeicherten medizinischen Daten. Es steht in der freien Entscheidung der Betroffenen, ob sie dem Arzt ihres Vertrauens eine umfassende Pflege aller Chipkarten-Daten – einschließlich der Sicherungskopien – übertragen oder nicht.

7. Leserecht des Karteninhabers

   Der Karteninhaber muß das Recht und die Möglichkeit haben, seine auf der Chipkarte gespeicherten Daten vollständig zu lesen.

8. Suche nach datenschutzfreundlichen Alternativen

   Angesichts der aufgezeigten Gefährdungen der informationellen Selbstbestimmung im Gesundheitswesen muß die Suche nach datenschutzfreundlichen Alternativen zur Chipkarte fortgesetzt werden.

Vorstehende Kriterien sind der Maßstab für die datenschutzrechtliche Bewertung von Projekten für die Einführung von Chipkarten im Gesundheitswesen.

Die Datenschutzbeauftragten von Bund und Ländern fordern die Gesetzgeber auf, die dringend notwendigen Regelungen zur Sicherung der Rechte von Patienten und Ärzten zu schaffen. Ebenso ist durch die Gesetzgeber den Besonderheiten der Datenverarbeitung auf Chipkarten durch bereichsspezifische Regelungen Rechnung zu tragen.

Anlage 6

Entschließung
der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995
zu Forderungen an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien (außerhalb der Öffentlichkeitsfahndung der Ermittlungsbehörden)

1. Für die Übermittlung von personenbezogenen Daten durch Justiz und Polizei an die Medien sollte eine bereichsspezifische Rechtsgrundlage geschaffen werden. Die Regelung sollte für den betroffenen Bürger den Umfang des Eingriffs in sein Recht auf informationelle Selbstbestimmung erkennbar machen.

2. Die Übermittlung personenbezogener Daten an die Medien ist nur ausnahmsweise gerechtfertigt, wenn das Verfahren gerade im Hinblick auf die Person des Betroffenen oder die besonderen Umstände der Tat für die Öffentlichkeit von überwiegendem Interesse ist.

3. Bei der Entscheidung, ob und in welchem Umfang personenbezogene Daten an die Medien übermittelt werden, sind die schutzwürdigen Belange der Betroffenen zu berücksichtigen. Dazu zählen insbesondere die privaten und beruflichen Folgen für das Opfer, den Beschuldigten/Angeklagten und deren Angehörige sowie die Schwere, die Umstände und die Folgen des Delikts.

   Bei der Übermittlung von personenbezogenen Daten über Beschuldigte/Angeklagte sind auch der Grad des Tatverdachts und der Stand des Verfahrens zu berücksichtigen. Vor Beginn der öffentlichen Hauptverhandlung ist ein besonders strenger Maßstab an das Vorliegen eines „überwiegenden Interesses" der Öffentlichkeit anzulegen.

   Bis zur rechtskräftigen Verurteilung ist die Unschuldsvermutung zugunsten des Beschuldigten oder Angeklagten zu beachten. Zu unterlassen sind alle Auskünfte oder Erklärungen, die geeignet sind, die Unbefangenheit der Verfahrensbeteiligten zu beeinträchtigen. Akteneinsicht durch Medienvertreter kommt nicht in Betracht.

4. Grundsätzlich sind in Auskünfte und Erklärungen über das Ermittlungs- und Strafverfahren keine Namen und sonstige personenbezogene Angaben, die Opfer von Straftaten, Zeugen, Beschuldigte und Angeklagte bestimmbar machen, aufzunehmen. Vor allem bei Hinweisen auf den Wohnort, das Alter, den Beruf und die familiären Verhältnisse oder sonstigen sozialen Bindungen (z. B. Partei- oder Vereinsmitgliedschaft) ist zu prüfen, inwieweit dadurch eine Identifizierung des Betroffenen möglich wird.

5. Personenbezogene Daten dürfen nicht übermittelt werden, wenn besondere bundesgesetzliche oder landesgesetzliche Verwendungsregelungen entgegenstehen.

6. Ist die Bekanntgabe der Person des Beschuldigten oder Angeklagten wegen des überwiegenden öffentlichen Interesses gerechtfertigt, muß auch bei der Übermittlung sonstiger personenbezogener Daten abgewogen werden, ob diese Informationen für die Berichterstattung über die Tat selbst oder die Hintergründe, die zu der Tat geführt haben, erforderlich sind, und in welchem Umfang der Betroffene dadurch in seinem Persönlichkeitsrecht beeinträchtigt wird.

7. Die Bekanntgabe von Vorstrafen ist nur ausnahmsweise zulässig. Sie setzt voraus, daß die frühere Verurteilung im Bundeszentralregister noch nicht getilgt und ihre Kenntnis für eine nachvollziehbare Berichterstattung über eine schwerwiegende Straftat – auch unter Berücksichtigung des Persönlichkeitsrechts des Betroffenen und des Resozialisierungsgedankens – erforderlich ist. Besondere Zurückhaltung ist bei Auskünften und Erklärungen über Sachverhalte geboten, die der früheren Verurteilung zugrunde liegen.

8. Wegen des überragenden Schutzes von Minderjährigen und Heranwachsenden ist bei Auskünften und Erklärungen über Verfahren gegen diesen Personenkreis besondere Zurückhaltung hinsichtlich der Bekanntgabe personenbezogener Daten zu wahren.

9. Opfer, Zeugen und Familienangehörige haben in der Regel keine Veranlassung gegeben, daß ihre persönlichen Lebensumstände in der Öffentlichkeit bekannt gemacht werden. Die Übermittlung personenbezogener Daten über diesen Personenkreis an die Medien kommt deshalb grundsätzlich nicht in Betracht.

10. Bildveröffentlichungen greifen wegen der damit verbundenen sozialen Prangerwirkung besonders tief in das Persönlichkeitsrecht des Betroffenen ein. Eine Bildherausgabe kommt daher für Zwecke der Medienberichterstattung nicht in Betracht.

Anlage 7

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

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

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

Die wichtigsten Ziele sind:

1. Weitgehende Vereinheitlichung der Vorschriften für den öffentlichen und privaten Bereich mit dem Ziel eines hohen, gleichwertigen Schutzes der Betroffenen, beispielsweise bei der Datenerhebung und bei der Zweckbindung bis hin zur Verarbeitung in Akten.

2. Erweiterung der Rechte der Betroffenen auf Information durch die datenverarbeitenden Stellen über die Verwendung der Daten, auf Auskunft, auf Widerspruch und im Bereich der Einwilligung.

3. Verpflichtung zu Risikoanalyse, Vorabkontrolle, Technikfolgenabschätzung und zur Beteiligung der Datenschutzbeauftragten bei der Vorbereitung von Regelungen mit Auswirkungen auf den Datenschutz.

4. Verbesserung der Organisation und Stärkung der Befugnisse der Datenschutzkontrolle unter den Gesichtspunkten der Unabhängigkeit und der Effektivität.

5. Einrichtung und effiziente Ausgestaltung des Amtes eines internen Datenschutzbeauftragten in öffentlichen Stellen.

6. Weiterentwicklung der Vorschriften zur Datensicherheit, insbesondere im Hinblick auf Miniaturisierung und Vernetzung.

Darüber hinaus machen die Datenschutzbeauftragten folgende Vorschläge:

7. Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen und Regelung der Videoüberwachung.

8. Stärkere Einbeziehung von Presse und Rundfunk in den Datenschutz; Aufrechterhaltung von Sonderregelungen nur, soweit dies für die Sicherung der Meinungsfreiheit notwendig ist.

9. Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren.

10. Sicherstellung der informationellen Selbstbestimmung bei Multimedia-Diensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsformen anzubieten, durch den Schutz vor übereilter Einwilligung, z. B. durch ein Widerrufsrecht, und durch strenge Zweckbindung für die bei Verbindung, Aufbau und Nutzung anfallenden Daten.

11. Besondere Regelungen für Chipkarten-Anwendungen, um die datenschutzrechtliche Verantwortung aller Beteiligten festzulegen und den einzelnen vor unfreiwilliger Preisgabe seiner Daten zu schützen.

12. Schutz bei Persönlichkeitsbewertungen durch den Computer, insbesondere durch Beteiligung des Betroffenen und Nachvollziehbarkeit der Computerentscheidung.

13. Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing.

14. Verbesserung des Datenschutzes bei grenzüberschreitender Datenverarbeitung; Datenübermittlung ins Ausland nur bei angemessenem Datenschutzniveau.

Anlage 8

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

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

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

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

Anlage 9

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

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

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

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

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

Anlage 10

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

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

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

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

Sie betonen jedoch, daß die herkömmlichen weitreichenden Eingriffsbefugnisse auch unter wesentlich veränderten Bedingungen nicht einfach auf die neuen Formen der Individual- und Massenkommunikation übertragen werden können. Die zum Schutz der Persönlichkeitsrechte des einzelnen gezogenen Grenzen müssen auch unter den geänderten tatsächlichen Bedingungen der Verwendung der modernen Informationstechnologien aufrechterhalten und gewährleistet werden. Eine Wahrheitsfindung um jeden Preis darf es auch insoweit nicht geben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher Thesen zur Bewältigung dieses Spannungsverhältnisses entwickelt.

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

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

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

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

Anlage 11

Entschließung
der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997
Beratungen zum StVÄG 1996

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Entwicklung, im Gesetzgebungsverfahren zu einem Strafverfahrensänderungsgesetz 1996 die Gewährleistung der informationellen Selbstbestimmung im Strafverfahren nicht nur nicht zu verbessern, sondern vielmehr bestehende Rechte sogar noch zu beschränken. Dies gilt insbesondere für den Beschluß des Bundesrates, der gravierende datenschutzrechtliche Verschlechterungen vorsieht.

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

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

Die Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung sind nicht hinreichend bestimmt. So wird z. B. nicht angemessen zwischen Beschuldigten und Zeugen differenziert. Für Privatpersonen und Stellen, die nicht Verfahrensbeteiligte sind, wird als Voraussetzung zur Auskunfts- und Akteneinsicht lediglich ein vages „berechtigtes" statt eines rechtlichen Interesses gefordert.

Die Regelungen über Inhalt, Ausmaß und Umfang von Dateien und Informationssystemen mit personenbezogenen Daten bei Staatsanwaltschaften sind unzureichend. Das hat zur Folge, daß nahezu unbeschränkt Zentraldateien oder gemeinsame Dateien eingerichtet und Daten ohne Berücksichtigung der Begehungsweise und Schwere von Straftaten gespeichert werden können. Die Zugriffsmöglichkeiten der Strafverfolgungs- und Strafjustizbehörden auf diese Daten gehen zu weit. Darüber hinaus werden Standardmaßnahmen des technischen und organisatorischen Datenschutzes (z. B. Protokollierung, interne Zugriffsbeschränkungen etc.) weitgehend abgeschwächt.

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

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

Beispiele hierfür sind:

Der Richtervorbehalt für die Anordnung der Öffentlichkeitsfahndung und der längerfristigen Observation soll gestrichen werden.

Die Verwendungsbeschränkungen bei Daten, die mit besonderen Erhebungsmethoden nach dem Polizeirecht gewonnen wurden, sollen herausgenommen werden.

Das Auskunfts- und Akteneinsichtsrecht auch für öffentliche Stellen soll erheblich erweitert werden.

Detaillierte Regelungen für Fälle, in denen personenbezogene Daten von Amts wegen durch Strafverfolgungs- und Strafjustizbehörden an andere Stellen übermittelt werden dürfen, die im weitesten Sinne mit der Strafrechtspflege zu tun haben, sollen gestrichen werden.

Das Verbot soll gestrichen werden, über die Grunddaten hinausgehende weitere Angaben nach Freispruch, endgültiger Verfahrenseinstellung oder unanfechtbarer Ablehnung der Eröffnung des Hauptverfahrens Daten in Dateien zu speichern.

Speicherungs- und Löschungsfristen für personenbezogene Daten in Dateien sollen ersatzlos gestrichen werden.

Kontrollverfahren für automatisierte Abrufverfahren sollen aufgehoben werden, und die Verwendungsbeschränkungen für Protokolldaten sollen entfallen.

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

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

Anlage 12

Entschließung
der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997
Genetische Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke

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

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

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

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

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

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

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

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

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

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

Eine Speicherung kommt insbesondere dann nicht in Betracht, wenn der Tatverdacht gegen den Beschuldigten ausgeräumt wurde. Bereits erfolgte Speicherungen sind zu löschen.

Gleiches gilt für den Fall, daß die Anordnung der DNA-Untersuchung oder die Art und Weise ihrer Durchführung unzulässig war.

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

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

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

Anlage 13

Entschließung
der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997
Geplante Verpflichtung von Teledienstanbietern, Kundendaten an Sicherheitsbehörden zu übermitteln

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

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

Mit guten Gründen haben deshalb die Länder davon abgesehen, in den inzwischen von den Ministerpräsidenten unterzeichneten Staatsvertrag über Mediendienste eine vergleichbare Vorschrift aufzunehmen. In der Praxis werden sich aber für Bürger und Online-Diensteanbieter schwierige Fragen der Abgrenzung zwischen den Geltungsbereichen des Mediendienste-Staatsvertrags und des Teledienstedatenschutzgesetzes ergeben. Auch aus diesem Grund halten die Datenschutzbeauftragten eine Streichung der Vorschrift des § 5 Absatz 3 aus dem Entwurf für ein Teledienstedatenschutzgesetz für geboten.

Anlage 14

Entschließung
der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997
Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen

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

Die folgenden Beispiele machen dies deutlich:

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

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

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

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

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

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

Anlage 15

Entschließung
der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997
Achtung der Menschenrechte in der Europäischen Union

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

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

Anlage 16

Entschließung
der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997
Informationelle Selbstbestimmung und Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren

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

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

Bild-Ton-Aufzeichnungen ermöglichen eine vollständige und authentische Dokumentation nicht nur des Inhalts, sondern auch der Entstehung und Begleitumstände einer Aussage. Die Beurteilung ihres Beweiswerts wird dadurch deutlich verbessert. Zugleich dient eine nur einmalige Vernehmung, die möglichst zeitnah zum Tatgeschehen durchgeführt und aufgezeichnet wird, der Wahrheitsfindung und erhöht die Qualität der gerichtsverwertbaren Daten („Vermeidung kognitiver Dissonanzen"). Ausgehend von diesen Überlgungen, hat der Gesetzgeber unter Einbeziehung von Erkenntnissen der Vernehmungspsychologie zu prüfen, ob und inwieweit eine wortgetreue Abfassung von Vernehmungsniederschriften ausreicht und eine Aufzeichnung der Aussage nur im Wort auf Tonband für die Zwecke des Strafverfahrens in ihrer Beweisqualität der Videotechnologie sogar überlegen ist.

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

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

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

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

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

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

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

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

Anlage 17

Staatliche Eingriffsbefugnisse in der modernen Informationsgesellschaft
(Von einer Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder erarbeitetes Thesenpapier; zustimmend zur Kenntnis genommen von der 52. Konferenz am 22. Oktober 1996.)

I. Vorbemerkung:

Die tiefgreifende Entwicklung der modernen Telekommunikation (insbesondere durch Privatisierung der Netze, weite Verbreitung nichtstationärer Telefongeräte, Digitalisierung der Kommunikation), die rasche Fortentwicklung und weltweit vernetzte Nutzung der Informationstechnologie zu Kommunikationszwecken (z. B. Mailboxen, Internet) und Zwecken der Informations- und Güterbeschaffung (z. B. Online-Datenbanken, Teleshopping) sowie die neuen Medien lassen die traditionellen Grenzen zwischen Medien-, Kommunikations- und Informationstechnik verschwinden und führen zu einem grundlegend veränderten Kommunikationsverhalten der Bürger. Traditionelle Büroarbeiten werden über Teleworking Gegenstand digitalisierter Übertragungen und damit überwachbar, Telebanking begründet die Überwachbarkeit von Banktransaktionen, Teleshopping kann zum transparenten Konsumverhalten führen, die Nutzung von Fernsehen mit Rückkanal oder der Informationsangebote des Rundfunks im Internet führen zur Nachvollziehbarkeit der Mediennutzung. Die „Informationsgesellschaft" wird von der Zukunftsvision zur Realität. Damit gehen Gefahren durch die Nutzung der neuen Technik zu kriminellen Zwecken einher. Es ist nicht nur legitim, sondern geboten, daß die Strafverfolgungsbehörden in die Lage versetzt werden, diesen Mißbräuchen zu begegnen.

Die dahin gehenden gesetzgeberischen und technischen Anstrengungen dürfen jedoch aus datenschutzrechtlicher Sicht nicht zur Folge haben, daß in die Grundrechte der Bürger, insbesondere in ihr informationelles Selbstbestimmungsrecht, aber auch in das Fernmeldegeheimnis und das Recht auf unbeobachtete Kommunikation mehr eingegriffen wird, als unabdingbar erforderlich. Die verfassungsrechtlich garantierten Freiheitsräume des einzelnen müssen auch bei Nutzung der neuen Techniken erhalten bleiben.

II. Konkret bedeutet dies:

1. Neue technische Bedingungen erfordern neue gesetzliche Regelungen

Die Eingriffstiefe der bestehenden Vorschriften über die Überwachung des Fernmeldeverkehrs (§ 100 a StPO, § 39 AWG, Gesetz zu Art. 10 GG) und über die Auskunft über den Fernmeldeverkehr (§ 12 FAG) erhält durch das Entstehen immer größer werdender Datenbestände über das Nutzungsverhalten (und dem dadurch bedingten Entstehen von Persönlichkeitsprofilen) eine neue Dimension. Vor diesem Hintergrund ist es fraglich, ob die genannten Regelungen noch eine verfassungsrechtlich ausreichende Rechtsgrundlage für Eingriffe in die digitalisierte Kommunikation darstellen. Wenn die Bedingungen der menschlichen Kommunikation und des sozialen Verhaltens insgesamt durch die moderne Telekommunikation und die Informationstechnologie grundlegend verändert werden, können diese Vorschriften, die unter gänzlich anderen Bedingungen geschaffen wurden, nicht einfach auf die neuen Formen der Telekommunikation angewendet werden. Das Rechtsstaatsprinzip, insbesondere auch der Bestimmtheitsgrundsatz, erfordern vielmehr Eingriffsgrundlagen, die unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes den neuen Bedingungen einer wesentliche größeren Wirkungsbreite Rechnung tragen.

2. Grundsatz der spurenlosen Kommunikation

Kommunikation mit Hilfe elektronischer Datenverarbeitung hinterläßt regelmäßig – vom Nuzter unbemerkt – umfassende Spuren. Aus datenschutzrechtlicher Sicht ist immer wieder betont worden, daß solche Verfahren Vorrang verdienen, die den Kommunikationsteilnehmern ein Höchstmaß an Anonymität gegenüber Netzbetreibern und Dienstleistungsanbietern sichern. Dies dient auch dem Schutz der Bürger vor kriminellen Mißbräuchen der bei der Interaktion entstehenden Informationen.

Schon bei der Gestaltung der Kommunikationstechniken ist deshalb darauf zu achten, daß keine oder möglichst wenige personenbezogene Daten zum Betrieb der Systeme verwendet werden müssen.

Ist die Datenerhebung und -speicherung aus betrieblichen Gründen erforderlich, so sind die Daten unverzüglich zu löschen, sobald sie für diesen Zweck nicht mehr benötigt werden. Auch der Gesetzgeber darf Vorratsdatenhaltung allein zum Zweck künftig eventuell denkbarer Strafverfolgung nicht anordnen.

3. Zunehmende Bedeutung von Verbindungs- und Bestandsdaten

Die Zunahme der Nutzung der Kommunikationstechnologie führt dazu, daß bereits auf der Ebene der bloßen „Verbindungsdaten" (wer hat mit wem Verbindung aufgenommen?) Verhaltensprofile erstellt werden können. Diese Daten können in ihrer Aussagekraft Inhaltsdaten erreichen oder übertreffen. Die bisherige rechtliche Grundlage für ihre Nutzung durch Strafverfolgungsbehörden in § 12 FAG ist zu weit gefaßt. Eine neue, normenklare Eingriffsnorm, die den Verhältnismäßigkeitsgrundsatz auch unter den neuen Bedingungen berücksichtigt, muß in die StPO aufgenommen werden und § 12 FAG ersetzen. Eine weitere Verlängerung der Geltungsdauer dieser Vorschrift kann nicht hingenommen werden. Insbesondere bei Mailboxdiensten kann aus den „Bestandsdaten" (der Tatsache der Registrierung als Vertragspartner und den näheren vertraglichen Nutzungsbedingungen, vgl. zum Begriff § 4 Abs. 1 S. 1 TDSV) bereits auf weltanschauliche, religiöse oder sonstige persönliche Interessen und Neigungen geschlossen werden. Der staatliche Zugriff auf solche Bestandsdaten sollte zumindest den gleichen Bedingungen wie die Beschlagnahme (§§ 94 ff. StPO) unterliegen.

4. Besonderer Schutz der Informationsfreiheit

Informationsvorgänge, die dem traditionellen Medienbereich zugehörig waren, werden künftig immer mehr zum Gegenstand der Nutzung moderner Kommunikationstechnologien. In Anbetracht dieser Entwicklung haben die Datenschutzbeauftragten des Bundes und der Länder datenschutzrechtliche Eckpunkte zu den Mediendiensten formuliert. Wenn Online-Abrufe das Fernsehen oder den Blick in die Zeitung und in das Lexikon ersetzen, wird durch die staatliche Auswertung von dabei entstandenen Informationsbeschaffungsspuren auch in das Grundrecht auf Informationsfreiheit eingegriffen. Dieses umfaßt den Anspruch auf staatlich nicht registrierte Information und deckt sich insofern auch mit dem Schutzbereich des informationellen Selbstbestimmungsrechts. Dem Grundsatz der anonymen Kommunikation und der unbeobachteten Information kommt zur Sicherung eines demokratischen Gemeinwesens besondere Bedeutung zu.

Ein Eingriff in dieses Grundrecht wäre nur im überwiegenden Allgemeininteresse unter besonderer Wahrung des Verhältnismäßigkeitsgrundsatzes zulässig. Seiner Bedeutung muß auch durch restriktive Anwendung der Eingriffsbefugnisnormen Rechnung getragen werden.

5. Schutz besonderer Vertrauensverhältnisse

Die Entwicklung zur Informationsgesellschaft hat zur Folge, daß traditionelle papiergebundene Speicherungs- und Kommunikationsformen zugunsten digitalisierter Datenverarbeitung zurückgedrängt werden. Die vom Gesetzgeber der „Wahrheitsfindung um jeden Preis" gezogenen Grenzen müssen aber auch unter den Bedingungen der modernen Informationstechnologie aufrechterhalten und gewährleistet bleiben. Die strafprozessualen Durchsuchungsbeschränkungen und Beschlagnahmeverbote zum Schutz besonderer Vertrauensverhältnisse (Arztgeheimnis, anwaltliches Vertrauensverhältnis etc. dürfen – unabhängig von der Frage, ob aus sonstigen Gründen eine derartige Auslagerung von Daten zulässig ist – nicht dadurch entwertet werden, daß ein Zugriff der Strafverfolgungsbehörden auf vergleichbare digitalisiert verarbeitete Informationen, die im Zugriff, nicht aber im traditionellen „Gewahrsam" des Zeugnisverweigerungsberechtigten stehen, ohne diese Schranken zulässig ist. Die Anknüpfung der StPO an den „Gewahrsam" des Zeugnisverweigerungsberechtigten (§ 97 Abs. 2 S. 1 StPO) wird den modernen technischen Bedingungen und den daraus folgenden Schutzbedürfnissen nicht gerecht (z. B. beim Einsatz von Mailboxen oder Patientenchipkarten). Die Beschlagnahme- und Durchsuchungsverbote der StPO müssen auch für solche „ausgelagerten" digitalisierten Speicherungen gelten.

6. Kryptographische Verfahren (Verschlüsselungsverbot)

Die Möglichkeit, Kommunikation durch geeignete Maßnahmen vor unberechtigten Zugriffen zu schützen, ist ein traditionelles Recht des Bürgers. Unter den Bedingungen der neuen Technik ist ein geeignetes, leicht verfügbares und weitgehend sicheres Mittel der Einsatz kryptographischer Verfahren (insbesondere der Verschlüsselung), deren Bedeutung für den Datenschutz herausragend ist und deren weitgehenden Einsatz die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt gefordert hat.

Die Datenschutzbeauftragten wenden sich nachhaltig dagegen, daß den Nutzern die Verschlüsselung des Inhalts ihrer Nachrichten verboten wird. Die Möglichkeit für den Bürger, seine Kommunikation durch geeignete Maßnahmen vor unberechtigten Zugriffen zu schützen, ist ein traditionelles verfassungsrechtlich verbürgtes Recht. Aus Sicht des Datenschutzes besteht andererseits durchaus Verständnis für das Interesse der Sicherheits- und Strafverfolgungsbehörden, sich rechtlich zulässige Zugriffsmöglichkeiten nicht dadurch versperren zu lassen, daß Verschlüsselungen verwandt werden, zu denen sie keinen Zugriff haben. Eine Reglementierung der Verschlüsselung, z. B. durch Schlüsselhinterlegung, erscheint aber aus derzeitiger technischer Sicht kaum durchsetzbar, da entsprechende staatliche Maßnahmen insbesondere im weltweiten Datenverkehr ohnehin leicht zu umgehen und kaum kontrollierbar wären.

7. Corporate Networks

Die technischen Bedingungen der Kommunikation von lokalen Netzen, die über öffentliche Leitungen zu erreichen sind (Corporate Networks, „Intranets" o. ä.), ermöglichen den Strafverfolgungsbehörden ein Eindringen in interne Kommunikationsvorgänge von Behörden und privaten Unternehmen sowie sonstigen privaten und öffentlichen Stellen. Ein Abhören in solchen Netzen ist nach der gegenwärtigen Rechtslage zwar unzulässig. Angesichts der Bestrebungen, hier Eingriffsbefugnisse zu schaffen, ist aus datenschutzrechtlicher Sicht auf folgendes hinzuweisen:

Die Befugnisse sind auf Maßnahmen in geschäftsmäßig genutzten Netzen zu beschränken. Das Eindringen in private, nichtwirtschaftlich genutzte Netze (beispielsweise in die familiäre häusliche Kommunikation zwischen Nebenstellen) würde die Privatsphäre unverhältnismäßig einschränken.

8. Bewegungsprofile bei der mobilen Telekommunikation

Die Aufzeichnung von Aktivmeldungen macht den jeweiligen Aufenthaltsort der Inhaber von Mobiltelefonen kenntlich. Hieraus können Bewegungsprofile entstehen, die das Mobilitätsverhalten der Betroffenen umfassend registrieren. Auf der Grundlage des geltenden Rechts sind derartige Aufzeichnungen und ihre Nutzung unzulässig.

Die Zulassung dieser Eingriffe würde einen neuartigen und gravierenden Eingriff in das Persönlichkeitsrecht darstellen. Falls es zum Zwecke der Strafverfolgung unerläßlich sein sollte, den Zugriff auf Aktivmeldungen von Mobiltelefonen zuzulassen, wäre dies allenfalls in Fällen vertretbar, in denen auch eine Überwachung des Mobiltelefonverkehrs richterlich angeordnet worden ist. Bei der Ausgestaltung einer etwaigen entsprechenden Befugnis muß der Schutz gesetzlich besonders geregelter Vertrauensverhältnisse sichergestellt werden. Betroffen können z. B. sein das Arzt- und Anwaltsgeheimnis, insbesondere auch der Grundsatz der Vertraulichkeit von Verteidigerkontakten und die Freiheit der Informationsgestaltung durch die Presse.

9. Transparenz und öffentliche Kontrolle

Die Nutzung neuer Techniken durch Strafverfolgungsbehörden erleichtert und erweitert unter verschiedenen Aspekten das Eindringen in private Informationen und Kommunikationen: Die Einrichtung automatisierter Schnittstellen bei den Netzbetreibern ermöglicht den Strafverfolgungsbehörden, ihre Befugnisse, auf konkrete Verbindungen zuzugreifen, einfach und schnell zu realisieren. Die digitalisierte Erfassung von Informationen bei den Strafverfolgungsbehörden ermöglicht schnelle und umfassende Auswertungen, leichte Weiterübermittlungen, dauerhafte Speicherungen abgehörter und aufgezeichneter Informationen. Diese neuen technischen Möglichkeiten dürfen nicht zu extensiver Ausweitung der Fernmeldeüberwachung führen. Es sind deshalb neue Mechanismen zu schaffen, die angesichts dieser neuen technischen Möglichkeiten verstärkt auf die Einhaltung des Verhältnismäßigkeitsgrundsatzes hinwirken. Hierzu wäre insbesondere eine Einführung von internen Berichtspflichten der Strafverfolgungsbehörden und die Einführung öffentlicher Statistiken über Durchführung und Erfolg solcher Maßnahmen geeignet. Außerdem sind Maßnahmen des technischen und organisatorischen Datenschutzes, insbesondere mit dem Ziel der Nachvollziehbarkeit der Zugriffe und der Nutzung, bereichsspezifisch zu regeln.

III. Schlußbemerkung:

Es muß ein kohärentes, in sich stimmiges System geschaffen werden, in dem alle staatlichen Eingriffe zu Strafverfolgungszwecken in das Kommunikationsverhalten unter Beachtung des Verhältnismäßigkeitsgrundsatzes geregelt werden. Die StPO ist der einzig geeignete Ort, die hier notwendigen Klarstellungen zu formulieren. Weder die Debatte um die Rechtsetzungskompetenz für Multimediadienste noch der Verweis auf die Internationaltät der Probleme und der erforderlichen Lösungsansätze rechtfertigen es, die genannten Fragen ungeregelt zu lassen, ihre Regelung aufzuschieben oder in technikbezogenen Rechtsmaterien zu verstecken.